LOGISTYKA • KOMUNIKACJA • BEZPIECZEŃSTWO

WYBRANE PROBLEMY

Redakcja naukowa
Marek Grzybowski, Janusz Tomaszewski

Gdynia 2009

Recenzenci:
dr hab. Stanisław Piocha
dr hab. Wiesław Czyżowicz
assoc. prof. Roman Jašek
assoc. prof. Samuel Uhrin
doc. Zlatan Šoškić
doc. Angela V. Piatova
doc. Vladislav Hofraiter

Adiustacja
Ewelina Bemke

ISBN 978-83-61505-04-4

Druk i oprawa: Sowa – druk na życzenie
www.sowadruk.pl
tel. 022 431-81-40

Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni
ul. Kielecka 7, 81-303 Gdynia
www.wsaib.pl

SPIS TREŚCI

WSTĘP

Na przełomie XX i XXI wieku w gospodarce światowej nastąpiły istotne przemiany. Dywersyfikacji produkcji towarzyszą po dzień dzisiejszy zmiany w rozmieszczeniu rynków pracy i rozwoju rynków konsumpcyjnych i przemysłowych. Do najdynamiczniej rosnących rynków zarówno biznesowych i konsumpcyjnych należą rynki takich krajów jak Chiny, Indie, Brazylia, czy Turcja. W Unii Europejskiej do szybko rosnących regionów zalicza się grupa krajów Europy Środkowej i Wschodniej. Taki rozkład rynków determinuje zmiany w wymianie handlowej między Europą a innymi rynkami, a to z kolei wymusza rozwój sieci logistycznych.

Zmiany na międzynarodowym rynku pracy i konsumpcyjnym znajdują swoje odzwierciedlenie w transporcie morskim. Przewozy morskie tylko w latach 2005-2008 wzrosły z 6,7 mld ton do 7,4 mld ton. Globalny popyt na przewozy drogą morską osiągnął 32 mld tonomil (w 2008 r.). Szacuje się, że rocznie popyt ten rósł do 2008 r. o 5%. Zakłada się, że po okresie recesji ten trend powróci do poprzedniego stanu co oznacza, że w 2030 r. może nastąpić nawet podwojenie przewozów drogą morską. W latach 1970-2008 międzynarodowy handel morski wzrósł o prawie 190% wraz z wzrostem konsumpcji i zmianami na międzynarodowym rynku produkcji. Przewozy ładunków płynnych wzrosły w tym okresie prawie o 100%. Przewozy ładunków suchych w latach 1970-2008 wzrosły natomiast o ponad 260%. Taka dynamika wymiany towarowej w wymiarze globalnym sprawiła szczególnie w ostatnich latach szybki rozwój sieci logistycznych i systemów informacyjnych. Globalnym powiązaniom handlowym towarzyszy sieć globalnych powiązań komunikacyjnych i łańcuchów logistycznych.

Kryzys na globalnym rynku finansowym w połowie 2008 r., a następnie załamanie się popytu na rynku dóbr i usług zahamowało

wzrost ładunków w kontenerach oraz przewozów ro-ro na rynku żeglugowym i portowym, a w mniejszym stopniu ładunków masowych. Okres prosperity wywołał na rynku transportu optymizm w planowaniu pozyskiwania nowych środków do transportu lądowego, lotniczego i morskiego. Duże nakłady poniesiono również na budowę infrastruktury logistycznej, w tym niezbędnej do przeładunku dynamicznie rosnącej podaży towarów w kontenerach. Załamanie koniunktury w wiodących gospodarkach wywołało najpierw perturbacje na rynku transportu morskiego, potem w portach (zmniejszone przeładunki), a następnie w przemyśle budowy statków, co przejawiało się wycofaniem armatorów z zamówień na nowe statki. To z kolei wywołało spadek popytu na wyroby stalowe i specjalistyczne urządzenia. To przykład sytuacji kryzysowej na kilku powiązanych z systemem logistycznym rynkach.

Autorzy badań zamieszonych w publikacji pt. *Logistyka, komunikacja i bezpieczeństwo* starali się nie tylko dokonać diagnozy zagrożeń w obszarze logistyki, komunikacji i energetyki, ale również znaleźć odpowiedź na problemy dnia dzisiejszego, a także proponować rozwiązania umożliwiające bezpieczne funkcjonowanie sieci logistycznych oraz informacyjnych.

W części 1. monografii pt. ***Logistyka i bezpieczeństwo*** autorzy zwrócili uwagę na cały zakres bezpieczeństwa procesów logistycznych, aż po bezpieczeństwo energetyczne i fizyczne obszarów logistycznych, a nawet aspekty techniczne bezpieczeństwa jednostek transportu kolejowego.

W części 2. pt. ***Komunikacja i bezpieczeństwo*** autorzy podzielili się wynikami badań dotyczących zarówno sprawności przepływu informacji wewnątrz organizacji w sytuacjach stabilnych i kryzysowych, jak i aspektami ochrony informacji przedsiębiorstwa. W tej części prezentowane są również wyniki badań nad bezpieczeństwem łączności w najnowszych rozwiązaniach ICT w aspekcie technicznym i organizacyjnym.

Monografia powstała na potrzeby tych czytelników, którzy zainteresowani są spojrzeniem na sprawy bezpieczeństwa z punktu widzenia menedżera sieci logistycznych, organizatora wymiany handlowej, czy osoby zarządzającej informacją w przedsiębiorstwie w warunkach stabilnych i kryzysowych.

Marek Grzybowski, Janusz Tomaszewski

Część 1

Logistyka i bezpieczeństwo

Wiesław Czyżowicz*

BEZPIECZEŃSTWO ŁAŃCUCHA LOGISTYCZNEGO W MIĘDZYNARODOWYM OBROCIE TOWAROWYM – TRENDY I TENDENCJE ROZWOJU W XXI WIEKU

Wstęp

Międzynarodowa wymiana towarowa – nie tylko handel towarami, ale i obrót (np. w ramach tzw. celnych procedur uszlachetniania czy tranzytu) – we współczesnych warunkach zdynamizowania globalizacji w coraz większym zakresie wiąże się z prawno-instytucjonalnymi mechanizmami jej regulacji odnoszącymi się zwłaszcza do kilku głównych problemów.

Wśród tych, jakie w ostatniej dekadzie znalazły się w centrum uwagi polityki nie tylko poszczególnych państw czy organizacji międzynarodowych, ale i przedsiębiorstw działających na rynku światowym na plan pierwszy wybiły się trzy z nich:

- ułatwienia w przepływie towarów przez granice celne;
- uproszczenia procedur celnych;
- bezpieczeństwo międzynarodowego łańcucha dostaw towarowych.

Każdy ze wskazanych problemów dominował w różnym okresie ostatnich kilkudziesięciu lat. Jeśli w końcu XX wieku, wraz z dynamicznym rozwojem międzynarodowego obrotu towarowego zarówno firmy włączone do tego procesu jak i państwa oraz organizacje gospodarcze, przede wszystkim Światowa Organizacja Handlu (WTO/GATT), Światowa Organizacja Celnictwa (WCO) jak i międzynarodowe organizacje gospodarcze, tak międzyrządowe (np. UE, EFTA, OECD i inne) jak i pozarządowe np. Międzynarodowa Izba Handlowa (ICC) czy Międzynarodowa Federacja Stowarzyszeń Agentów Celnych (IFCBA) czy Europejska Konfederacja Agentów Celnych –

* Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.

(CONFIAD) skupiały się na ułatwieniach i uproszczeniach obrotów towarowych, na szybkości ich dostaw i przepływu przez granice celne w myśl hasła „czas to pieniądz", to po zamachach terrorystycznych z 11 września 2001r. na plan pierwszy wysunęły się problemy bezpieczeństwa międzynarodowego łańcucha dostaw.

W tym momencie okazało się, że dla polityków, przede wszystkim w USA, nie pieniądze są najważniejsze lecz te wartości, które w powszechnym przekonaniu są najistotniejsze – życie i zdrowie. A te, niezależnie od zasadności przyjęcia tezy o zwiększonym ich zagrożeniu w rezultacie zdynamizowania procesów międzynarodowego handlu towarami w warunkach globalizacji, przesłoniły wymogi ułatwień i uproszczeń tego obrotu na rzecz zaostrzenia i efektywności kontroli ich przepływu przez granice. Podstawą okazały się tezy o powiązaniu międzynarodowych obrotów towarowych z zagrożeniem przemytu broni, amunicji i materiałów rozszczepialnych i/lub podwójnego stosowania jako źródeł zagrożenia bezpieczeństwa narodowego poszczególnych państw. Nawet jeśli nie dotyczyłoby wskazanych, to w odniesieniu także do innych wysokodochodowych towarów przemycanych na rynki krajów wysokorozwiniętych, powiązane zostało ze zjawiskiem tzw. prania brudnych pieniędzy służących lub mogących służyć finansowaniu zorganizowanych grup przestępczych i międzynarodowego terroryzmu.

Tezy te, niezależnie od ich realnej podstawy, legły u podłoża podjętych działań politycznych oraz stworzenia nowych i rozbudowania już istniejących mechanizmów instytucjonalno-prawnych metod regulacji tego obrotu. Takie rozwiązania miały na celu nie tylko zwiększenie efektywności kontroli obrotu, ale i – przynajmniej deklaratywnie – utrzymanie, a nawet rozbudowanie istniejących ułatwień i uproszczeń. Punktem wyjścia dla takiego podejścia okazało się nowoczesne środowisko międzynarodowego handlu towarami związanego z gospodarką elektroniczną i szerokim wykorzystywaniem w działalności firm oraz instytucji rządowych nowoczesnych technik informatycznych i komunikacyjnych (ICT).

W tym przypadku podtrzymując wymóg ogromnego zwiększenia efektywności kontroli międzynarodowego obrotu towarowego wskazano na możliwości rozwiązania dylematu między nią a szybkością przepływu towarów przez granice. Teoretycznie, wg twórców takich propozycji jest to już w chwili obecnej możliwe i ta „kwadratura koła" możliwa jest do korzystnego dla wszystkich zainteresowanych stron (biznesu międzynarodowego, przedsiębiorców, społeczeństw poszczególnych

państw i ich służb kontrolnych) rozwiązania. Przy tym założeniu nie wzięto jednak pod uwagę, a przynajmniej nie zbilansowano kosztów takiego rozwiązania. Okazało się, że bezpieczeństwo nade wszystko – niezależnie od realnego zagrożenia, jego zasadności i kosztów. Dzięki temu politycznemu zabiegowi ukształtowano nowy paradygmat polityki celnej i handlowej – nie tyle uproszczenia oraz ułatwienia w międzynarodowym obrocie towarowym, ile jego bezpieczeństwo i to nie w jednym kraju czy punkcie, ale w całym łańcuchu dostawy – od producenta, eksportera, spedytora, przewoźnika po ostatecznego odbiorcę. Pod pretekstem ogromnego zagrożenia wymienionych wartości przez międzynarodowy terroryzm poddano nie tylko wewnętrzne życie społeczno-gospodarcze i polityczne wielu demokratycznych państw wysokorozwiniętych procesowi ideologizacji, militaryzacji i rozszerzania policyjnych metod we wszystkich dziedzinach. To się przeniosło na arenę międzynarodową. Nie ominęło także międzynarodowego obrotu towarowego.

1. Nowe uwarunkowania międzynarodowego obrotu towarowego

Zagadnienie to stało się przedmiotem zainteresowania dla wielu służb odpowiedzialnych za bezpieczeństwo narodowe w jego najszerszym znaczeniu. Szczególna uwaga administracji celnych skupiona została na problemach bezpieczeństwa związane z handlem międzynarodowym, a precyzyjniej z międzynarodowym obrotem towarowym. To nie tylko kwestia handlu towarami militarnymi (bronią, uzbrojeniem, materiałami rozszczepialnymi czy binarnego przeznaczenia) regulowanymi międzynarodowymi konwencjami[1] ale i wieloma innymi towarami w tym przede wszystkim narkotykami oraz wieloma innymi mogącymi służyć do prania tzw. brudnych pieniędzy i finansowania terroryzmu.[2]

[1] Wykaz tych aktów można znaleźć na stronie domowej Departamentu Kontroli Eksportu Ministerstwa Gospodarki: http://www.mgip.gov.pl/GOSPODARKA/DKE/Akty/. Znajdują się na niej także ścieżki (linki) do aktów organizacji międzynarodowych, przede wszystkim Unii Europejskiej. Obszerne informacje na temat międzynarodowych porozumień eksportowych (Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group inne) oraz regulacji tych spraw w USA znajdują się na stronie domowej Biura Bezpieczeństwa i Przemysłu Ministerstwa Handlu USA: http://www.bis.doc.gov/PoliciesAndRegulations/MultilateralExportRegimes.htm .

[2] Por. informacje na ten temat na stronie domowej tzw. Grupy Egmont: http://www.egmontgroup.org/ oraz na stronie domowej Generalnego Inspektora

To nie tylko przemyt narkotyków, broni, binarnych środków, ale i np. obrót ginącymi lub zagrożonymi wyginięciem gatunkami flory i fauny oraz wieloma innymi).[3]

Te i wiele innych aspektów związanych ze współczesnym międzynarodowym handlem, a dokładniej obrotem, towarowym łączą się bezpośrednio z bezpieczeństwem nie tylko militarnym, ale i ekonomicznym społeczeństw państw uczestniczących w tym procesie. Nie jest to jednak zjawisko całkowicie nowe. Zagrożenie bezpieczeństwa życia i zdrowia ludzi, zwierząt czy roślin funkcjonowało i wcześniej w handlu międzynarodowym. Jednak jego całkowicie nowa jakość pojawiła się w okresie przemian ustrojowy w krajach tzw. obozu socjalistycznego zapoczątkowanych w początkach lat dziewięćdziesiątych XX w. przez polską aksamitną rewolucję zapoczątkowaną powstaniem szerokiego ruchu społeczno-politycznego „Solidarność".

Sytuacja ta jednak ulegała zmianie w następnej dekadzie, zwłaszcza po przystąpieniu Polski, na mocy tzw. Układu Europejskiego[4] do grupy państw stowarzyszonych z UE i uzyskujących preferencje w obrotach towarowych w miarę budowy strefy wolnego handlu. Układ ten nie tylko dawał nam pewne preferencje w handlu z państwami członkowskimi, ale i nakładał na Polskę określone wymogi, których spełnienie było *conditio sine qua non* dla uzyskania preferencji. Jednymi z takich wymogów były problemy związane z reformą naszego celnictwa, w tym procedur ustawodawstwa i procedur celnych, zmian struktury i zakresu zadań organów celnych. Wśród głównych zadań wówczas przyjętych w polskiej służbie celnej znalazła się harmonizacja prawa, procedur i zadań mających na celu z jednej strony wprowadzanie ułatwień i uproszczeń w procedurach celnych, z drugiej zaś zwiększenie

---

Informacji Finansowej:
http://www.mf.gov.pl/index.php?const=1&dzial=79&wysw=82&sub=sub8

[3] Por. akty prawne z tym problemem związane na stronie domowej polskiej służby celnej: http://www.mf.gov.pl/dokument.php?const=2&dzial=525&id=47104

[4] Układ Europejski Ustanawiający stowarzyszenie między Rzeczpospolitą Polską, z jednej strony, a Wspólnotami Europejskimi i ich państwami członkowskimi, z drugiej strony, [w:] Dz. U., z 27 stycznia 1994 r., załącznik do nr 11, poz. 38. Z punktu widzenia niniejszych rozważań niezwykle istotnym, bo wprowadzało nowe wymogi np. dotyczące dokumentowania pochodzenia towarów, było wejście w życie na 2 lata wcześniej niż wszedł w życie cały Układ, tzw. Umowy przejściowej dotyczącej handlu i spraw związanych z handlem między Rzecząpospolitą Polska a Europejską Wspólnotą Gospodarczą i Europejską Wspólnotą Węgla i Stali, [w:] Dz.U. z dnia 28 lutego 1992 r., Załącznik do nru 17, poz. 69. Był to w istocie III rozdział Układu Stowarzyszeniowego.

efektywności kontroli obrotu towarowego mającej zagwarantować większe bezpieczeństwo tego obrotu. Nie było to łatwe i do dziś, w zasadzie, proces ten nie został zakończony. Co więcej nowe projekty zmian strukturalnych polskiej służby celnej powodują szereg niepokojów związanych ze skutecznością jaką administracja ta w tej chwili osiągnęła.[5]

Przystąpienie Polski do UE na mocy Traktatu Akcesyjnego[6] pociągnęło za sobą przyjęcie przez nasz kraj wielu nowych rozwiązań także w zakresie polityki zagranicznej, w tym i handlu zagranicznego, rozwiązań w zakresie polityki handlowej , celnej oraz wielu uregulowań wynikających z całokształtu dorobku prawa unijnego tzw. *acquis communautaire*.[7]

---

[5] Por.: List otwarty zw. zawodowych Służby Celnej, [w:] POLSKA. „The Times", Warszawa, 2008-11-28, s. 15, a także wcześniejsze próby podejmowane w ramach inicjatywy tzw. Krajowej Administracji Skarbowej. Patrz np. E. Matuszewska, *Reforma: Połączenie celników i skarbówki – Krajowa Administracja Skarbowa zacznie funkcjonować od 1 stycznia 2008r.*, [w:] „Gazeta Prawna", Warszawa, 2007, 03-04÷02, a także 3 tomowe wydawnictwo pt. *Efektywna Administracja Skarbowa*, pod red. Z. Gilowskiej, H. Izdebskiego i K. Raczkowskiego, Ministerstwo Finansów, Wyd. DIFIN, Warszawa, 2007.

[6] Pełna nazwa tego aktu to: Traktat między Królestwem Belgii, Królestwem Danii, Republiką Federalną Niemiec, Republiką Grecką, Królestwem Hiszpanii, Republiką Francuską, Irlandią, Republiką Włoską, Wielkim Księstwem Luksemburga, Królestwem Niderlandów, Republiką Austrii, Republiką Portugalską, Republiką Finlandii, Królestwem Szwecji, Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej (Państwami Członkowskimi Unii Europejskiej) a Republiką Czeską, Republiką Estońską, Republiką Cypryjską, Republiką Łotewską, Republiką Litewską, Republiką Węgierską, Republiką Malty, Rzecząpospolitą Polską, Republiką Słowenii, Republiką Słowacką dotyczący przystąpienia Republiki Czeskiej, Republiki Estońskiej, Republiki Cypryjskiej, Republiki Łotewskiej, Republiki Litewskiej, Republiki Węgierskiej, Republiki Malty, Rzeczypospolitej Polskiej, Republiki Słowenii i Republiki Słowackiej do Unii Europejskiej, podpisany w Atenach w dniu 16 kwietnia 2003 r. (Dz.U. 2004 nr 90 poz. 864) oraz Dziennik Urzędowy Unii Europejskiej L 236 z 23 września 2003.

[7] Por. np.: E. Kawecka-Wyrzykowska, E. Synowiec (red.), *Unia Europejska. Integracja Polski z Unią Europejską*, IKC HZ, Warszawa 1996; E. Kawecka-Wyrzykowska, E. Synowiec (red.), *Unia Europejska. Przygotowania Polski do członkostwa*, IKC HZ, Warszawa 2001; W. Czyżowicz (red.), *Warunki i zadania w zakresie handlu zagranicznego po akcesji Polski do Unii Europejskiej*. Raport przygotowany przez Zespół Międzyresortowy. Tom I – IV, T. I Synteza, Rządowe Centrum Studiów Strategicznych, Warszawa, luty 2003. Ekspertyza, czy J. Barcz, E. Kawecka-Wyrzykowska i K. Michałowska-Gorywoda, *Integracja Europejska*, Wyd. Wolters Kluwer, Warszawa 2007.

Zmiany dotyczyły, przede wszystkim, naszej granicy wschodniej, która stała sie zewnętrzną granicą lądową Unii Europejskiej, a tym samym i zewnętrzną granicą celną unii celnej Wspólnoty Europejskiej. Pozostałe granice celne (z wyjątkiem morskiej i na lotniskach międzynarodowych) z Niemcami, Czechami , Słowacją i Litwą zniknęły. To ogromnie istotna zmiana tak z punktu widzenia odpowiedzialności za jej ochronę przez polskie służby kontrolne – przede wszystkim Straż Graniczną i Polską Administrację Celną. W tych dwóch dziedzinach nastąpiły ogromne zmiany formalne i organizacyjne.[8]

Dotyczyło to przede wszystkim przygotowań polskiej Straży Granicznej do dostosowania swoich standardów do standardów wynikających z Układu z Schengen. Efektem wysokiej oceny ochrony zewnętrznej granicy UE było przekazanie Polsce siedziby nowoutworzonej Agencji UE ds. Ochrony Zewnętrznej Granicy UE.[9]

Wraz z przystąpieniem do UE Polska stała się częścią składową unii celnej tego ugrupowania. W rezultacie tego faktu Polska utraciła suwerenność w handlu zagranicznym, ponieważ polityka handlowa i celna, taryfowa i pozataryfowa przeszły z narodowych decyzji do organów UE. Najbardziej istotnymi dla obrotów towarowych okazały się Dyrekcje Generalne Komisji UE ds. Handlu, Wspólnej Polityki Rolnej, Ceł i Podatków Pośrednich. W pełnym zakresie polskie służby celne, fitosanitarne i weterynaryjne przejęły całość regulacji odnoszących się do międzynarodowej wymiany towarowej. Jednak tylko polityka celna, prawo celne, procedury i dokumentacja celna są w pełni ujednolicone w UE. A przecież Polska jest nie tylko członkiem Unii Europejskiej, ale i uczestnikiem międzynarodowego obrotu towarowego z państwami trzecimi. Stosowanie rozwiązań unijnych nie może być powodem do niekorzystnych zmian w zakresie bezpieczeństwa tego obrotu. Co więcej, dzięki standardom unijnym stosowanych w naszym kraju, bezpieczeństwo to znacznie wzrosło, mimo, że współczesny rozwój stosunków społeczno-gospodarczych nabrał ogromnego tempa i przebiega w nowych jakościowo warunkach zewnętrznych.

[8] Szerzej na ten temat pr.: A. Maksimczuk, L. Sidorowicz, *Graniczna obsługa ruchu osobowego i towarowego w Unii Europejskiej (wybrane aspekty)*, Wyd. ALMAMER WSE, Warszawa 2008.

[9] Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej została ustanowiona na mocy rozporządzenia Rady (WE) nr 2007/2004 (26.10.2004, Dz. U. L 349 z 25.11.2004).

Przede wszystkim odnosi się to do zjawiska globalizacji i pogłębiania procesów regionalizacji.

Równocześnie z rozwojem tych zjawisk następował proces eliminacji wielu wcześniej istniejących barier w międzynarodowym obrocie towarowym i związanym z nim łańcuchem dostaw.

Towarzysząca tym procesom dynamika zmian technik komunikacyjnych i informacyjnych, nowoczesna organizacja obrotu towarowego, łańcucha dostaw oraz związanej z nim kontroli pozwalają nie tylko na ograniczanie wielu barier biurokratyczno-organizacyjnych, w tym – dotychczas często występującego w służbach celnych – najbardziej czasochłonnego i kosztownego wymogu niemal 100% granicznej, fizycznej rewizji towarów w handlu międzynarodowym, ale i jej radykalne uproszczenie i skrócenie, przy równoczesnym zwiększeniu jej efektywności. Jej podstawowym zadaniem - do niedawna niemal we wszystkich służbach celnych, a dziś jeszcze w bardzo wielu administracjach celnych krajów rozwijających się – była kontrola prowadzona, przede wszystkim, ze względów fiskalnych.

Nic dziwnego, że w sytuacjach, kiedy dochody budżetowe wielu państw (przede wszystkim rozwijających się) pochodzące z cła i jego pochodnych (opłat wyrównawczych, antydumpingowych, ceł eksportowych, podatków granicznych – obrotowego, od wartości dodanej od towarów – VAT, akcyzowego, ekologicznego, etc.) stanowią nierzadko ok.20% a czasami ok.25% budżetu[10], że kontrola celna poprawności fiskalnej międzynarodowego obrotu była, czy niekiedy nadal jeszcze jest tak rygorystyczna i szczegółowa. A fakt, że w sytuacjach krajów mniej rozwiniętych czy znajdujących się w procesie transformacji, w których infrastruktura gospodarcza, w tym i teleinformatyczna, bądź nie istniały, bądź okazały się na bardzo niskim poziomie, nic dziwnego, że bezpośrednia, graniczna kontrola była najskuteczniejszą, bo po prostu nie było innych możliwości stosowania nowoczesnych metod (poza powtórną kontrolą) i instrumentów możliwych do skutecznego egzekwowania podstawowego obowiązku wobec państwa nałożonego na przedsiębiorcę prowadzącego międzynarodowy obrót towarowy – zapłaty danin, właśnie cła i podatków oraz innych opłat nakładanych na towary przywożone lub

[10] Por.: dane zawarte w materiałach IMF, „Governmental Financial Statistics and World Economic Outlook" oraz „OECD Revenue Statistics" (różne wydania), cyt. za: James T.Walsh: New Customs, [w:] „Finance & Development", A quarterly magazin of the IMF, Washington, March 2006, vol.43, Nr 1, p.3, tab.1

wywożone poza granice państwa, czy unii celnej. Mniej istotną rolę odgrywały inne niż fiskalne funkcje służb celnych. Współcześnie jednak, zwłaszcza po wkroczeniu w erę rozwoju wysokich technik i technologii informacyjnych, komputerów i internetu, powstania międzynarodowych sieci konglomeratów produkcyjno-usługowych, ogromnego wzrostu przepływu towarów i środków transportowych oraz osób, dalsze utrzymywanie i stosowanie tej skutecznej przez tysiące lat metody okazało nie tylko nieskuteczne, ale i nieracjonalne, nieefektywne ekonomicznie i społecznie a w efekcie finalnym i szkodliwe politycznie.

Równocześnie wraz z tymi tradycyjnymi, fiskalnymi zadaniami kontrolnymi, nie tyle pojawiła się ile nasiliła się konieczność rozszerzenia ich o kontrolę międzynarodowego obrotu towarowego prowadzoną przez pryzmat zagrożenia nowymi, negatywnymi zjawiskami, w tym przede wszystkim zagrożenia związanego z działalnością zorganizowanych międzynarodowych grup przestępczych, w tym i terrorystycznych. Zjawisko to, którego najbardziej drastycznymi przykładami w ostatnich latach były akty terrorystyczne w Nowym Jorku, Moskwie, Madrycie i Londynie, stale utrzymuje się. Czy i na ile jest ono wyolbrzymiane w propagandzie inspirowanej przez służby specjalne to inna sprawa.[11]

Mimo negatywnej oceny tej propagandowej ofensywy strachu, zawsze istnieje jakieś realne zagrożenie, zwłaszcza przy uwzględnieniu możliwości użycia broni masowej zagłady, broni nie tylko jądrowej, ale i chemicznej czy biologicznej. Fakt ten jest podstawową przesłanką, zwłaszcza w krajach rozwiniętych, do zmiany a raczej uzupełnienia podstawowej funkcji fiskalnej służb celnych o drugą, dziś wysuwaną w tych krajach na plan pierwszy – kontrolą międzynarodowego obrotu towarowego z punktu widzenia ostatecznego celu wykorzystania towarów, w tym i potencjalnego ich wykorzystania bezpośrednio przez terrorystów bądź też do finansowania działalności terrorystycznej. Ta zaś grozi dziś już nie tylko interesom finansowym państw i społeczeństw , ale wręcz najbardziej podstawowych wartości – samego życia osób i społeczeństw. Stąd też konieczność znalezienia nowych, bardziej

[11] Niezwykle charakterystyczną w tym zakresie jest krytyka „wojny z międzynarodowym terroryzmem" rozpętanej przez USA, jaką dał w połowie stycznia 2009r szef dyplomacji brytyjskiej David Miliband w wywiadzie dla „The Guardian": „Pojęcie to ma dobre strony: uświadamia znaczenie zagrożeń, potrzebę solidarności i konieczność natychmiastowej odpowiedzi, również siłowej, jeżeli jest potrzeba. Ale ostatecznie jest mylący i błędny" Por. także: „Gazeta Wyborcza", 09-01-16, s. 15.

skutecznych niż dotychczasowe, metod kontroli celnej które byłyby w stanie nie tylko zwiększyć efektywność tej kontroli, ale i ułatwić międzynarodowy obrót towarowy. Niezależnie od skali realnego zagrożenia dla międzynarodowego obrotu towarowego, sprawa ta, przede wszystkim pod wpływem służby celnej USA (Customs and Border Protection – CBP) znalazła się w centrum uwagi także służb celnych niemal wszystkich państw współczesnego świata.

2. Globalizacja i wyzwania dla współczesnej kontroli celnej

Postępujący rozwój technik komunikacyjnych i informacyjnych tzw. sektora ICT („Information and Communication Technology"), nowoczesna organizacja obrotu towarowego,międzynarodowego łańcucha dostaw oraz związanej z nim kontroli pozwalają na ograniczanie wielu biurokratycznych barier , w tym – dotychczas często występującego w służbach celnych – najbardziej czasochłonnego i kosztownego wymogu niemal 100 procentowej kontroli granicznej, fizycznej rewizji towarów w handlu międzynarodowym, zapewniając równocześnie maksymalizację skuteczności tej kontroli z równoczesnym skróceniem jej czasu.

Dlatego też w wielu służbach celnych podjęto wysiłki na rzecz zastępowania, tej od tysięcy lat tradycyjnej metody bezwzględnej granicznej kontroli towarów i środków transportowych, innymi, nowoczesnymi takimi, które mają możliwość połączenia skuteczności z ułatwieniami i uproszczeniami odpraw celnych. Wśród nich znalazły się rozwiązania nie tylko techniczno-technologiczne (wykorzystujące ICT czyli e-Customs, tj. elekroniczne celnictwo), ale i organizacyjno-metodologiczne takie, jak np.: kontrola *ex ante* i *ex post* z szerokim stosowaniem analizy ryzyka, czy takie jak kontrola przedwysyłkowa (*pre-departure clearence*) lub kontrola wstępna przed przybyciem dostawy do granicznego przejścia lub portu (tzw. *pre-arrival clearence*).

W procesie tym występuje zjawisko przenoszenia kontroli celnych z granicy kraju docelowego czy granicy unii celnej, do innych miejsc, tym samym powodując odblokowywanie samych przejść granicznych poprzez skracanie czasu oczekiwania na graniczną odprawę towarów i środków transportu. Dzięki temu zwiększa się szybkość obrotu towarowego, jego bezpieczeństwo a w konsekwencji i wzrost konkurencyjności przedsiębiorstw takimi działaniami objętych.

Nie jest to jednak rezultat jednostronnych rozwiązań podejmowanych przez administracje celne, czy szerzej, graniczne służby kontrolne, lecz wynik rozwijającej się współpracy tych służb między sobą, nie tylko w jednym kraju, ale na arenie międzynarodowej oraz rozwój współpracy z partnerami biznesowymi, tak w ramach narodowych, jak i międzynarodowych.

Choćby tylko te wskazane metody pozwalają – w coraz szerszym zakresie – traktować procesy kontroli międzynarodowego obrotu towarowego jako otwieranie, dość ściśle do niedawna zamkniętych i mniej czy bardziej szczelnie strzeżonych, granic państw narodowych.

Metody te, choć wielce kosztowne w początkowej fazie, nie tylko powodują skrócenie, przyspieszenie czasu poświęcanego przez przedsiębiorców na odprawy celno-paszportowe, ale i zwiększają skuteczność kontroli, tym samym zapewniając obydwu stronom – państwu i biznesowi, określone , wymierne korzyści, nie tylko finansowe. Z jednej strony graniczne służby państwowe – celne, paszportowe, fitosanitarne i weterynaryjne mają możliwość dłuższego i spokojnego analizowania danej dostawy pod każdym kątem – fiskalnym, zdrowotnym, techniczno-technologicznym, etc., z drugiej biznes zyskuje coraz szybszą możliwość dysponowania towarem. Proces ten odbywa się jednak kosztem (i to znacznym) przenoszenia, zwiększania społecznej odpowiedzialności za bezpieczeństwo międzynarodowego łańcucha dostaw ze służb granicznych na przedsiębiorców.

Coraz szerszą współpracę biznesu ze służbami granicznymi wymusiło samo życie. Okazało się, że w trakcie rozwoju międzynarodowego obrotu towarowego, dającego ogromne ilości miejsc pracy i przyczyniającego się do utrzymywania wysokich stóp rozwoju ekonomicznego państw biorących w nim udział, twórcy tych tendencji znaleźli się w sytuacji w której narodowe bariery graniczne, przede wszystkim celne – taryfowe i pozataryfowe – stały się ich hamulcami. To musiało ulec zmianie. Nie można było nadal utrzymywać różnego rodzaju dowolności w sposobach prowadzenia kontroli celnych na granicach poszczególnych państw czy też stosować różnych wymogów dokumentacyjnych czy dowolnych procedur celnych oraz sposobów interpretacji polityki i prawa celnego. Problem ten nie był nowym.

Od dawna społeczność międzynarodowa starała się nie tyle likwidować te bariery ile uczynić je przejrzystymi i czytelnymi dla wszystkich uczestników handlu międzynarodowego. Dotyczyło to

zarówno barier taryfowych (pierwsza międzynarodowa organizacja celna, istniejąca do dzisiaj, to Międzynarodowa Unia dla Publikacji Taryf Celnych i jej Biuro Publikacji Taryf Celnych powstały już w 1890 r.[12]), jak i pozataryfowych (powstanie GATT – Układu Ogólnego o Taryfach Celnych i Handlu a następnie WTO czyli Światowej Organizacji Handlu oraz CCC czyli Rady Współpracy Celnej znanej obecnie jako WCO – Światowa Organizacja Celnictwa).[13] Organizacje te zrobiły ogromnie dużo dla ujednolicenia zarówno nomenklatury celnej, jak i klasyfikacji towarów znajdujących się w obrocie międzynarodowym, jak i ujednolicenia procedur celnych oraz obniżenia taryf celnych i ich przejrzystości, dostępności i ujednolicenia stosowania, wreszcie doprowadziły do stopniowego zanikania jednej z najistotniejszych i najstarszych, realizowanej przez tysiące lat przez wszystkie służby celne w świecie – funkcji fiskalnej.

Jednakże funkcja fiskalna, podobnie jak i wszystkie inne podporządkowana była podstawowej funkcji wszystkich służb celnych – funkcji kontrolnej. Można skrótowo określić, że „*celnictwo to kontrola*". Wraz z rozwojem społeczno-ekonomicznym, ochroną interesów narodowych wyrażanych w polityce celnej, rozwijała się i zmieniała kontrola celna – jej zadania i funkcje. Już w drugiej połowie, a zwłaszcza pod koniec XX wieku , wraz z obniżaniem stawek celnych i wzrostem przejrzystości parataryfowych oraz pozataryfowych instrumentów polityki celnej[14] coraz więcej uwagi poświęcano nie tyle funkcji fiskalnej

[12] Por. informacje na stronie domowej: http://www.bitd.org/default.asp

[13] Por. np. P .R. Krugman, M. Obstfeld, *Ekonomia międzynarodowa. Teoria i polityka,* t.1, PWN, Warszawa, 2007, s. 269 i nast.; M. B. Smitienko, (red.), *Mieżdunarodnyje ekonomiczeskije otnoszenija*, Moskwa, INFRA-M, 2008, s.107 i nast.; B. Hoekman, M. M. Kostecki, *Ekonomia światowego systemu handlu-WTO:Zasady i mechanizmy negocjacji*, Wyd. Akademii Ekonomicznej im. O.Langego, Wrocław 2002; J. Kaczurba i E. Kawecka-Wyrzykowska (red.), *Polska w WTO*, IKC HZ, Warszawa 2002; T. Bartoszewicz, *GATT a Międzynarodowa Polityka Handlowa*, PWE, Warszawa 1988.

[14] Por.: R. Molski, *Administracyjnoprawna regulacja obrotu towarowego z zagranicą*, Szczecin, Uniwersytet Szczeciński, „Rozprawy i Studia" T. (CDLII) 378, 2001; A. Drwiło, *Postępowanie ochronne w prawie celnym*, Wyd. Arche, Gdańsk 2003; W. Czyżowicz (red.), *Prawo celne*, Wyd. C. H. Beck, Warszawa 2004; A. Kuś, *Publicznoprawne pozataryfowe i parataryfowe instrumenty reglamentacji obrotu towarowego z zagranicą. Studium teoretyczno-prawne*, Oficyna wyd. Branta, Bydgoszcz-Lublin, 2006. Szeroki przegląd polskiej literatury o problemach celnych przedstawiłem w monografii: W Czyżowicz, *Polskie cło 1997-2003*, WSE, Warszawa 2003.

ile innym ochronnym i promocyjnym, ułatwiającym obrót i uproszczającym dokumentację oraz procedury celne.

Pierwotne i stałe utrzymywanie jako jednej z głównych funkcji fiskalnych (z wyłączeniem sytuacji jaka istniała w państwach o gospodarce centralnie planowanej w której funkcje fiskalne kontroli celnej praktycznie zanikły na rzecz ochrony wartości ideologicznych socjalizmu) powoli było uzupełniane i rozwijane na rzecz innych funkcji gospodarczych i społecznych. Dotyczyło to przede wszystkim ochrony uczciwej konkurencji w międzynarodowym obrocie towarowym, ochrony przed napływem na rynki narodowe lub unii celnych towarów o cechach dumpingowych lub subsydiowanych, przemytu i przywozu towarów podrabianych, ochrony własności intelektualnych czy walki o przetrwanie zagrożonych wyginięciem gatunków flory i fauny (Konwencja CITES) i wielu ,wielu innych.

Całkowicie nowa sytuacja powstała na arenie międzynarodowej, w tym związanej z międzynarodowym obrotem towarowym stosunkowo niedawno, bo na początku XXI wieku po terrorystycznym zamachu na World Trade Center Towers (Wieże Centrum Handlu Światowego) w Nowym Jorku w dniu 11 września 2001 roku. Niezależnie od tego, że w praktyce atak ten został przeprowadzony z terytorium samych Stanów Zjednoczonych z użyciem ich samolotów i innych instrumentów amerykańskich niezbędnych do dokonania tego zamachu, to w rezultacie nastąpiła radykalna zmiana pozycji amerykańskiej służby celnej w całej strukturze administracji państwowej USA. Uległa także zmianie jej pozycja na arenie międzynarodowej. To właśnie celnictwo amerykańskie stało się centralną administracją w ramach powołanego nowego, największego, niemal 200-tysięcznoosobowego, Ministerstwa Bezpieczeństwa Wewnętrznego (Homeland Security Department). To służbie celnej USA (Customs and Border Protection Service – CBP) przekazano całość koordynacji ochrony granic USA. Wrócono tym samym do prawie 120-letniej tradycji tej służby od momentu jej powstania do 1913r, kiedy była w istocie jedyna służba graniczną o niezwykle rozbudowanych funkcjach nie tylko fiskalnych, ale i społecznych.

To właśnie z inicjatywy tej służby zwrócono szczególną uwagę na funkcje pozafiskalne, przede wszystkim ochronne i to w najgłębszym sensie tego słowa – ochrony podstawowych wartości ludzkich – życia i zdrowia tak pojedynczych ludzi, jak i całych społeczeństw przed

zagrożeniem jakie może stwarzać współczesny terroryzm międzynarodowy.

Takie rozłożenie akcentów w międzynarodowym obrocie towarowym i przełożenie ich nie funkcje fiskalne lecz na bezpieczeństwo tego obrotu określanego z angielska jako safety and security international trade (forein trade turnover, supply chain security, etc.) jest nadal dziś w pełni aktualne.

Tak więc bezpieczny, wolny od zagrożeń terrorystycznych, nie tylko ekonomicznych, międzynarodowy obrót towarowy staje się dzisiaj podstawową wytyczną dla polityki i kontroli celnej. Temu też muszą zostać podporządkowane zarówno działania biznesu, jak i administracji celnych.

Nie jest to proces ani łatwy, ani szybki, ani tani. W przekonaniu wielu służb celnych, międzynarodowych organizacji celnych (WCO, UE) i znacznej części biznesu międzynarodowego, przede wszystkim korporacji transnarodowych, jest to jednak konieczne.

Trochę inne stanowisko zajmują przedsiębiorcy z tzw. grupy małych i średnich przedsiębiorstw. Jest ono pochodną, przede wszystkim, ich zdolności finansowych do ponoszenia nowych, niemałych kosztów rozwiązań związanych z bezpieczeństwem, a proponowanych czy wręcz narzucanych przedsiębiorcom funkcjonującym na międzynarodowym rynku towarowym przez służbę celną USA oraz WCO czy UE.

Niezależnie od stanowiska nikt nie ma wątpliwości, że międzynarodowy obrót towarowy musi być związany z zapewnieniem jego maksymalnego bezpieczeństwa przed zagrożeniami dla życia i zdrowia całych społeczeństw i poszczególnych ludzi. Równocześnie proces ten ma się odbywać z zapewnieniem ułatwień i uproszczeń dla tego obrotu wprowadzanych przez administracje celne poszczególnych państw.

Początkowo zadanie to wydawało się niewykonalne, a w najlepszym wypadku bardzo trudne i kosztowne. Dziś ze względu na nowoczesne techniki komunikacyjne i łączności (ICT) oraz nowoczesne metody kontroli ten niemożliwy wcześniej do rozwiązania problem: zwiększenie efektywności kontroli celnej z równoczesnym wprowadzeniem ułatwień i uproszczeń w tej kontroli skutkujących skróceniem czasu poświęcanego na dokonywanie odpraw celnych jest nie tylko potencjalnie możliwe, ale wręcz praktycznie realizowany, choć ze względu na koszty, nadal w bardzo ograniczonym zakresie.

3. Nowy paradygmat polityki celnej w warunkach globalizacji – bezpieczeństwo i ułatwienia międzynarodowego obrotu towarowego

Bez wątpienia atak 11 września 2001r. na WTC w Nowym Jorku, a następnie zamachy terrorystyczne na Bali (12 października 2002 r.), w Moskwie (23 października 2002 r.), Madrycie (11 marca 2004 r.), w Biesłanie (1 września 2004 r.) i Londynie (7 lipca 2005 r.) stały się sygnałami dla wszystkich służb i organizacji kontrolnych w świecie do wzmożenia wysiłków na rzecz zwalczania takiego zagrożenia.[15] Nie ominęło to również administracji celnych. I nie ma tu znaczenia, że w istocie wysiłki te nie zmniejszyły ilości dokonywanych w świecie ataków terrorystycznych.[16]

To właśnie w związku z zagrożeniem terrorystycznym w polityce celnej nastąpiła zmiana paradygmatu. Jeśli przez wieki główny nacisk położony był na fiskalną funkcję i dostarczanie dochodów do budżetu przez administracje celne, to w końcu XX wieku nastąpiła jego zmiana. Podejście służb celnych do kontroli i zadań fiskalnych zostało włączone w szerszą wizję – tworzenia warunków dla rozwoju społeczno-gospodarczego, a więc odejście od bieżącego fiskalizmu na rzecz strategicznych dochodów budżetowych będących pochodną ciągnionych zysków z rozwoju międzynarodowego obrotu towarowego. Wówczas też pojawiła się idea, ale i konieczność gospodarcza, tzw. uproszczeń i ułatwień w dokonywaniu odpraw celnych w międzynarodowych obrotach towarowych.

Wreszcie na początku XXI wieku, właśnie po zamachach terrorystycznych w kilku krajach, także ten paradygmat uległ zmianie. Został zastąpiony nowym paradygmatem – paradygmatem bezpieczeństwa tych obrotów. Natomiast nowym wyzwaniem dla służb celnych stało się zapewnienie równocześnie bezpieczeństwa i ułatwień oraz uproszczeń w międzynarodowych obrotach towarowych.

---

[15] Ewolucję definicji terroryzmu oraz kalendarium poważniejszych zamachów terrorystycznych w ostatnich latach podała „Rzeczpospolita" z 5 kwietnia 2006 r., s. 63.

[16] Zgodnie z danymi kongresu USA ilość ta już w pierwszych kilku latach po zamachach na WCT potroiła się. Por.: „The U.S. count of major world terrorist attacks more than tripled in 2004, a rise that may revive debate on whether the Bush administration is winning the war on terrorism, congressional aides said on Tuesday. The number of "significant" international terrorist attacks rose to about 650 last year from about 175 in 2003, according to congressional aides briefed on the numbers by State Department and intelligence officials".Source: Reuters, 050426, http://www.commondreams.org/headlines05/0426-09.htm.

Niezależnie od istniejącej sytuacji w administracjach celnych wielu państw podjęto szereg inicjatyw i rozwiązań, które mogą pomóc w rozwiązaniu tego trudnego zadania.

4. Globalizacja i inicjatywy w zakresie bezpieczeństwa międzynarodowych obrotów towarowych podjęte przez służbę celną USA (CPB)

Rolę inicjatora tych działań przejęła na siebie służba celna USA (CBP).[17] To ona wystąpiła z inicjatywą nie tylko pierwszych działań w sferze bezpieczeństwa międzynarodowego obrotu towarowego prowadzonego w kontenerach czyli z tzw. inicjatywą CSI – Container Security Iniciative, ale i wielu innych. Także pod naciskiem wymogów CBP międzynarodowe organizacje, w tym WCO oraz UE zaczęły podejmować inicjatywy rozwiązania tego trudnego zadania – ułatwień i uproszczeń w odprawach celnych z jednej strony, z drugiej zaś – zwiększenia efektywności kontroli celnej i zwiększenia bezpieczeństwa międzynarodowych obrotów towarowych.

Podstawowe inicjatywy jakie pojawiły się w tej sferze w służbie celnej USA w początku XXI wieku to przede wszystkim takie jak:

- Inicjatywa Bezpieczeństwa Kontenerowego -Container Security Iniciative (C.S.I.) i zawarta w niej zasada "24 godzin" – „24 hours" Rule,
- Bezpieczeństwo Ułatwień Załadowczych i Portowych – International Ship and Port, – Facility Security (ISPS Code of IMO),Inicjatywa megaportów (Bezpieczeństwa Nuklearnego) – Magaports iniciatives – (Nuclear Security),
- Partnerstwo Handlowo-Celne Przeciwko Terroryzmowi – Customs-Trade Partnership Against Terrorism (C-TPAT),
- Własna Ocena Bezpieczeństwa Importerów – Importer Self – Assessment (I.S.A),

[17] Por. wywiad Nicole Nelson z Szefem (Comissioner) Celnictwa USA (Customs and Border Protecion-CBP) Robertem C. Bonnerem„One Face at the Border – the New Role for US Customs", [w:] Customs World, London, Autumn 2003,s.11-15. Fragmenty niniejszego opracowania, uaktualnione, były prezentowany na konferencji: „Swoboda międzynarodowego obrotu towarowego i jej ograniczenia ze względów na zagrożenie terrorystyczne (w inicjatywach i regulacjach celnych USA)". Referat na konferencję naukową *Otwarcie granic rynku a perspektywa BYĆ i MIEĆ człowieka oraz narodu* KUL, Lublin, 06-02-23.

- Ustawa o Terroryzmie Biologicznym – Bioterrorism Act (BTA) of the FDA (Food and Drug Administration),
- Inicjatywa Rozprzestrzenienia Bezpieczeństwa – Proliferation Security Iniciative (P.S.I.),
- Inicjatywa Bezpieczeństwa w Transporcie Lotniczym – Aviation.

To tylko niektóre z inicjatyw i ustaw przyjętych w USA z inicjatywy CBP.[18] Znacznie szerszą ich gamę przedstawił naukowiec fiński pracujący w szwajcarskim uniwersytecie w Lozannie – Juha Hintsa na marcowej (2006) konferencji w WCO.[19] Przyjrzyjmy się najważniejszym, ze względu na wpływ na międzynarodową współpracę administracji celnych między sobą oraz ich współpracę z kręgami biznesu, wybranym z tych które zostały przyjęte w USA.

Inicjatywa Bezpieczeństwa Kontenerowego - CSI

Pierwszą z inicjatyw (programów i ustaw) związanych bezpieczeństwem międzynarodowego łańcucha dostaw była CSI. Została ogłoszona przez CBP już w styczniu 2002 r. Po kilku latach od jej ogłoszenia już (aż albo zaledwie) 26 narodowych administracji celnych przystąpiło do tej Inicjatywy. Ich stopień zaawansowania w realizacji CSI jest jednak b. zróżnicowany. Co prawda CSI jest implementowana w wielu portach (na początku 2006r. było to 36 zagranicznych portów morskich) na wszystkich kontynentach, to jednak jeszcze daleko jest do osiągnięcia postawionego Inicjatywie Bezpieczeństwa

[18] Cyt. za: Noel Colpin – Dir. Gen. of the Belgian Customs and Excise Administration & Paul Raes – Programme Menager – Presentation ,WCO Session , Brussels 2004-06-25.

[19] Por.: Juha Hintsa: Future Research Agenda for Supply Chain Security, Border Security and Port Security Management. Cross-border Research Association & HEC University of Lausanne, w: WCO Research, Conference Brussels, March 1-3, 2006, slajd zatytułowany: *Trade and cargo security nothing new under the sun, but a jungle…?* Autor wymienia ok. 25 różnych inicjatyw bezpieczeństwa podejmowanych zarówno w USA jak i na świecie. Por. również: Dictionary of International Trade, ed. E.G. Hinkelmann, Novato, California, wyd. World Trade Press, 2005, p.543-621, cyt.za: P.M. Sikorski: Bezpieczeństwo łańcucha dostaw, [w:] „Polska gazeta transportowa", Warszawa, nr 13 z 29 marca 2006, s.10; tegoż:C-TPAT i CSI, tamże, nr 14 z 5 kwietnia 2006, s.8; WCO Framework of Standards. To Secure and Facilitate of Global Trade, [w:] http://www.wcoomd.org/ie/en/en.html, Jan Sobieski, *Światowy Dzień Celnictwa.Czas na standardy*, w: „Wiadomości celne", 2006, nr 2/3, s.10-14. W artykule tym są omówione założenia i podstawowe standardy wspomnianego dokumentu WCO.

Kontenerowego przez CPB osiągnięcia do końca 2006 r. co najmniej 50 portów morskich. Taki stan zaangażowania państw w CSI pozwoliłby na objęcie nią ok. 90% wszystkich dostaw morskich. Do dzisiaj jednak założony cel nie został osiągnięty pomimo zmian w zasadach wyboru tych portów w rezultacie rezygnacji z rezydentów zagranicznych CPB, przerzucenia kosztów i odpowiedzialności za CSI na narodowe służby celne państw i administratorów wybranych portów.[20]

Przesłanką wiodącą przy tworzeniu i przyjmowaniu CSI przez CPB było to, że ogromna ilość towarów importowanych do USA (ponad 80 %) dostarczanych jest do tego kraju kontenerami. Nic więc dziwnego, że można oczekiwać tego, iż w takiej masie towarów dostarczanych kontenerami może znajdować się towar niezgłoszony albo zgłoszony fałszywie, to jest, że może nim być np. broń masowego rażenia, artykuły binarnego przeznaczenia czy inne towary mogące być źródłem pochodzenia środków dla finansowania grup terrorystycznych.

Drugą, nie mniej istotną, ale faktycznie stanowiącą *conditio sine qua non* dla skutecznego zrealizowania tej inicjatywy było funkcjonowanie bezpiecznej sieci elektronicznej – Internetu. Co prawda i przy pomocy innych środków technicznych, np. faksu czy teleksu można byłoby realizować podstawowe założenia CSI jednak byłoby to rozwiązanie znacznie mniej doskonałe a tym samym i mniej bezpieczne, wolniejsze i znacznie droższe.

Sama Inicjatywa zakładała – i do dziś to uległo zmianie – 4 podstawowe cele związane z bezpieczeństwem międzynarodowego łańcucha dostaw kontrolowanego przez administracje celne państw i terytoriów z których kontenery wysyłane są do USA. Miała i ma ona zapewnić:

- Identyfikację kontenerów tzw. wysokiego ryzyka z wykorzystaniem automatycznych metod analitycznych bazujących na wstępnej, przedwysyłkowej informacji (*pre-departure declaration*) oraz danych wywiadu strategicznego;
- Prześwietlenie (przy pomocy dużych skanerów – rentgenów i innych tzw. nie inwazyjnych metod kontroli) oraz ocenę kontenerów przed ich załadunkiem możliwie jak najwcześniej, co ma zapewnić bezpieczeństwo łańcucha dostaw, najczęściej w porcie załadunku;

[20] Spis tych portów na: http://www.worldtraderef.com/WTR_site/csi.asp (08-11-30, godz.15:20).

- Dokonanie prześwietleń kontenerów musi odbywać się przy pomocy skanerów pozwalających na szybkie dokonywanie tego, bez spowalniania obrotów towarowych;
- Wykorzystanie tzw. inteligentnych (smarter) bardziej bezpiecznych kontenerów, które pozwalają oficerom CBP już w portach USA zidentyfikować te z kontenerów, które zostały poddane jakimkolwiek niedozwolonym działaniom podczas operacji tranzytowych.

Załadunki w portach zagranicznych dokonywane były do niedawna w obecności oficerów CBP. Jednakże na wysokie koszty utrzymywania zagranicznych rezydentów CBP ogólna ilość portów była niewielka w których faktycznie pełnili służbę. Stąd też zasada ta została zmieniona na rzecz przekazania, po inspekcji dokonywanej przez oficerów CBP i ich akceptacji, odpowiedzialności za nadzór za załadunek w porcie wysyłki na rzecz narodowej służby celnej. Na zasadzie wzajemności oficerowie administracji celnych współdziałających z CBP mogą być kierowani do USA. Do dzisiaj jedynie administracje celne Kanady i Japonii skorzystały z takiej możliwości. Wiąże się to po prostu z wysokimi kosztami utrzymania zagranicznych placówek celnych.

W CBP włączano do CSI kolejne porty morskie, w tym Szczecin. Od marca 2007 do września 2007 r. realizowany był pilotaż tego programu w morskim porcie w Szczecinie. Tak więc na zasadzie przekazania całkowitej odpowiedzialności na polską administrację celną, bez obecności oficerów CBP, za wysyłkę kontenera do USA nasz port został włączony do CSI.

Sama idea CSI polegała na tym żeby informacja o towarach umieszczonych w kontenerach mających być załadowanymi na środek transportu zmierzający do USA była dostarczona (***obligatoryjnie!!!***) do CBP wcześniej niż załadunek w miejscu odprawy celnej w kraju wysyłki a dokładniej niż załadunek na środek transportu (statek lub samolot) udający się do USA. Co więcej informacja ta musi być dostarczona do CPB elektronicznie co najmniej 24 godz. przed załadunkiem na statek czy samolot. To ***zasada tzw. 24 godz***. („24 hours principle").[21]

Dopiero po analizie uzyskanych w ten sposób danych , CBP przekazuje zwrotnie zgodę – albo nie - na załadunek danego kontenera na statek lub

[21] Szczegóły CSI znajdują się na stronie domowej CBP pod adresem: http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml.

samolot kierowany do USA. Istotnym jest jednak to, że CBP wymuszają na zagranicznych partnerach biznesowych ***obligatoryjne dostarczanie tych danych.***

Partnerstwo biznesu i celnictwa przeciwko terroryzmowi - C-TPAT

To druga z globalnych, wiodących inicjatyw cła amerykańskiego, która tym razem ***oparta na dobrowolnym uczestnictwie firm*** współpracujących ze służbą celną jako agencją rządową, ma na celu zwiększenie bezpieczeństwa międzynarodowego łańcucha dostaw w obrocie towarowym.[22] Zapoczątkowana została w listopadzie 2001 r. z udziałem siedmiu wielkich importerów amerykańskich. W do grudnia 2008 r. ponad 10 tys. firm złożyło wnioski o włączenie ich do tego programu, zaś ponad 5300 otrzymało już status jego uczestnika.[23]

Wśród biznesowych partnerów enumeratywnie wskazano na następujące grupy przedsiębiorców związanych z międzynarodowym obrotem towarowym i łańcuchem dostaw:

- Zarejestrowanych importerów amerykańskich,
- Przewoźników drogowych na granicy z Kanadą,
- Przewoźników drogowych na granicy z Meksykiem,
- Przewoźników kolejowych,
- Przewoźników morskich,
- Przewoźników lotniczych,
- Władze portów amerykańskich portów morskich i operatorów (administratorów) terminali,
- Konsolidatorów frachtów powietrznych, pośredników transportów oceanicznych oraz tzw. nie-okrętowych operatorów wspólnych, przewozów (Non-Vessel Operating Common Carriers – NVOCC)
- Meksykańskich producentów,
- Zaproszonych, wybranych producentów zagranicznych oraz licencjonowanych amerykańskich agentów celnych

Głównym kryterium wyboru tych a nie innych firm jest określenie ich wiarygodności wynikającej z analiza ryzyka. Na liście wybranych do programu C-TPAT mogą się znaleźć tylko takie firmy, które przez CBP

[22]Por.:http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml (08-11-30, godz.15:40).
[23] Cyt. za: http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/.

zostały zaliczone do firm o niskim stopniu zagrożenia dla bezpieczeństwa państwa, które spełniają minimum standardowych kryteriów bezpieczeństwa łańcucha dostaw towarów do USA. Są one opracowane dla chętnych w takich sposób, by zainteresowane firmy mogły elektronicznie (on-line) dokonać zgłoszenia z wypełnieniem wymagań dla partnerów biznesowych, procedur bezpieczeństwa, bezpieczeństwa fizycznego, bezpieczeństwa kadrowego, odpowiedniego szkolenia i doskonalenia zawodowego, wyników kontroli i możliwości jej prowadzenia, procedur zgłaszania dostawy, bezpieczeństwa środków transportowych. Nie są to wymogi małe, mimo określenia ich minimalnymi, ponieważ w każdej ze wskazanych grup jest wiele szczegółowych kryteriów.

Celem C-TPAT jest umożliwienie współpracującym przedsiębiorcom zmniejszenia fizycznych kontroli, a tym samym zapewnienie szybkich odpraw dostaw importowych. Ułatwienie to pozwala także CBP na skupienie uwagi na kontroli pozostałych firm, które niemal automatycznie objęte są założeniem wysokiego ryzyka. Tak więc i w tym przypadku realizowane są dwa cele: zwiększenie bezpieczeństwa i przyspieszenie międzynarodowego obrotu towarowego. Ten ostatni cel to biznesowa wartość sama w sobie i to wartość bardzo mierzalna – „Time is Money" („czas to pieniądz"). W warunkach ostrej konkurencji na rynku amerykańskim to przysłowie ma realną, namacalną, wymierną, finansową treść.

Podstawowym celem tej inicjatywy jest *„...takie budowanie stosunków współpracy, które umocnią i udoskonalą bezpieczeństwo zarówno międzynarodowego łańcucha dostaw jak i granic USA*."[24]

Punktem wyjścia dla tego programu jest uznanie faktu, że CBP może skutecznie zapewnić na najwyższym poziomie bezpieczeństwo obrotu towarowego jedynie w ścisłej współpracy z ostatecznymi właścicielami tych dostaw, takimi jak importerzy, przewoźnicy, spedytorzy, agenci celni i producenci. Zgodnie z deklaracjami rządowymi

„C-TPAT oferuje biznesowi związanemu z międzynarodowym obrotem towarowym możliwość odgrywania aktywnej roli w wojnie przeciwko terroryzmowi. Udział w tym pierwszym na światową skalę programie międzynarodowego łańcucha dostaw zapewnia firmom, jej

[24] Tamże.

pracownikom, dostawcom i klientom większą szybkość i więcej bezpieczeństwa".[25]

Bez wątpienia to atrakcyjne dla biznesu wartości w jego działalności na arenie międzynarodowej. Jednak ze względu na fakt, że ogromnie wiele jest branżowych partnerów, wspomnianych przykładowo w cytowanym wyżej fragmencie założeń tego programu, dlatego też przewidziano dla każdych z nich odpowiednie, zróżnicowane wymogi przystąpienia do tej inicjatywy.

Wraz z tym został opracowany „***Strategiczny plan działania***" w którym szczegółowo określono nie tylko cele, ale i odpowiednie kryteria włączenia danej firmy do tego programu.[26] Wzajemne porozumienia, ze specyficznymi kryteriami dla przystąpienia do tego programu, zostały sformułowane dla przewoźników drogowych, morskich, lotniczych, agentów celnych oraz innych przedsiębiorców biorących udział w międzynarodowym łańcuchu dostaw.

Kryteria te zostały na nowo sformułowane, stały się bardziej precyzyjne i przejrzyste od marca 2006r. To nowe, tzw. minimalne kryteria obejmują, m.in. takie jak: zapewnienie bezpieczeństwa postoju samochodu na parkingu czy terminalu właściciela czy nadawcy, zapewnienie kompetencji i wiarygodności kierowców, etc. tak by zapewnić bezpieczeństwo dostawy od załadunku do dostarczenia towaru do odbiorcy. Podobne kryteria zostały na nowo sformułowane w tymże miesiącu dla pozostałych grup partnerów biznesowych.[27]

Bez wątpienia amerykańskie inicjatywy – programy bezpieczeństwa międzynarodowego łańcucha dostaw wskazują na możliwość rozwiązania dychotomii między skutecznością kontroli celnej i jej szybkością, choć nie zwracają specjalnej uwagi na koszty takiego rozwiązania. A te stają się coraz większe dla biznesu i narodowych administracji celnych, przynajmniej w początkowym okresie tworzenia odpowiednich systemów i programów komputerowych.

Jak widać na przykładzie tylko dwóch inicjatyw – programów zwalczania nie tylko samego terroryzmu międzynarodowego, ale i prewencyjnie zapobiegać zagrożeniu atakami groźnych dla obywateli

---

[25] Tamże.

[26] http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf

[27] http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/

i całych społeczeństw amerykańska służba celna położyła nacisk na bardzo ścisłą i jak najszerszą współpracę programowo-organizacyjną z partnerami biznesowymi, nie tylko własnymi, ale i międzynarodowymi.

Podobne rozwiązania przewidują i pozostałe inicjatywy amerykańskie. Niektóre z nich , tak jak CSI czy C-TPAT, przenoszone są na arenę międzynarodową.

Równocześnie wiele z tych rozwiązań wynika z mniej czy bardziej realnych politycznych obaw przed atakiem terrorystycznym z zewnątrz poszczególnych państw, mimo, że dotychczasowa praktyka pokazała, że wszystkie dotychczasowe były rezultatem sił znajdujących się wewnątrz danych społeczeństw narodowych. Tym nie mniej mimo, że inicjatywy w większym stopniu propagandowym wykorzystując naturalną potrzebę Człowieka i całych narodów do życia bezpiecznego wprowadziły szereg ograniczeń praw obywatelskich (np. USA Patriot Act of October 24, 2001), to ostatecznie doprowadziły do pewnych zmian w międzynarodowym łańcuchu dostaw towarowych.

5. Światowa Organizacja Celnictwa – (World Customs Organization –WCO) i jej podejście do bezpieczeństwa odpraw celnych w warunkach rynku globowego

Naciski USA wymusiły zarówno na administracjach celnych, jak i na partnerach biznesowych zmiany w podejściu do wzajemnej współpracy. Odnosi się to przede wszystkim do specjalnego projektu Światowej Organizacji Celnictwa, tzw. Ramowych Standardów Bezpieczeństwa i Ułatwień dla Międzynarodowego Łańcucha Dostaw (*WCO SAFE Framework of Standards to Secure and Facilitate Global trade* – dalej określanych jako "***SAFE Framework***").[28]

[28]Por. tekst tego dokumentu na: http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/SAFE%20Framework_EN_2007_for_publication.pdf , wg stanu z : 081017.godz.9:43 Dokument ten jest dostępny także w wielu innych językach w postaci broszury, także w j. rosyjskim. Por. też szereg analiz i informacji w specjalistycznej prasie poświęconej celnictwu i procedurom celnym, takich jak, np.: „The international Customs Community Wants to be Safe" [w:] Customs Today.Startegic Perspectives on Trade, Security and Canadian Business, Ottawa, May 2007, s.5 czy art. M.Giffoni: Programma SAFE, [w:] Il Doganalista, Roma, 2008, no 4 Luglio-Agosto 2008, s.15 i nast. czy R.Mc Donagh: Customs In the 21st Century, [w:]Rechtsfragen des Zolls in globalen Markten, Schriften zum Aussenwirtschaftsrecht, Heraugegeben von Dirk Ehlers Und Hans-Michael Wolffgang, Frankfurt AM Main, 2005, s.7-11, czy D. Tweddle: Logistics, Security

Ramowe Standardy Bezpieczeństwa i Ułatwień dla Międzynarodowego Łańcucha Dostaw (SAFE Framework) Światowej Organizacji Celnictwa (WCO)

Cele i zasady jakie zostały sformułowane w programie SAFE Framework WCO to :

- ustanowienie standardów które zapewnią ułatwienia bezpieczeństwo międzynarodowego łańcucha dostaw na poziomie globowym, ich przewidywalność i pewność;
- umożliwienie zintegrowania zarządzania łańcuchem dostaw dla wszystkich rodzajów transportu;
- podwyższenie rolę celnictwa, jego funkcji i zdolności sprostania wyzwaniom i możliwościom XXI wieku;
- umocnienie współpracy pomiędzy administracjami celnymi w doskonaleniu wykrywania dostaw wysokiego ryzyka;
- wzmocnienie współpracy celnictwa ze środowiskiem biznesu;
- promowanie płynności obrotu towarowego w ramach bezpiecznego międzynarodowego łańcucha dostaw.

Powyższe cele znalazły szczegółowe opisanie w czterech zasadniczych (core) elementach SAFE Framework.

Pierwszy z nich odnosi się do harmonizacji wymogów związanych z wykorzystywaniem zaawansowanej informacji elektronicznej o odprawianej, wyładowywanej i transportowanej dostawie towarowej.

Drugi wiąże się z koniecznością stosowania przez państwa sygnatariuszy SAFE Framework metody analizy ryzyka uwzględniającej zagrożenia dla wymogów bezpieczeństwa.

Trzeci to wymóg powiadamiania kraju odbiorcy, na bazie porównywalnej metodologii profilowania ryzyka przez administrację celną kraju wysyłki i kraju przeznaczenia, a opartej na dokonywaniu kontroli towarów i kontenerów wysokiego ryzyka związanej z wykorzystaniem, przede wszystkim, nieinwazyjnych detektorów takich jak duże skanery rentgenowskie czy podobne aparaty.

I **czwarty** element, to zdefiniowanie korzyści jakie służby celne przedłożą tym przedsiębiorcom, którzy spełnią minimalne wymogi dla

---

and Compliance: The Part To Be Played by Authorised Economic Operators (AEOs) and Data Management, [w:] World Customs Journal, Canberra, INCU, 2008 April,Vol.2, no 1, s. 101-105.

standardów bezpieczeństwa łańcucha dostaw oraz najlepszych praktyk (best practices).[29]

Przedstawiony powyżej zestaw czterech elementów standardów bezpieczeństwa wiąże się faktycznie z dwoma wzajemnie połączonymi między sobą funkcjonalną współpracą filarami – filarem celniczym i biznesowym (celnictwo jednego kraju z celnictwem innego kraju „C2C" a raczej zgodnie z tradycją akronimów „G2G" lub „A2A" oraz partnerstwo przedsiębiorcy (biznesu) z celnictwem (business – customs partnership „B2C" lub tradycyjnie „B2G").

Strategia międzynarodowego łańcucha dostaw bazująca na tych dwóch filarach ma, zgodnie z założeniami omawianego dokumentu, wiele zalet dla obydwu stron tego procesu. Przede wszystkim tworzy partnerstwo i wzajemne zaufanie między biznesem i celnictwem już choćby przez sam fakt jawnego, jasnego, precyzyjnego i zrozumiałego sformułowania wymogów kontrolnych związanych z realizacją zasad bezpieczeństwa w międzynarodowym łańcuchu dostaw towarowych. Co więcej, w przekonaniu twórców dokumentu, ten zestaw jednolitych na arenie międzynarodowej wymogów jest stosunkowo łatwym do wprowadzenia w życie przez wszystkich zainteresowanych, mimo, że w istocie bezpośrednie środki i programy komputerowe będą narodowo (narodowe programy komputerowe, softwares) dostępnymi w państwach sygnatariuszach tego dokumentu.

W SAFE Framework, podobnie jak i w innych tego typu dokumentach, znaczną część zajmuje ideologiczno-polityczne ich podbudowanie poprzez wskazanie interesu przedsiębiorstw które przyjmą te projekty. Kładzie się w nim nacisk właśnie nie tylko na bezpieczeństwo, ale i na korzyści. Wymienia się tu przede wszystkim, że wreszcie na arenie międzynarodowej powstała nowa, skonsolidowana platforma która pozwala na to, że można udoskonalić międzynarodowy obrót towarowy, lepiej zapewnić bezpieczeństwo przed terroryzmem, zwiększyć wkład celnictwa i partnerów handlowych do gospodarczego i społecznego dobrobytu narodów. Równocześnie zrealizowanie założeń WCO SAFE Framework sprzyjać ma udoskonaleniu zdolności celnictwa do wykrywania i zarządzania dostawami o wysokim ryzyku dla bezpieczeństwa, powiększeniu efektywności i przyspieszeniu odpraw towarów. Tak więc realizacja przewidzianych reguł ma przynieść

[29] Tamże.

korzyści wszystkim zainteresowanym – biznesowi, celnictwu, rządom i narodom.[30]

Zgodnie z intencją WCO omawiany dokument miał stworzyć i formalnie stworzył, m.in., przesłanki – kryteria i wymogi dla nie tylko bezpieczeństwa międzynarodowego łańcucha dostaw towarowych, ale i dla ułatwień dla tego obrotu oraz promocji międzynarodowego handlu towarami. Tym samym miał wesprzeć i ułatwić kupującym i sprzedającym obrót towarowy między państwami. To także odnosić się ma sfery produkcji i dystrybucji. Dzięki przyjęciu instytucji tzw. upoważnionego przedsiębiorcy (Authorized Economic Operator-AEO) certyfikowane firmy mają osiągać dodatkowe korzyści, takie jak np. szybsze postępowanie kontrolne czy zmniejszenie ilości kontroli, co ma się przełożyć na ich czas a tym samym i koszty funkcjonowania przedsiębiorstwa.[31]

Jednym z podstawowych założeń ***SAFE Framework*** jest stworzenie pakietu międzynarodowych jednolitych i przewidywalnych standardowych wymogów minimalnych dla wypełnienia potrzeb bezpieczeństwa, a także ograniczenie informacji sprawozdawczych łańcucha dostaw towarowych. Powinno to zapewnić AEO korzyści z dokonanych inwestycji wynikających z wymogów techniczno-organizacyjnych i kadrowych.

6. Upoważniony przedsiębiorca (AEO) w Unii Europejskiej

Problem AEO pozostawiony jednak został w gestii narodowej i to narodowa administracja celna, zgodnie z prawem celnym, określa warunki uzyskania odpowiedniego certyfikatu. W tej chwili sygnatariuszami tego dokumentu, jako dobrowolnego zobowiązania, jest 154 państw, regionów i ugrupowań. W samej Unii Europejskiej sprawa zapobiegania groźbie i zwalczania terroryzmowi wywołały szereg działań opartych na różnych przedsięwzięciach.[32] Wśród nich państwa członkowskie UE i UE jako organizacja międzynarodowa.[33]

---

[30] Tamże.

[31] Por.: *One More International Trade Acronym – what is an AEO?*, [w:] "Customs Today. Strategic Perspectives", *op.cit*., s.4

[32] Por. ciekawy art.: K. Jałoszyński- *Unia wobec zagrożenia terroryzmem*, [w:] „Monitor Unii Europejskiej", Warszawa, 2008, nr 7/8(49/50), s. 104 i nast.

[33] Cyt. za: http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Enforcement/

W przypadku Polski zagadnienie to nie jest jednak wyłączną kompetencją naszej służby celnej lecz jest związane z wyłączną kompetencją organów UE – Parlamentu i Rady oraz Komisji. To co w dokumencie WCO zostało podkreślone to, poza ideologicznymi wartościami (bezpieczeństwo, ułatwienia, dobrobyt, przyspieszenie obrotu, etc.) to wskazanie na fakt, że status AEO może uzyskać każdy przedsiębiorca, który wypełni odpowiednie kryteria. Może nim być zarówno producent, jak i dystrybutor towaru czy pośrednik, przewoźnik, spedytor, agent celny, port, skład , w tym i skład celny, etc.

I tu dochodzimy do tego o czym mówi stare przysłowie, że „diabeł tkwi w szczegółach". A te zostały określone w UE w Rozporządzeniu 648 z 13 kwietnia 2005r.[34] a więc akcie powszechnie obowiązującym, bezpośrednio skutecznym i egzekwowalnym. Jego podstawowe elementy znalazły się zarówno w poprzednim Wspólnotowym Kodeksie Celnym z 1992 po uzupełnieniu go o art. 5a („Upoważnione Podmioty Gospodarcze) jak we Wspólnotowym Kodeksie Celnym (zmodernizowanym) z 2008 r. (art.13-15).[35]

Niezależnie od faktu, że zarówno UE jak i WCO przyjęły odpowiednie akty już w 2005 r., to w UE dopiero z dniem 1 stycznia 2008 r. weszły w życie przepisy wykonawcze umożliwiające funkcjonowanie instytucji upoważnionego przedsiębiorcy (AEO). Z tą datą przedsiębiorcy zainteresowani uzyskaniem statusu AEO mogli zacząć składać do organów celnych wnioski o wydanie świadectwa AEO, a po jego uzyskaniu korzystać z ułatwień odnoszących się do kontroli celnej dotyczącej bezpieczeństwa i ochrony i/lub z uproszczeń przewidzianych w ramach przepisów celnych.[36] Należy jednak zwrócić uwagę na fakt, że zarówno wg SAFE Framework jak i aktów prawnych

---

WCO%20TABLE%20Intention%20to%20implement%20the%20FOS-%20EN-FR_June08V2.pdf z :081017, godz.10:55

[34] Rozporządzenie (WE) nr 648/2005 Parlamentu Europejskiego i Rady z dnia 13 kwietnia 2005 r. zmieniające rozporządzenie Rady (EWG) nr 2913/92 ustanawiające Wspólnotowy Kodeks Celny (Dz. Urz. UE L 117 z 4.05.2005, s. 13)-na: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005R0648:PL:HTML;081017,godz.11:21

[35] Tekst nowego Wspólnotowego Kodeksu Celnego, Rozp.450/2008: http://www.mf.gov.pl/_files_/sluzba_celna/akty_prawne/przepisy_celne/wspolnotowe/pc_lexuriserv-pl.pdf

[36] Szerzej na temat AEO piszą: M. Laszuk, M. Masłowska, *Wady i zalety instytucji upoważnionego przedsiębiorcy,*[w:] Zeszyty Naukowe Wyższej Szkoły Administracji Publicznej „Administracja Publiczna. Studia Krajowe", Białystok, Nr 2/2008

UE dotyczących AEO status ten może być uzyskiwany (podobnie jak ma to miejsce w przypadku C-TPAT w USA) na ***DOBROWOLNEJ ZASADZIE czyli nie jest to obowiązek a prawo i możliwość uzyskania takiego statusu.***

7. Podstawa prawna

Instytucja upoważnionego przedsiębiorcy (AEO) została wprowadzona do porządku prawnego Unii Europejskiej rozporządzeniem (WE) nr 648/2005 (dalej jako Rozp. 648) Parlamentu Europejskiego i Rady z dnia 13 kwietnia 2005 r. zmieniającym rozporządzenie Rady (EWG) nr 2913/92 ustanawiające Wspólnotowy Kodeks Celny (Dz. Urz. UE L117 z 4.05.2005, s. 13), z tym, że jej zastosowanie uzależnione było od opracowania i przyjęcia przepisów wykonawczych. Stało się to możliwe z dniem 1 stycznia 2008r., kiedy to weszły w życie przepisy rozporządzenia Komisji (WE) nr 1875/2006 z dnia 18 grudnia 2006 r. zmieniającego rozporządzenie (EWG) nr 2454/93 ustanawiające przepisy w celu wykonania Wspólnotowego Kodeksu Celnego (Dz. Urz. WE L 360 z 19.12.2006 str. 64).[37]

Rozporządzenie Wykonawcze reguluje procedurę przyznawania statusu AEO oraz określa wymogi i kryteria, jakie powinien spełniać przedsiębiorca ubiegający się o uzyskanie tego statusu, wskazuje na korzyści wynikające z posiadania świadectwa AEO oraz obowiązki przedsiębiorcy i organów celnych.

Przyjęte rozwiązania w Rozporządzeniu 648 o AEO częściowo zostały włączone do Zmodernizowanego Wspólnotowego Kodeksu Celnego (ZWKC). Upoważnionemu przedsiębiorcy poświęcony jest Sekcja 3 i tak też zatytułowana „U p o w a ż n i o n y p r z e d s i ę b i o r c a" (art.13-15).

8. Definicja i warunki uzyskania świadectwa AEO

[37] Por. tekst: Rozporządzenie Komisji (WE) nr 1875/2006 z dnia 18 grudnia 2006r. zmieniającego rozporządzenie (EWG) nr 2454/93 ustanawiające przepisy w celu wykonania Wspólnotowego Kodeksu Celnego (Dz. Urz. WE L 360 z 19.12.2006 str. 64): http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:360:0064:01:PL:HTML z 081017,godz.11:43.

Punktem wyjścia dla zrozumienia formalnoprawnego statusu AEO jest enumeratywne wymienienie instytucjonalnych dowodów takiego statusu czyli posiadanie odpowiedniego świadectwa (certyfikatu)[38] .

Zgodnie ze ZWKC o status AEO może ubiegać się każdy przedsiębiorca z UE. Wg art.13 tego aktu prawnego *„1.Przedsiębiorca mający siedzibę na obszarze celnym Wspólnoty i spełniający warunki określone w art. 14 i 15 może wystąpić o przyznanie statusu upoważnionego przedsiębiorcy.*
1. Status ten przyznawany jest przez organy celne — w stosownych przypadkach po przeprowadzeniu konsultacji z innymi właściwymi organami — i podlega nadzorowi.
2. Status upoważnionego przedsiębiorcy obejmuje dwa rodzaje upoważnienia: przedsiębiorcy upoważnionego do korzystania z uproszczeń celnych i przedsiębiorcy upoważnionego do korzystania z ułatwień w zakresie bezpieczeństwa i ochrony.

Pierwszy rodzaj upoważnienia umożliwia przedsiębiorcom korzystanie z niektórych uproszczeń zgodnie z przepisami prawa celnego. Na mocy upoważnienia drugiego rodzaju jego posiadacz ma prawo do korzystania z ułatwień w zakresie bezpieczeństwa i ochrony. Można korzystać z obydwu rodzajów upoważnienia jednocześnie."

Choć mamy tu określenie tego KTO może WYSTĄPIĆ (aplikować) o status AEO, to nie definiuje się odpowiedzi wprost na pytanie KIM JEST podmiot posiadający taki status. To bardziej precyzyjnie zostało sformułowane w Rozp.648. I tak w art.14a tego właśnie rozporządzenia stwierdza się, ***że upoważnionym przedsiębiorcą jest ten przedsiębiorca***, który posiada przynajmniej jedno z poniżej wymienionych dokumentów:

- świadectwo AEO – uproszczenia celne,
- świadectwo AEO – bezpieczeństwo i ochrona,
- świadectwo AEO – uproszczenia celne/bezpieczeństwo i ochrona.

„***Świadectwo AEO – uproszczenia celne***" przeznaczone dla przedsiębiorców wnioskujących o korzystanie z uproszczeń celnych przewidzianych w przepisach prawa celnego,
„***Świadectwo AEO – bezpieczeństwo i ochrona***" przeznaczone dla przedsiębiorców chcących korzystać z ułatwień w kontroli celnej

[38] Por. także: Informacja o AEO na stronie domowej polskiej Służby Celnej: http://www.mf.gov.pl/index.php?const=2&dzial=764&wysw=4&sub=sub13

w zakresie bezpieczeństwa i ochrony towarów przy przywozie na obszar celny Wspólnoty Europejskiej lub przy wywozie z obszaru celnego Wspólnoty Europejskiej,
„***Świadectwo AEO – uproszczenia celne/bezpieczeństwo i ochrona***" przeznaczone dla przedsiębiorców chcących korzystać z uproszczeń przewidzianych przepisami celnymi oraz udogodnień w zakresie bezpieczeństwa i ochrony towarów."

Powyższe certyfikaty dają przedsiębiorcom szereg uprawnień. Świadectwo AEO – ***uproszczenia celne*** dają przedsiębiorcy możliwość łatwiejszego dostępu do uproszczeń celnych wyszczególnionych w artykule 14b ust. 1 Reg. 648 czyli mniejszej liczby kontroli fizycznych i kontroli dokumentów, priorytetowego traktowania w przypadku wytypowania do kontroli oraz możliwość składania wniosku o określone miejsce przeprowadzenia takiej kontroli.

Status AEO może zostać udzielony każdemu przedsiębiorcy posiadającemu siedzibę na obszarze celnym Wspólnoty (wyjątki określają przepisy Rozporządzenia Wykonawczego) spełniającemu warunki i kryteria, o których mowa w art. 5a ust. 2 Wspólnotowego Kodeksu Celnego[39]. Są to:

- odpowiednie przestrzeganie wymogów celnych,
- odpowiedni system zarządzania ewidencjami handlowymi i, gdzie zachodzi taka potrzeba, ewidencjami transportowymi, który umożliwia właściwą kontrolę celną,
- udokumentowana wypłacalność,
- tam, gdzie ma zastosowanie, odpowiednie standardy bezpieczeństwa i ochrony.

Powyższe warunki i kryteria, badane są przez organy celne w toku procedury o wydanie świadectwa AEO, zostały szczegółowo rozpisane w art. 14h – art. 14k Rozporządzenia 648.

Te pozornie niewinnie brzmiące sformułowania są, niestety, dla praktycznej realizacji przez przedsiębiorcę niezwykle skomplikowane i kosztowne. Mimo, że polska Służba Celna uczyniła ogromnie wiele, co

[39] Po wejściu w życie ZWKC artykuły określające warunki i kryteria zawarte we wskazanych już wcześniej artykułach znalazły się w nowym kodeksie w art.13-15. Por. tekst ZWKC oraz załącznika do ZWKC „Tabela zbieżności" w Dz. U. UE nr 145 z 2008 r., a także jego przedruk [w:] Monitor Prawa Celnego i Podatkowego, Szczecin, Wyd. BW, nr 9 (158)/2008, rok XII, wrzesień 2008.

warto podkreślić jako bardzo istotny wyraz nowych wzajemnych stosunków tych partnerów, dla konsultacji i ich spopularyzowania w kręgach biznesowych, to w istocie niewiele przyniosło to efektów w praktycznej realizacji szczytnych założeń zarówno SAFE Framework, jak i Rozp.648.[40]

Wśród promowanych **korzyści dla przedsiębiorców**, jakie idea instytucji AEO zakłada zarówno w przyjętym dokumencie WCO, jak i w dokumentach UE czy też praktycznej ich adaptacji w Polsce podkreśla się szereg rozwiązań, jakie mają zachęcać przedsiębiorców do występowania do organów celnych o uzyskiwanie tego statusu.

Zgodnie z Rozporządzeniem 648, ZWKC jak i promocją zawartą w innych dokumentach oraz materiałach propagandowo-szkoleniowych wskazuje się na to, że ***status AEO przyznany w jednym państwie członkowskim Unii Europejskiej jest uznawany przez wszystkie służby celne UE.*** A co to w praktyce oznacza? Dla kogo, którego przedsiębiorcy jest to istotne? Jeśli w ogóle ma to jakiekolwiek praktyczne znaczenie to jedynie w sytuacji, kiedy przedsiębiorca dokonuje odpraw celnych w innym państwie członkowskim niż w tym w którym prowadzi swoją działalność. Choć zdarza się to coraz częściej, to jednak do czasu dopóki w całej UE nie będzie funkcjonować elektroniczna platforma dostępu do poszczególnych urzędów celnych czy miejsc odpraw niezależnie od miejsca znajdowania się towaru celnego w UE czyli Single European Authorization-SEA (pojedyncze pozwolenie europejskie) oraz dopóki nie będzie w pełni skomputeryzowanych europejskich baz danych przedsiębiorców, to w istocie wspominana korzyść może – ewentualnie - odnosić się jedynie do firm ekspresowych typu FEDEX, DHL, UPS czy MAERSK. I one też są najczęstszymi aplikantami o ten status i najczęściej go otrzymują.

[40] Warto podkreślić rzeczywiście nowe podejście PSC do stosunku z biznesem w tej kwestii. Już wiosna 2007 r. (w marcu i maju) odbyły się dwa specjalne warsztaty i szkolenia-konsultacje zorganizowane w Centralnym Ośrodku Doskonalenia Funkcjonariuszy Celnych w Świdrze dla przedsiębiorców. Przedstawione zostały na nich podstawowe założenia oraz etapy wdrażania AEO w Polsce. Przedsiębiorcy bardzo aktywnie włączyli się do opracowania kryteriów oceny warunków niezbędnych dla uzyskania statusu AEO wskazując jednocześnie na fakt niezwykłej złożoności i rygoryzmu w ocenie i egzekwowaniu tych kryteriów przy realnie niewielkich, a w istocie żadnych korzyściach – w stosunku do już funkcjonujących w unijnym i polskim prawie celnym preferencjach celnych w stosowaniu procedur celnych, w tym i uproszczeń w dokonywaniu zgłoszeń. Por. informacje na stronie domowej PSC: http://www.mofnet.gov.pl/index.php?const=2&dzial=771&wysw=4&sub=sub13

Status AEO uprawnia do korzystania z ułatwień odnoszących się do kontroli celnej dotyczącej bezpieczeństwa i ochrony i/lub z uproszczeń przewidzianych w ramach przepisów celnych.

Z punktu widzenia przedsiębiorcy te właśnie udogodnienia są najistotniejszymi w ich działalności na międzynarodowym rynku towarowym. Jednym z najbardziej istotnych elementów zarządzania przedsiębiorstwem jest zarządzanie czasem. Stąd też i w wielu firmach realizowana jest metoda zarządzania znana jako „Just In Time" („Na czas"). Najprościej mówiąc polega ona na dostarczaniu do odbiorcy towarów niezbędnych do prowadzenia działalności w tym momencie, kiedy dany towar jest potrzebny. Dzięki takiej organizacji pracy zmniejsza się koszty działalności o koszty utrzymywania magazynów czy składów. W przypadku międzynarodowych obrotów towarowych, które wiążą się z koniecznością dokonywania zgłoszeń i odpraw celnych, to dodatkowy czas wydłużający okres oczekiwania dostawę. A w tym przypadku to wręcz namacalny przykład przysłowia, że „czas to pieniądz". Stąd też takie ułatwienia jakie są propagowane w idei AEO i wspomnianych regulacjach są, przynajmniej na pierwszy rzut oka, najbardziej atrakcyjnymi i pożądanymi przez przedsiębiorców.

I tak w przypadku posiadanie świadectwa ***AEO – uproszczenia celne*** daje przedsiębiorcy możliwość łatwiejszego dostępu do uproszczeń celnych wyszczególnionych w artykule 14b ust. 1 Rozp.648 czyli mniejszej liczby kontroli fizycznych i kontroli dokumentów, priorytetowego traktowania w przypadku wytypowania do kontroli oraz możliwość składania wniosku o określone miejsce przeprowadzenia takiej kontroli.

W przypadku posiadania certyfikatu „***AEO bezpieczeństwo i ochrona***" przedsiębiorca może korzystać z następujących ułatwień:

- podlega mniejszej niż inni przedsiębiorcy liczbie kontroli fizycznej i kontroli dokumentów,
- w przypadku wytypowania go do kontroli przeprowadzana jest ona w sposób priorytetowy,
- uprawnienia do wcześniejszego powiadomienia o wytypowaniu przesyłki do kontroli,
- uprawnienia do składania przywozowej deklaracji skróconej z ograniczonym zakresem danych bezpieczeństwa,

- możliwości wnioskowania o przeprowadzenie kontroli w innym miejscu niż urząd celny.

Na dodatek w przypadku złożenia przez AEO wniosku o stosowanie uproszczeń enumeratywnie wymienionych w art. 14b ust. 1 Reg. 648 organy celne nie badają ponownie tych warunków, które już były badane przy przyznawaniu świadectwa AEO.

Trzeci rodzaj świadectwa „***AEO – uproszczenia celne/bezpieczeństwo i ochrona***" daje uprawnienie do wszelkich korzyści wymienionych powyżej. Jednak musimy mieć na uwadze to, że certyfikat upoważnionego przedsiębiorcy nie ma wpływu na ***korzystanie z uproszczonej procedury.***[41]

To wszystko wygląda niezwykle atrakcyjnie, ale by uzyskać którykolwiek z wymienionych certyfikatów niezbędnym jest spełnienie wymogów przewidzianych zarówno w unijnych aktach prawnych (ZWKC, Rozp. 648, inne przepisy wykonawcze), jak i w polskich dokumentach przygotowanych przez Ministerstwo Finansów i Służbę Celną w postaci „*Wytycznych w sprawie sposobów badania i oceny spełniania wymogów i kryteriów w postępowaniu w sprawie przyznania statusu upoważnionego przedsiębiorcy – AEO wersja 10 z dnia 21.04.2008r.”*****, oraz w „***Kwestionariuszu samooceny AEO***" i w „***Deklaracji Bezpieczeństwa***".**

Na ile jest to skomplikowana, a w sumie trudna do praktycznej realizacji przez ogromną większość przedsiębiorców związanych z odpowiedzialnym zarządzaniem firmą, procedura, wystarczy popatrzeć na ten ostatni dokument „Deklarację Bezpieczeństwa". W pozostałych nakłada się dodatkowo jeszcze czasochłonność i kosztowność przygotowania aplikacji.

Dokument ten, „Deklaracja Bezpieczeństwa" wynika z Rozp. 648 (art. 14k ust.1e). Nakłada on na wnioskodawcę ubiegającego się o status AEO obowiązek wdrożenia środków umożliwiających jednoznaczną

[41] W związku z tym, że pojawiło się szereg wątpliwości, jakie odnosiły się do stosowania tzw. uproszczonych procedur zgłoszenia celnego MF wyjaśniło, że posiadanie certyfikatu AEO nie likwiduje dotychczasowych pozwoleń na stosowanie tych form uproszczonego zgłoszenia jakie są stosowane. Jednak zgodnie z propozycją TAXUD czyli Dyrekcja Generalna ds. Unii Celnej i Podatków Pośrednich w Komisji UE zmierza do stworzenia niemal identycznych jak dla AEO kryteriów dla wydawania pozwoleń dla stosowania uproszczeń, w tym i dla tzw. procedury w miejscu („wpis do rejestru"). Por.: http://www.mf.gov.pl/_files_/sluzba_celna/aeo/aeo_wyjasn.pdf .

identyfikację jego zagranicznych partnerów handlowych w celu zabezpieczenia międzynarodowego łańcucha dostaw. Powyższe stanowi element realizacji kryterium posiadania odpowiednich standardów bezpieczeństwa i ochrony koniecznych do uzyskania Świadectwa AEO „bezpieczeństwo i ochrona" lub Świadectwa mieszanego tj. AEO – „uproszczenia celne bezpieczeństwo i ochrona".

Zgodnie z dokumentem opracowanym przez Komisję Europejską i państwa członkowskie nr TAXUD/2006/1450 z dnia 29 czerwca 2007 r. „***Upoważnieni Przedsiębiorcy – Wytyczne***" „*…upoważnieni przedsiębiorcy mogą odpowiadać wyłącznie za swoją część łańcucha dostaw, towary znajdujące się pod ich pieczą oraz ułatwienia, które stosują. Jednakże są także uzależnieni od standardów bezpieczeństwa stosowanych przez partnerów handlowych w celu zapewnienia bezpieczeństwa towarów znajdujących się pod ich pieczą. W celu spełnienia tego wymogu przy wchodzeniu w nowe stosunki umowne z partnerem handlowym upoważnieni przedsiębiorcy powinni zachęcać drugą stronę umowy do oceny i poprawy bezpieczeństwa ich łańcucha dostaw oraz, w zakresie odpowiednim dla ich modelu biznesowego, do uwzględnienia takich sformułowań w ustaleniach umownych.*"[42]

Proponowane przez Komisję Europejską rozwiązanie polegające na stosowaniu „Deklaracji Bezpieczeństwa dla Upoważnionego Przedsiębiorcy AEO" może być wykorzystywane przez przedsiębiorców w celu realizacji i udowodnienia spełnienia wymagań do uzyskania statusu AEO. Jest to jedna z możliwości jakie powinni spełnić aplikanci. Jednak przedsiębiorcy z certyfikatami AEO ***nie są zobowiązani*** do wymagania od swoich partnerów handlowych, by również posiadali status AEO. A to jeden z najprostszych i w sumie jeden z najłatwiej weryfikowalnych kryteriów dla dużych przedsiębiorstw. Znacznie bardziej skomplikowane i trudniejsze, bardziej czasochłonne i tym samym znacznie kosztowniejsze jest zrealizowanie pozostałych

[42] Por. informacja ze str. Domowej PSC: http://www.mf.gov.pl/index.php?const=2&dzial=771&wysw=4&sub=sub13 , 08-10-19, godz.13:44.

kryteriów. I odnosi się to w istocie do wszystkich trzech rodzajów certyfikatów AEO.[43]

Pozornie prostym jest (dla wszystkich rodzajów świadectw AEO) spełnienie takiego wymogu-kryterium jak ***przestrzeganie wymogów celnych***. Warunek ten uznany będzie za spełniony, jeżeli *w* ***ciągu ostatnich trzech lat*** poprzedzających złożenie wniosku ***nie doszło do poważnego naruszenia przepisów*** lub do powtarzających się naruszeń przepisów prawa celnego przez osoby kierujące przedsiębiorstwem wnioskodawcy lub nadzorujące takie przedsiębiorstwo, przez przedstawiciela prawnego reprezentującego wnioskodawcę w sprawach celnych albo przez osobę odpowiedzialną w przedsiębiorstwie wnioskodawcy za sprawy celne. Pojawia się, trudne do jednoznacznego sprecyzowania na gruncie poszczególnych państw, pytanie o to czym jest „***poważne naruszenie przepisów celnych***" lub „***powtarzających się naruszeń***"? Życie pokazuje, że w praktyce dla służby celnej w istocie KAŻDE naruszenie, nawet najdrobniejsze, prawa celnego skutkuje zaliczeniem go do „poważnego" naruszenia i odmową uzyskania jakichkolwiek ułatwień i uproszczeń w procedurach zgłoszenia celnego. To kwestia , która w trakcie wspomnianych warsztatów wzbudzała ogromne , rozbieżne , interpretacje z jednej strony przez celników z drugiej przez przedstawicieli biznesu.

Kolejnym, wydawałoby się jasnym i oczywistym wymogiem jest to, że przedsiębiorca aplikujący o status AEO dowolnego typu powinien również posiadać ***odpowiedni system zarządzania ewidencjami handlowymi oraz w przypadku, gdy jest to potrzebne, ewidencjami transportowymi***, który umożliwia właściwą kontrolę celną. Wymóg ten znów tylko pozornie oznacza to, że system ten powinien być zgodny z ogólnymi zasadami rachunkowości prowadzonymi przez państwo

[43] Por.: „Wytyczne w sprawie sposobów badania i oceny spełniania wymogów i kryteriów w postępowaniu w sprawie przyznania statusu upoważnionego przedsiębiorcy – AEO (Wytyczne AEO)",
na: http://www.mf.gov.pl/index.php?const=2&dzial=771&wysw=4&sub=sub13. Choć jest to materiał dobrze przygotowany, także w oparciu o konsultację z biznesem, to jednak zawiera ogromną ilość wymogów, z których część została przedstawiona jako egzemplifikacja tezy o niezwykle wysokich wymogach dla przedsiębiorstw aplikujących o status AEO. Dodatkowe wyjaśnienia zawiera obszerny (29 stron) „Kwestionariusz samooceny AEO", tamże.

członkowskie. Jednak sytuacja znacznie się komplikuje wówczas, kiedy (a tak dzieje się coraz częściej), kiedy działy finansowo – księgowe aplikujących firm funkcjonują na zasadach out-sourcingu, na dodatek nie tylko w kraju dokonywania odpraw celnych, ale i w ogóle nie w którymkolwiek państwie członkowskim UE, lecz np. w Indiach. Wówczas kolejny element odnoszący się do tego wymogu, jakim jest możliwość kontroli standingu finansowego firmy opartej na audycie stwarza jedną z trudniejszych barier uzyskania certyfikatu AEO. Podmiot ubiegający się o status AEO powinien umożliwić organowi celnemu fizyczny (sic!) i elektroniczny dostęp do swoich ewidencji celnych oraz transportowych. Co więcej powinien również posiadać system logistyczny rozróżniający towary wspólnotowe i niewspólnotowe. Na dodatek powinien mieć strukturę administracyjną, która jest zgodna z rodzajem prowadzonej działalności i odpowiednia do zarządzania przepływem towarów. W ramach tej struktury przedsiębiorstwo winno posiadać system kontroli wewnętrznej, zdolny do wykrywania transakcji nielegalnych lub nieprawidłowych. A takie rozwiązanie strukturalne nie tylko nie obniża kosztów funkcjonowania i nie upraszcza zarządzania przedsiębiorstwem, lecz je komplikuje i podraża. Wprowadza odwrotne do zamierzonych skutki danej regulacji.

Dobry standing finansowy czyli płynność i wypłacalność finansowa przedsiębiorstwa jest kolejnym warunkiem uzyskania statusu AEO. Oznacza to wymóg posiadania dobrej sytuacji finansowej, która umożliwia przedsiębiorcy regulowanie jego zobowiązań stosowanie do rodzaju prowadzonej przez niego działalności gospodarczej związanej z międzynarodowym obrotem towarowym. Sytuacja tak odnosi się do trzech ostatnich lat[44]. Oto pytania na jakie aplikujący przedsiębiorca musi dać odpowiedź pozytywną (odpowiednio udokumentowaną): niezaleganie z daninami publicznymi (podatki, cła, ZUS); pozytywna opinia banku o ostatnich trzech latach obrotów finansowych; podobna opinia biegłego rewidenta; odpis z rejestru dłużników; informacja o tytule prawnym do użytkowanego majątku; informacja o zawarciu umów na użyczenie własnego majątku; inne dokumenty jakie wnioskodawca uważa za istotne. Nie jest to wbrew pozorom mało,

[44] Por. Kwestionariusz samooceny, sekcja 4., na: http://www.mf.gov.pl/index.php?const=2&dzial=771&wysw=4&sub=sub13

a przecież to zaledwie jeden z bloków informacji, jaka musi być dostarczona do organów celnych przez wnioskujące przedsiębiorstwo.

Jeszcze bardziej rozbudowane są wymogi w przypadku występowania o certyfikat dla potrzeb ***bezpieczeństwa i ochrony*** albo ***o uproszczenia celne oraz bezpieczeństwa i ochrony***. W tym przypadku, zgodnie z „Kwestionariuszem samooceny" przedsiębiorstwo winno wykazać się posiadaniem odpowiednich standardów bezpieczeństwa i ochrony[45]. Przedsiębiorca powinien więc wykazać się wysokim stopniem wiedzy o środkach bezpieczeństwa i ochrony zarówno wewnątrz przedsiębiorstwa, jak i w kontaktach z klientami, dostawcami i usługodawcami zewnętrznymi. Powinien mieć udokumentowane procedury dotyczące kontroli bezpieczeństwa dostępu do budynków, towarów na terenie przedsiębiorstwa, jak i transportu, rekrutacji pracowników oraz doboru partnerów biznesowych. W sumie ok. 40 (sic!) wymogów jakie winny być spełnione, a bez których takiego certyfikatu nie można otrzymać.

Co więcej dla uzyskania obojętnie któregokolwiek z certyfikatów AEO koniecznym jest, jako *conditio sine qua non* **spełnienie wszystkich łącznie**, przewidzianych dla danego rodzaju świadectwa kryteriów, przewidzianych we wspomnianym „Kwestionariuszu samooceny". Musimy pamiętać o tym, że status AEO uzyskiwany jest na podstawie dobrowolnej aplikacji przedsiębiorcy i nie jest to obowiązek, lecz – powtórzmy to – prawo do takiego statusu. Jest to kwestia wyboru samych przedsiębiorców, w zależności od ich konkretnej sytuacji, możliwości organizacyjnych, finansowych, kadrowych, etc., etc.

Zasadą jest, że status upoważnionego przedsiębiorcy może być przyznany każdemu przedsiębiorcy posiadającemu siedzibę na obszarze celnym Wspólnoty Europejskiej. Jednakże i w tym przypadku możliwe są określone wyjątki, takie jak np. wówczas kiedy istnieje odpowiednia umowa między UE a krajem trzecim o wzajemnym uznawaniu takich certyfikatów[46], czy wówczas kiedy aplikuje o status AEO linia lotnicza lub żeglugowa posiadająca swoje oddziały w UE i posiadające uproszczenia w zgłoszeniach do odpraw celnych.

[45] Tamże, sekcja 5.

[46] Odnosi się to możliwości wynikającej z sytuacji przewidzianej w WCO SAFE Framework jako jednego z możliwych wariantów upowszechnienia AEO i tym samym zrealizowania założeń dotyczących bezpieczeństwa i ułatwień dla łańcucha międzynarodowego łańcucha dostaw towarowych.

Pojęcie ***przedsiębiorcy*** oznacza w tym kontekście osobę, która w ramach prowadzonej działalności gospodarczej jest włączona w czynności określone przepisami prawa celnego. Statusu AEO nie mogą uzyskać, więc przedsiębiorcy, którzy nie prowadzą działalności związanej z cłami.[47] Zaznaczyć należy, że pojęcie przedsiębiorcy nie ogranicza pojęcia „włączenie w czynności określone przepisami prawa celnego" jedynie do bezpośredniego włączenia. Producent wytwarzający towary przeznaczone do wywozu może złożyć wniosek o status AEO, nawet, jeżeli formalności wywozowe są realizowane przez inną osobę.[48]

Jednakże w tym przypadku może to być stosowane pod warunkiem, że posiadacz statusu AEO, albo jest uwzględniony jako partner biznesowy przedsiębiorcy poddanemu weryfikacji przy wydawaniu certyfikatu, albo sam jest posiadaczem takiego certyfikatu. W istocie może nim być, w praktyce, jedynie agent celny (w Polsce agencja celna).

Wnioski

Jeśli więc weźmiemy pod uwagę wszystkie omówione, a przecież to tylko przykładowe, nawet nie minimalne wymogi, a równocześnie uwzględnimy czas aplikowania czyli nie mniej niż rok przed uzyskaniem statusu oraz warunki powodujące utratę tego statusu, przy tak niewielkich korzyściach realnych jakie status AEO daje przedsiębiorstwu międzynarodowego obrotu towarowego, to nic dziwnego, że brak jest większego zainteresowania przedsiębiorców tą instytucją. Co więcej, instytucjonalno-prawne otoczenie AEO i jej ideologiczne powiązanie z ogłoszoną wojną z terroryzmem, której koszty obciążają nie tylko samą instytucję upoważnionego przedsiębiorcy, ale i w rezultacie zaostrzenia kontroli celnej, wydłużania czasu odprawa towarów znajdujących się w międzynarodowym łańcuchu dostaw, stanowią dodatkowe bariery dla upowszechnienia tej instytucji nie tylko w UE, ale i w świecie.

Z jednej strony nastąpiły, bądź też następują zmiany w organizacji samej administracji celnej. Pojawiło się co najmniej dwa modele tych zmian – z jednej strony ze względu na zmniejszenie fiskalnej funkcji celnictwa i ceł w kształtowaniu dochodów narodowych z równoczesnym wzrostem ochronnych funkcji – nastąpiło zlanie się funkcji granicznej

[47] P. Molik, *Na czym polega status upoważnionego podmiotu gospodarczego* [w:] Gazeta Prawna Nr 24 z dnia 4.02.2008, s. 16

[48] *Upoważnieni przedsiębiorcy. Wytyczne*, Komisja Europejska Dyrekcja Generalna ds. Podatków i Unii Celnej (TAXUD/2006/1450)

kontroli celnej z ochroną granicy w ogóle, z drugiej zaś przy wzroście ochronnej funkcji nastąpiło przełożenie nacisku na zlanie się administracji celnej z administracją skarbową.

Pierwszy model został zastosowany w USA. Przywrócona została pierwotna rola i zadania amerykańskiej służby celnej jako koordynatora wszystkich działań ochronnych nie tylko na granicach (lądowych, morskich i powietrznych), ale i wewnątrz a nawet na zewnątrz kraju, o czym najlepiej świadczy CSI oraz C-TPAT i zaangażowanie w zagranicznych portach oficerów CBP.

Drugi model, łączenia administracji celnych i skarbowych, uwzględniając aspekty bezpieczeństwa i ochrony międzynarodowego łańcucha dostaw towarowych, znalazł zastosowanie w Europie, np. Wielkiej Brytanii , Belgii czy Łotwie i Estonii. Jednak doświadczenia i wnioski płynące z tego rozwiązania nie zawsze są pozytywne, mimo nadania tym administracjom (w praktyce reprezentowanych przez tzw. wydziały lub piony celne, które w istocie, poza zmianami czyli przede wszystkim, zmniejszeniem kadr niewiele zmieniły w zakresie dotychczasowych zadań) szerokich uprawnień nie tylko w zakresie kontroli fiskalnej, ale w zakresie bezpieczeństwa międzynarodowego łańcucha dostaw towarów.

Rozwiązania te, będąc pochodnymi od współczesnej filozofii rozwoju służb granicznych i formułowanych na nowo definicji misji celnictwa, rzutują również na pozycję tej administracji na arenie międzynarodowej. Najbardziej wyraźnie widać to w Unii Europejskiej, gdzie zostały wyodrębnione dwa filary, w ramach których funkcjonują dwie struktury organizacyjne – TAXUD (Dyrekcja Generalna ds. Unii Celnej i Podatków Pośrednich) oraz samodzielna jednostka FRONTEX (Agencja ds. Zarządzania Zewnętrzną Granicą UE).[49]

Pierwszy z tych organów nadal jest w UE traktowany, jako organ z tzw. I filaru (gospodarczego) zaś drugi, utworzony w 2005r., to reprezentant III filaru czyli sfery bezpieczeństwa, sprawiedliwości i wolności (Justice, Security and Liberty – JSL). Czy i na ile narodowe służby celne w UE zostaną szerzej włączone w prace FRONTEXu miał pokazać przegląd działania tej agencji jaki został dokonany w 2007 r. Jednakże zgodnie z założeniami agencja ta skupia się na wymianie osobowej, a zwłaszcza na ochronie granic zewnętrznych UE przed nielegalnymi imigrantami, a nie międzynarodowych obrotach

[49] Por. informacje na temat FRONTEX na: http://www.frontex.europa.eu/

towarowych. W związku z tym w praktyce nie nawet praktycznie współpracy na poziomie unijnym tych dwóch służb.

Dlatego też szczególna rola w zakresie bezpieczeństwa międzynarodowego obrotu towarowego przypada służbie celnej. Funkcja ta została, po serii zamachów terrorystycznych z lat 2001-2005, wybita na plan pierwszy w działalności nie tylko europejskich służb celnych, ale i pozostałych państw członkowskich WCO. Odpowiednie projekty zostały sformułowane, pod dużym wpływem ideologicznym, organizacyjnym i koncepcyjnym służby celnej USA, zarówno przez WCO, jak i UE.

Tradycyjny paradygmat celnictwa – z poborcy cła, z fiskalnej funkcji i modernizacji procedur, ułatwień i uproszczeń procedur celnych, jakie dominowały w końcu XX wieku został po tych wydarzeniach zastąpiony nowym paradygmatem – bezpieczeństwem międzynarodowego łańcucha dostaw towarowych. W rezultacie dokonano szeregu zmian w unijnym prawie celnym, w tym w nowym (znowelizowanym z 2008 r.) Wspólnotowym Kodeksie Celnym.

Widać więc wyraźnie, że na szczeblu wspólnotowym ten aspekt znalazł się wśród podstawowych zadań jakie mają do spełnienia administracje celne Zjednoczonej Europy, a wśród nich i polska administracja celna.

Drugim, niezwykle ważnym rezultatem zapoczątkowanych przez CBP programów bezpieczeństwa i ochrony przed zagrożeniem terrorystycznym, okazała się konieczność ścisłej współpracy narodowych administracji celnych między sobą oraz tych służb z kręgami biznesowymi.

W obydwu przypadkach okazało się niezbędnym doskonalenie procedur kontrolnych z wykorzystaniem współczesnych technik komunikacyjnych i informatycznych (ICT), jak i nowoczesnych metod kontrolnych, przede wszystkim wykorzystujących prewencję i analizę ryzyka, a tym samym odstępujących od kompleksowych rewizji dostaw na granicach czy w miejscach odpraw, z równoczesnym wprowadzeniem ułatwień i uproszczeń tych odpraw z przy zwiększeniu skuteczności dokonywanych kontroli.

Dla biznesu inicjatywy te miały okazać się korzystne, choć rzeczywistość, przynajmniej na razie, tego nie potwierdziła. Ilość kryteriów i koszty jakie muszą ponieść, by je spełnić, przedsiębiorcy by uzyskać określone, zresztą w istocie mało znaczące w porównaniu do już posiadanych, przywilejów, uproszczeń i ułatwień skutkuje tym, że idea

tzw. upoważnionego przedsiębiorcy (AEO) okazała się mało atrakcyjną dla biznesu[50].

Co więcej, nie zmieniło tego stanu ani przyjęcie Rozporządzenia 648 ani europejskiej strategii celnictwa elektronicznego[51] związanej z ideą bezpieczeństwa i ułatwień w międzynarodowym łańcuchu dostaw, ani nowego WKC. Przedsiębiorcy i ich firmy w dalszym ciągu znajdują się na etapie analizy kosztów i zysków z aplikowania o status AEO. A te, wynikające z badanych przez organy celne, kryteriów funkcjonowania przedsiębiorstw wiążą się z ogromnymi jednorazowymi i stale ponoszonymi kosztami, których efektywność biznesowa jest znikoma. Dlatego zarządzanie przedsiębiorstwem współczesnym działającym na międzynarodowym rynku towarowym, jest mocno powiązane z ekonomiczną analizą regulacji celnych. Tych, niestety, nie przeprowadzili twórcy takich regulacji ani w WCO, ani w USA, ani w UE. Uczynili to jednak przedsiębiorcy, a zwłaszcza menadżerowie odpowiedzialni za funkcjonowanie firmy na rynku, za pomnażanie jej wartości, za utrzymanie i zwiększanie jej konkurencyjności na rynku. Ich analizy pokazują, że w praktyce sama idea polityczna nie jest wystarczająca dla dokonywania remodelingu zarządzania firmą na rzecz dostosowania się do kryteriów upoważnionego przedsiębiorcy.

---

[50] Zgodnie z danymi Komisji (TAXUDu) z połowy lipca 2008r. w centralnej bazie AEO znajdowało się 1040 aplikacji o uzyskanie statusu AEO złożonych przede wszystkim przez wielki przedsiębiorstwa. Spośród nich: 78% złożyło wnioski o certyfikat na uproszczenia celne i bezpieczeństwa oraz ochrony; 19% tylko dla uproszczeń celnych oraz 3% wyłącznie dla bezpieczeństwa i ochrony. Uzyskało certyfikat AEO zaledwie 164 przedsiębiorstw z 13 państw członkowskich. Najwięcej ze Szwecji (46). Mimo to Komisja prognozuje, że do 1 lipca 2009 r. może otrzymać ok. 10-20 tys. aplikacji. Jak wskazują analizy dokonane przez CLECAT i CONFIAD to zbyt daleko posunięty optymizm, ale nawet gdyby udało się to osiągnąć to i tak byłby to zaledwie znikomy procent od milionów europejskich MSP (SME).Cyt.za: CONFIAD Paneuropean Network World E-flash no 42 of July 14, 2008.

[51] *Por. Komunikat na temat osiągnięcia przez Europejską Radę Ministrów porozumienia politycznego w sprawie pan-europejskiego wprowadzenia celnictwa elektronicznego – "European Council of Ministers to reach a political agreement on the implementation of pan-European electronic customs"* - http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/627&format=HTML&aged=0&language=EN&guiLanguage=en *z dnia 08 maja 2007r, godz. 21:44* ostatecznie przyjęta jako*:* DECISION No 70/2008/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 January 2008 on a paperless environment for customs and trade, w: OJ EU, L 23/21 z dnia 26 stycznia 2008.

Przynajmniej nie na aktualnym etapie rozwoju procesu globalizacji i integracji europejskiej.

Tym nie mniej dają się i w tej sferze zaważyć, że i w UE zmienia się stary paradygmat celnictwa – z poborcy cła, z fiskalnej funkcji i modernizacji procedur, ułatwień i uproszczeń procedur celnych jakie dominowały w końcu XX wieku na rzecz bezpieczeństwa międzynarodowego łańcucha dostaw towarowych oraz uproszczeń i ułatwień dla tego obrotu.

To właśnie w uzasadnieniu do projektu znowelizowanego WKC wskazuje się na to, m.in., że jednymi z przyczyn konieczności jego przyjęcia jest *„...zwiększenie bezpieczeństwa na granicy zewnętrznej...*" oraz , że w nowych warunkach *„(...) zmienia się rola służb celnych. Zmiany polegają na przechodzeniu od pobierania należności celnych, które w ostatnich 20 latach drastycznie się zmniejszyły, do stosowania środków pozataryfowych, w szczególności do środków związanych z bezpieczeństwem(...)*".[52]

Jest to kontynuacja procesu związanego z wprowadzaniem do Kodeksu celnego zmian, które mają służyć zwiększeniu bezpieczeństwa międzynarodowego obrotu towarowego.[53] To tu wprowadzono nowe instytucje do WKC takie jak Upoważniony Przedsiębiorca (Upoważniony Podmiot Gospodarczy – Authorized Economic Operator-AEO), nowe metody kontroli poprzez szerokie stosowanie analizy ryzyka, etc., etc. Dlatego też w projekcie Znowelizowanego Wspólnotowego Kodeksu Celnego wśród podstawowych zadań organów celnych (Rozdz.I, Artykuł 2, pkt c) znalazło się sformułowanie: „***zapewnienie bezpieczeństwa i ochrony obywateli oraz środowiska ...***". Widać więc wyraźnie, że i na szczeblu wspólnotowym ten aspekt znalazł się wśród podstawowych zadań jakie mają do spełnienia administracje celne Zjednoczonej Europy, a wśród nich i polska administracja celna.

Drugim, niezwykle ważnym rezultatem zapoczątkowanych przez CBP programów bezpieczeństwa i ochrony przed zagrożeniem

[52] Rozporządzenie (WE) Parlamentu Europejskiego i Rady ustanawiający Wspólnotowy Kodeks Celny (Zmodernizowany Kodeks Celny) przedstawiony przez Komisję), COM(2005) 608 końcowy, s. 2-3.

[53] Por. np. Zmiana WKC na rzecz rozszerzenia zakresu kontroli odnoszącej się do bezpieczeństwa w Rozporządzeniu ROZPORZĄDZENIE (WE) NR 648/2005 PARLAMENTU EUROPEJSKIEGO I RADY z dnia 13 kwietnia 2005 r. w Dz.U. UE L z 4 maja 2005, nr 117, s.13 i nast.

terrorystycznym, okazała się konieczność ścisłej współpracy narodowych administracji celnych między sobą oraz tych służb z kręgami biznesowymi.

W obydwu przypadkach okazało się niezbędnym doskonalenie procedur kontrolnych z wykorzystaniem współczesnych technik komunikacyjnych i informatycznych (ICT) jak i nowoczesnych metod kontrolnych, przede wszystkim wykorzystujących prewencję i analizę ryzyka, a tym samym odstępujących od kompleksowych rewizji dostaw na granicach, czy w miejscach odpraw, z równoczesnym wprowadzeniem ułatwień i uproszczeń tych odpraw z przy zwiększeniu skuteczności dokonywanych kontroli.

Wreszcie dla biznesu inicjatywy te okazały się także korzystne, choć oczywiście tylko dla uczciwych przedsiębiorców. Co prawda, jak zawsze przy wprowadzaniu nowości techniczno-organizacyjnych, tak i w tym przypadku koszty wprowadzanych rozwiązań były i są jednym z elementów hamujących ich upowszechnienie. Jednakże strategiczna przewaga konkurencyjna będąca pochodną od skrócenia czasu odpraw („time is money") zaczyna dominować zarówno wśród administracji celnych jak i kręgów biznesowych.

Tak więc, niezależnie od efektów polityczno-ideologiczno-propagandowych praktyczne efekty inicjatyw i programów okazały się korzystne dla wszystkich zainteresowanych czyli także europejskich administracji celnych oraz kręgów biznesowych.

Dzięki omówionym inicjatywom zostały w warunkach globalizacji stworzone przesłanki dla bardziej bezpiecznego życia człowieka i narodów, a tym samym i bezpiecznego łańcucha międzynarodowych dostaw towarowych. Odnosi się to także w dużym stopniu do administracji celnych, procedur i prawa celnego Unii Europejskiej. Co więcej, zwłaszcza po przyjęciu europejskiej strategii celnictwa elektronicznego[54] związanej z ideą bezpieczeństwa i ułatwień w międzynarodowym łańcuchu dostaw proces ten nie tylko, że nie zakończył się, ale na dobrą sprawę dopiero nabiera nowego rozmachu.

---

[54] Por. Komunikat na temat osiągnięcia przez Europejską Radę Ministrów porozumienia politycznego w sprawie pan-europejskiego wprowadzenia celnictwa elektronicznego – "European Council of Ministers to reach a political agreement on the implementation of pan-European electronic customs" – http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/627&format=HTML&aged=0&language=EN&guiLanguage=en z dnia 08 maja 2007r, godz. 21:44

Bibliografia

Druki zwarte

1. Barcz J.,. Kawecka-Wyrzykowska E, Michałowska-Gorywoda K., *Integracja Europejska*, Wyd. Wolters Kluwer, Warszawa, 2007.
2. Bartoszewicz T., *GATT a Międzynarodowa Polityka Handlowa*, PWE, Warszawa 1988.
3. Czyżowicz W. (red.), *Warunki i zadania w zakresie handlu zagranicznego po akcesji Polski do Unii Europejskiej*. Raport przygotowany przez Zespół Międzyresortowy. Tom I – IV, T. I Synteza, Rządowe Centrum Studiów Strategicznych, Warszawa 2003.
4. Czyżowicz W., *Polskie cło 1997-2003*, WSE, Warszawa 2003.
5. Czyżowicz W. (red.), *Prawo celne*, Wyd. C. H. Beck, Warszawa 2004.
6. Drwiło A., *Postępowanie ochronne w prawie celnym*, Wyd. Arche, Gdańsk 2003.
7. Gilowska Z., Izdebski H. Raczkowskiego K. (red.), *Efektywna Administracja Skarbowa*, Ministerstwo Finansów, Wyd. DIFIN, Warszawa 2007.
8. Hoekman B., Kostecki M. M., *Ekonomia światowego systemu handlu-WTO: Zasady i mechanizmy negocjacji*, Wyd. Akademii Ekonomicznej im. O.Langego, Wrocław 2002.
9. Kaczurba J., Kawecka-Wyrzykowska E. (red.), *Polska w WTO*, IKC HZ, Warszawa 2002.
10. Kawecka-Wyrzykowska E., Synowiec E., (red.), *Unia Europejska. Integracja Polski z Unią Europejską*, IKC HZ, Warszawa 1996
11. Kawecka-Wyrzykowska E., E. Synowiec (red.), *Unia Europejska. Przygotowania Polski do członkostwa*, IKC HZ, Warszawa 2001.
12. Kuś A., *Publicznoprawne pozataryfowe i parataryfowe instrumenty reglamentacji obrotu towarowego z zagranicą. Studium teoretyczno-prawne*, Oficyna wyd. Branta, Bydgoszcz-Lublin, 2006.
13. Krugman P. R., Obstfeld M., *Ekonomia międzynarodowa. Teoria i polityka,* t.1, PWN, Warszawa, 2007.
14. Maksimczuk, L. Sidorowicz, *Graniczna obsługa ruchu osobowego i towarowego w Unii Europejskiej (wybrane aspekty)*, Wyd. ALMAMER WSE, Warszawa 2008.

15. Molski R., *Administracyjnoprawna regulacja obrotu towarowego z zagranicą*, Szczecin, Uniwersytet Szczeciński, „Rozprawy i Studia" T. (CDLII) 378, 2001.
16. Smitienko M. B., (red.), *Mieżdunarodnyje ekonomiczeskije otnoszenija*, Moskwa, INFRA-M, 2008.

Dzienniki i periodyki

1. „Gazeta Wyborcza", 09-01-16.
2. „Rzeczpospolita" z 5 kwietnia 2006r, s. C3.
3. „Customs World", London, Autumn 2003.
4. „Wiadomości celne", 2006, nr 2/3.
5. "Customs Today. Startegic Perspectives on Trade, Security and Canadian Business", Ottawa, May 2007.
6. Monitor Prawa Celnego i Podatkowego", Szczecin, Wyd. BW, nr 9 (158)/2008, rok XII, wrzesień 2008.
7. Molik P., *Na czym polega status upoważnionego podmiotu gospodarczego* [w:] „Gazeta Prawna" Nr 24 z dnia 4.02.2008.
8. CONFIAD Paneuropean Network World E-flash no 42 of July 14, 2008.
9. Matyszewska E., *Reforma: Połączenie celników i skarbówki – Krajowa Administracja Skarbowa zacznie funkcjonować od 1 stycznia 2008r.*, [w]: „Gazeta Prawna", Warszawa, 2007.
10. Jałoszyński K., *Unia wobec zagrożenia terroryzmem*, [w:] „Monitor Unii Europejskiej", Warszawa, 2008, nr 7/8(49/50).
11. „Monitor Prawa Celnego i Podatkowego", Szczecin, Wyd. BW, nr 9 (158)/2008, rok XII, wrzesień 2008.
12. Finance & Development", A quarterly magazine of the IMF, Washington, March 2006, vol.43, Nr 1, p.3, tab.1.

Dokumenty o charakterze normatywnym

1. Dz. U. z dnia 28 lutego 1992r, Załącznik do nr 17, poz. 69. Był to w istocie III rozdział Układu Stowarzyszeniowego.
2. Układ Europejski Ustanawiający stowarzyszenie między Rzeczpospolitą a Wspólnotami Europejskimi i ich państwami członkowskimi, z drugiej strony, Dz. U., z 27 stycznia 1994 r., załącznik do nr 11, poz. 38.
3. Dziennik Urzędowy Unii Europejskiej L 236 z 23 września 2003.
4. DECISION No 70/2008/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 January 2008 on a paperless

environment for customs and trade, [w:] OJ EU, L 23/21 z dnia 26 stycznia 2008 „Finance & Development", A quarterly magazine of the IMF, Washington, March 2006, vol.43, Nr 1, p.3, tab.1.
5. „Monitor Prawa Celnego i Podatkowego", Szczecin, Wyd. BW, nr 9 (158)/2008, rok XII, wrzesień 2008.
6. *Upoważnieni przedsiębiorcy. Wytyczne*, Komisja Europejska Dyrekcja Generalna ds. Podatków i Unii Celnej (TAXUD/2006/1450).

Strony internetowe

1. http://www.mgip.gov.pl/GOSPODARKA/DKE/Akty/. Departament Kontroli Eksportu Ministerstwa Gospodarki
2. http://www.bis.doc.gov/PoliciesAndRegulations/MultilateralExportRegimes.htm Strona domowa Biura Bezpieczeństwa i Przemysłu Ministerstwa Handlu USA.
3. http://www.egmontgroup.org/, Strona domowa tzw. Grupy Egmont http://www.mf.gov.pl/index.php?const=1&dzial=79&wysw=82&sub=sub8, Strona domowa Generalnego Inspektora Informacji Finansowej.
4. http://www.mf.gov.pl/dokument.php?const=2&dzial=525&id=47104, Strona domowa polskiej służby celnej
5. http://www.commondreams.org/headlines05/0426-09.htm. Source: Reuters, 050426.http://www.worldtraderef.com/WTR_site/csi.asp.
7. http://www.cbp.gov/xp/cgov/border_security/international_activities/csi/csi_in_brief.xml.
8. http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml.
9. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/.
10. http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf
11. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/
12. http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/SAFE%20Framework_EN_2007_for_publication.pdf.
13. http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Enforcement/WCO%20TABLE%20Intention%20to%20implement%20the%20FOS-%20EN-FR_June08V2.pdf z :081017.
14. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005R0648:PL:HTML;081017.

15. http://www.mf.gov.pl/_files_/sluzba_celna/akty_prawne/przepisy_celne/wspolnotowe/pc_lexuriserv-pl.pdf.
16. http://www.mofnet.gov.pl/index.php?const=2&dzial=771&wysw=4&sub=sub13.
17. http://www.mf.gov.pl/_files_/sluzba_celna/aeo/aeo_wyjasn.pdf .
18. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/627&format=HTML&aged=0&language=EN&guiLanguage=en z dnia 08 maja 2007r.
19. http://www.bitd.org/default.asp.
20. http://www.frontex.europa.eu/ Informacje na temat FRONTEX

LOGISTIC CHAIN SECURITY IN INTERNATIONAL GOODS TURNOVER – DEVELOPMENT TENDENCIES IN XXI CENTURY

Summary

Paper is dedicated to the „Logistic Chain Security in International Goods Turnover – Development Tendencies in XXI century". Author presents multidisciplinary approach to international turnover (not only trade) in goods from customs policy, customs laws and customs procedures as well as ICT points of views.

The analysis starts with the new paradigm for customs control policy aim ("***security first***", instead "***customs facilitation and simplifications***") after the 9/11/2001. It describes the international aspects related to the proclaimed by USA "***war against international terrorism***" presented in war propaganda particularly by Al – Qaida groups. Here is presented detailed history of US, WCO and EU legal projects, programs, laws and regulation and their implementation into practice in e-business environment and in various institutions, regions and countries as well as positions of business communities

It is related, particularly, to US ***Container Security Initiative*** (CSI) and ***Customs – Trade Partnership Against Terrorism*** (C-TPAT). The next specific field is related to the international context dedicated to the World Customs Organization resolution on ***WCO SAFE Framework of Standards to Secure and Facilitate Global Trade)***.

The next part of the paper is connected with detailed analysis of EU Regulation 648 (Reg.on AEO). Author presents review arguments in favor and contra this regulation from business point of view. The end

of the article presents some conclusions on practical aspects of the antiterrorist hysteria and its international and national business communities' consequences. The most general lessons from the presented in paper analysis are questions: who is going to pay for it?, how much?, and when? These are theoretical and very practical questions for all of us.

Janusz Tomaszewski*
Dominik Iwen**

BEZPIECZEŃSTWO GOSPODARKI MORSKIEJ W WARUNKACH ZAGROŻENIA KRYZYSEM GOSPODARKI ŚWIATOWEJ

Streszczenie

W artykule przedstawiono zasadnicze problemy związane z bezpieczeństwem gospodarki morskiej. Autorzy zdefiniowali bezpieczeństwo morskie, jako część polityki morskiej państwa. W oparciu o przykłady statystyczne zwrócili uwagę na negatywne tendencje gospodarce morskiej. Wskazali na bezpieczeństwo ekologiczne jako komponent bezpieczeństwa w rejonie Morza Bałtyckiego. Omówili najważniejsze porozumienia międzynarodowe mające związek z bezpieczeństwem gospodarki morskiej. Opisali zadania służb i instytucji odpowiedzialnych za owe bezpieczeństwo, w tym wybranych ogniw Systemu Obronnego Państwa. W zakończeniu zaprezentowali obszary i kierunki rozwoju, które w chwili obecnej stanowią priorytetowe wyzwanie dla polskiego systemu bezpieczeństwa morskiego.

Wstęp

Problematyka bezpieczeństwa, poruszana przez autora artykułu na licznych konferencjach krajowych i międzynarodowych jest wciąż aktualna oraz tak w teorii, jak i praktyce wymaga ciągłych badań. Doświadczenia ostatnich lat – od tragedii WTC w 2001 roku, przez zaangażowanie polityczno-militarne Polski w konflikty w Iraku oraz Afganistanie, „wojny gazowo-naftowe", do zagrożenia światowym kryzysem gospodarczym – wskazują, że paradygmat o dominującej roli sektora militarnego w walce o bezpieczeństwo został złamany. Wspomniane doświadczenia podpowiadają konieczność rozwijania współpracy międzynarodowej dla utrwalania koalicyjnego bezpieczeństwa ekonomicznego. Wydarzenia na rynkach finansowych wskazują na dewaluację sprawdzonych wcześniej rozwiązań monetarystycznych, zaś już w roku 2004 stwierdzono, że zasadniczych

celów strategii lizbońskiej nie udało się wcielić w życie.[1] Recesja finansowa w gospodarce światowej zatacza coraz szersze kręgi, co wymaga odejścia od skrajnie liberalnej polityki państwa, na rzecz jego aktywnej roli w gospodarce. Szczególnie dziedzinie polityki monetarnej oraz zatrudnienia.
Weryfikacji wymagają przyjęty budżet, a także Strategie i Narodowy Plan Rozwoju, konstruowane w oparciu o wskaźniki fazy rozkwitu gospodarki lat 2005 - 2007. Zmieniająca się na niekorzyść sytuacja gospodarcza implikuje konieczność nowych koncepcji w dziedzinie bezpieczeństwa. Coraz większe przy tym znaczenie ma poczucie bezpieczeństwa energetycznego, finansowego, żywnościowego – słowem ekonomicznego. Niezależnie od tego, czy mówimy o bezpieczeństwie militarnym, geopolitycznym, czy ekonomicznym w każdym z tych wariantów mamy na myśli bezpieczeństwo państwa i jego obywateli. Osadzone ono jest na elementach potencjału obronno ekonomicznego. Komponentem owego bezpieczeństwa jest bezpieczeństwo gospodarki morskiej.

1. Bezpieczeństwo Państwa

Bezpieczeństwo państwa to niezależny byt jego obywateli, brak poczucia zagrożenia podstawowych dla społeczeństwa wartości politycznych ideologicznych i gospodarczych. Pojęcie bezpieczeństwa państwa kojarzone jest często z bezpieczeństwem narodowym.[2]

Zdaniem Ryszarda Stemplowskiego państwo bezpieczne to takie, „(…) które może realizować swoją rację stanu (podstawowy interes narodowy) w sposób wykluczający naruszenie pokoju (…)[3]. Ten sam autor zwraca uwagę na konieczność występowania warunków wstępnych niezbędnych dla realizacji racji stanu. Wśród nich *na pierwszym* miejscu

*Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.
** Autor jest oficerem okrętów zabezpieczenia hydrograficznego MW RP

[1] Szerzej Janusz Tomaszewski, *Strategia lizbońska a bezpieczeństwo ekonomiczne Polski – sukces, czy porażka?* w: M. Grzybowski, J Tomaszewski (red.), Bezpieczeństwo w administracji i biznesie, WSA i B Gdynia 2007, s. 203 i następne.

[2] Z. Stachowiak, *Bezpieczeństwo ekonomiczne,* w*:* W. Stankiewicz, Ekonomika obrony, AON, Warszawa 1994, s. 181 - 183.

[3] R. Stemplowski, *Horyzont poznawczy i polityczny pojęcia „Bezpieczeństwo Państwa”*, *w:* R. Kuźniar, Z. Lachowski, (red.), *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia- Koncepcje – Instytucje*, Państwowy Instytut Spraw Międzynarodowych, Warszawa 2003, s. 255.

wymienia warunki egzystencjalne o charakterze obiektywnym, jak: integralność terytorialna państwa związana z bezpieczeństwem ekonomicznym społeczeństwa, podaż podstawowych dóbr, zatrudnienie siły roboczej przy efektywnym jego kontrolowaniu przez rząd. Na tym poziomie zwraca również uwagę na wzrost gospodarczy, umiarkowany wzrost demograficzny oraz umiejętność przeciwdziałania negatywnym zjawiskom w dziedzinie ochrony i opieki zdrowotnej z najgroźniejszymi epidemiami włącznie, a także zdolność do likwidowania katastrof wywołanych siłami przyrody. Nie bez znaczenia jest tu również percepcja bezpieczeństwa przez społeczeństwo. Choć jest to warunek subiektywny, to badania opinii społecznej powinny wskazać na szczegółowe zamierzenia w dziedzinie polityki i edukacji[4] dla bezpieczeństwa. Wobec wyzwań współczesnego świata, bezpieczeństwo państwa uzależnione jest również od potencjału wojskowego, policyjnego i wywiadowczego[5], budowanych na przesłankach ekonomicznych.[6] *Po drugie* do czynników umożliwiających realizację racji stanu zalicza się warunki instytucjonalne, w tym między innymi:[7]instytucje demokratycznego państwa prawa, racjonalnie zorganizowany rynek, system oświaty, instytucje religijne. W końcu *po trzecie* zwraca uwagę na warunki funkcjonalne, czyli:[8] zapobieganie pojawieniu się warunków zagrożenia do wykonywania tradycyjnych funkcji państwa wobec społeczeństwa w gospodarce[9]; analiza informacji

[4] Dotyczy to również edukacji niepełnosprawnych, gdzie szczególną uwagę zwraca się na zagadnienia bezpieczeństwa - zobacz szerzej K. Kaganek, *Przygotowanie oferty dla osób niepełnosprawnych,* Materiały szkoleniowe z zakresu funkcjonowania biur podróży, Ministerstwo Gospodarki i Pracy, Nowosądecka Organizacja Turystyczna, Warszawa 2004, zob. też: Kaganek K., *Psychologia pracy w turystyce z osobami niepełnosprawnymi,* w: „Tworzenie i dostosowywanie produktów turystycznych do potrzeb osób niepełnosprawnych", Forum Turystyki Regionów, Szczecin 2007.

[5] Szerzej L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy. Historia i współczesność, EAS,* Kraków 2005.

[6] R. Stemplowski, *Horyzont poznawczy ...op. cit.,* s. 255.

[7] *Ibidem,* s. 255-256.

[8] *Ibidem.*

[9] Wskazuje na to elementarny wykład z makroekonomii. Podstawowe funkcje państwa w gospodarce to: „(…)określenie i ochrona praw własności, ochrona przed przestępcami i wymierzanie sprawiedliwości przestępcom, zapewnienie obrony narodowej, powszechna oświata (…), stabilizowanie gospodarki, to znaczy ograniczenie wahań ogólnego poziomu działalności gospodarczej i poziomu bezrobocia, kontrola wykorzystania środowiska naturalnego (…), ochrona konsumentów przed nadużyciami konkurencyjnego procesu rynkowego, zapewnienie bezpieczeństwa dochodów i opieki zdrowotnej"; zobacz: D. R. Kamerschen, R. B. McKenzie,

oraz formułowanie ocen zmieniających się kryteriów bezpieczeństwa; utrzymywanie międzynarodowych stosunków bilateralnych i multilateralnych w ramach sojuszy gospodarczych, w tym finansowych i militarnych; prowadzenie badań naukowych i adaptowanie pozytywnych doświadczeń w dziedzinie umacniania bezpieczeństwa. Elementem bezpieczeństwa państwa jest bezpieczeństwo ekonomiczne.

Na gruncie ekonomiki obrony, przyjmując za bazę potencjał obronno – ekonomiczny, bezpieczeństwo ekonomiczne, wyrastające a jednocześnie wpływające na bezpieczeństwo państwa definiowane jest, *jako zdolność systemu gospodarczego państwa do takiego wykorzystania wszystkich wewnętrznych i zewnętrznych czynników wzrostu gospodarczego, które by zapewniało niezagrożony rozwój gospodarczy.* Tradycyjnie za wstępne warunki wzrostu uważa się odpowiednią ilość i jakość siły roboczej (kapitału ludzkiego), odpowiednią ilość i jakość kapitału (w ujęciu rzeczowym i finansowym), posiadane zasoby naturalne, technologię oraz warunki socjo-kulturowe. Wewnętrzne czynniki wzrostu to stan gospodarki, struktury własnościowe, przyjęte w Ustawie zasadniczej oraz ustawodawstwie gospodarczym zasady i mechanizmy funkcjonowania wszystkich podmiotów gospodarczych; wzajemne ich powiązania. Czynniki zewnętrzne to stopień powiązania z otoczeniem: międzynarodowe współzależności ekonomiczne, w tym poziom zaangażowania w realizację międzynarodowych inicjatyw i programów gospodarczych. Stąd może wynikać stopień odporności na zewnętrzną ingerencję gospodarczą; na niemilitarne środki wojny gospodarczej.

Praktyka ostatnich lat dowodzi słuszności przyjętej w artykule problematyki bezpieczeństwa ekonomicznego oraz zagrożeń wynikających, na przykład z szantaży gazowych. Groźba światowego kryzysu gospodarczego odsunęła na plan dalszy dyskusje nad światowym terroryzmem. Recesja finansowa w ramach efektu domina wpływa na wciąż nowe dziedziny gospodarowania. W tej sytuacji konieczną staje się dyskusja nad bezpieczeństwem oraz nad zagrożeniami bezpieczeństwa - tak w ujęciu teoretycznym przez rozwój ekonomiki obrony, securitologii,[10] w końcu ekonomiki bezpieczeństwa, jako nauki szczegółowej o różnych aspektach bezpieczeństwa ekonomicznego, jak

C. Nardinelli, *Ekonomia,* Fundacja gospodarcza NZSS „Solidarność", Gdańsk 1991, s. 82.

[10] L. F Korzeniowski,. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych,* EAS, Kraków 2008.

i praktycznych zadaniach dla bezpieczeństwa ekonomicznego. Praktyka przekłada się również na zarządzanie kryzysowe na szczeblu krajowym oraz realizowanym przez samorządy terytorialne.

2. Bezpieczeństwo gospodarki morskiej

Konsekwencją przytoczonych wyżej nowych uwarunkowań wzrostu i rozwoju są drastyczne zmiany w gospodarce morskiej kraju. Gospodarka morska obejmuje różnorodne dziedziny gospodarowania związane z wymianą międzynarodową drogą morską, realizowaną w obszarze działania portów morskich przez żeglugę morską, przemysł stoczniowy i portowy, rybołówstwo morskie, administrację morską.

Bezpieczeństwo gospodarki morskiej to bardzo szeroki obszar badań. Od czysto ekonomicznych (handlowych, finansowych, transportowych) przez zagadnienia ochrony środowiska do problemów obrony wybrzeża. ile polityka morska zajmuje się *kreśleniem wizji i strategii działań*,[11] to gospodarka morska *spełnia rolę dyspozycyjno-koordynacyjną*, dotyczy bieżącej działalności polegającej na pozyskiwaniu niejako „z morza" zasobów, ich przetwarzaniu i podziale. Ograniczanie gospodarki morskiej do strefy przybrzeżnej byłoby błędne. Niezwykle ważne, bowiem dla jej rozwoju, (głównie portów) są połączenia transportowe z przedsiębiorstwami z głębi kraju, których produkty można transportować drogą morską dzięki sprawnie funkcjonującym portom. Poza tym, biorąc pod uwagę rybołówstwo, rozwój transportu spowodował, że w przetwórstwie ryb nadmorska lokalizacja straciła znaczenie. Połowa firm umiejscowiona jest poza pasem nadmorskim. Taka sama sytuacja odnotowujemy w relacjach między surowcem krajowym i z importu. W połowie przetwarzamy surowiec sprowadzany jest zza granicy[12]. W sytuacji zagrożenia kryzysem oraz unijnymi limitami połowów, stan ten się pogarsza.

Procesy restrukturyzacji, w efekcie których, obserwuje się sprzedaż najważniejszych jej ogniw – podmiotów gospodarczych przemysłu stoczniowego naruszają bezpieczeństwo ekonomiczne gospodarki morskiej. Bezpieczeństwo to można zdefiniować jako *zdolność regionów*

[11] Szerzej o strategiach w wojewódzkich: T. Białas, *Interesariuszy jako partnerzy w strategicznym zarządzaniu regionem,* [w:] T. Białas, (red.), „Dylematy i wyzwania współczesnego zarządzania organizacjami publicznymi", WSAiB, Gdynia 2007, s. 65-74.

[12] P. Rot, *Ryby płyną do Unii*, w: „Pomorski Przegląd Gospodarczy", IBnGR, Gdynia, 2/2000.

*nadmorskich do wykorzystania istniejących regionalnych zasobów pracy, kapitałowych i rzeczowych, a także uwarunkowa*ń *międzynarodowych do niezagrożonego ich rozwoju oraz wzrostu udziału w produkcie narodowym.* W ujęciu ogólnym chodzi o brak zagrożenia oraz brak poczucia zagrożenia realizowanych procesów gospodarczych.

Dobra koniunktura, której potwierdzeniem był portfel zamówień dla przemysłu stoczniowego przypadała ostatnio na lata 2000-2001. Niestety zmiany cen na rykach światowych wpłynęły na spadek rentowności polskich stoczni. Konkurencyjność gwarantowały tylko stocznie remontowe. Nie pomogły fundusze UE. Pomoc publiczna dla tego przemysłu przekroczyła przyjęte standardy, a poza tym kłóciła się z zasadą konkurencyjności. W przekształconych przedsiębiorstwach państwowych finansowanie działalności inwestycyjnej powinno być oparte na środkach własnych. W zaistniałej sytuacji – kryzys branży stoczniowej, nadzieję mogły budzić zapisy programu transport i gospodarka morska, który, wobec nowych uwarunkowań, również musi podlegać procesom walidacji.

Marek Grzybowski już w 1992 roku zwracał uwagę na upadek rybołówstwa bałtyckiego i dalekomorskiego, pozbawionego dostępu do wydajnych łowisk; na zatory płatnicze i rosnące wciąż długi. Przestrzegał przed pogarszającą się kondycją stoczni, co było związane między innymi odstąpieniem rządu od dotowania gwarantowanych wcześniej kontraktów eksportowych oraz wstrzymaniem płatności przez armatorów budżetowych.[13] Był to okres, w którym południowokoreański i japoński przemysł stoczniowy przechwycił 60% światowego rynku dzięki protekcjonizmowi państwowemu. Jeśli nawet w krajach EWG tamtego okresu ograniczano dotacje do produkcji stoczniowej, to nie dotyczyło to okrętów i statków krajów słabiej rozwiniętych.[14]

Alarmujące również były komunikaty zamieszczane nawet codziennej w prasie, już w roku 2002, np. „Naszego Dziennika" cyt „(…)Polskie statki starzeją się, maleje liczba morskich połowów, pracę traci coraz więcej osób. Liczba zatrudnionych w gospodarce morskiej spadła w latach 1993-2000 o 16 procent, a połowy ryb spadły o połowę w ciągu 10-ciu lat. Wiąże się to zdaniem autora z ogromnym importem ryb, odławianych przez inne kraje. Wyraźnie spadł też potencjał

[13] M. Grzybowski, J. Tomaszewski, *Obronne aspekty funkcjonowania gospodarki morskiej* w: „Budownictwo okrętowe i gospodarka Morska", Wyd. Okrętownictwo i Żegluga, Gdańsk 2/1992.
[14] *Ibidem*.

rybackiej floty dalekomorskiej. Od połowy lat 90-tych inwestycje w gospodarce morskiej wyraźnie wzrosły, ale po 1999-roku zostały poważnie ograniczone. Ponad 77 procent statków morskich i przybrzeżnych wykazuje najwyższy stopień zużycia. (…)".[15] Potwierdzają to bieżące dane statystyczne: na 121 statków o łącznej nośności 2482 tys. DWT., 65 to statki o ponad dwudziestojednoletniej wysłudze. „(…) W niedługim czasie polscy armatorzy będą zmuszeni do wymiany swej floty, aby utrzymać się ma rynku. Los polskich stoczni jest jednak zagrożony pod względem finansowym. Także polscy armatorzy są wypierani z rynków przez tak zwane "tanie bandery" (…)".[16] Potencjał ludzki Województw Pomorskiego oraz Zachodniopomorskiego, najmocniej związanych z gospodarką morską – tylko w miastach, które zamieszkują 20-tys. i więcej mieszkańców, to ponad 10% ludności zamieszkującej w takich miastach w Polsce (tabela 1).

Tab. 1.
Powierzchnia i ludność miast liczących w 2007 20 i więcej tys mieszkańców w rejonie nadbrzeżnym (województwa Pomorskie i Zachodniopomorskie)

Województwo	Powierzchnia w km^2	Ludność w tys.
Pomorskie	**670**	**1101,6**
Zachodniopomorskie	**815**	**813,5**
Razem	**1485**	**1915,1**
Ogółem ludność miast, liczących w 2007 20 i więcej tys. mieszkańców:	**18383,7**	

Źródło: opracowanie własne J. T., na podstawie Rocznik statystyczny Rzeczypospolitej Polskiej, Główny Urząd Statystyczny, ZWS, Warszawa 2008, s. 198 – 200.

Wykorzystanie tego potencjału, szczególnie w miastach portowych zmniejsza się o czym świadczą: spadek przewozów ładunków transportem morskim według zasięgów pływania oraz wiek morskiej floty transportowej – tabela 2.
Informacje za lata 2000-2007 zawarte w tabeli2 wskazują, że kryzys polskiej floty rozpoczął się niezależnie od koniunktury światowej. Poza

[15] „Nasz Dziennik", z 07.01 2002, http://wiadomosci.onet.pl/437529,10,item.html
[16] *ibidem.*

tym na 121 statków floty transportowej, 65 to statki z ponad dwudziestoletnią wysługą.

Tab. 2.
Przewozy ładunków transportem morskim w latach 2000 – 2007 (stan na 31 XII)

Wyszczególnienie	2000	2005	2006	2007	Spadek 2007/2000
Przewozów ładunków transportem morskim według rodzajów żeglugi i zasięgów pływania, łącznie (w tys. t.)	22774	9362	10021	11432	49,8%
Przewozów ładunków transportem morskim według rodzajów żeglugi i zasięgów pływania, łącznie (w milionach tonomili)	72167	17134	17203	15432	78,6%

***Źródło**: opracowanie własne J. T., na podstawie Rocznik Statystyczny Rzeczypospolitej Polskiej, Główny Urząd Statystyczny, ZWS, Warszawa 2008, s. 530 – 531.*

Korzystne trendy można odnotować w przewozie ładunków, w morskich portach handlowych, w tym ładunków tranzytowych, pomimo spadków odnotowanych w latach 2005-2006 w portach: Kołobrzeg, Police, Szczecin oraz w latach 2006-2007 w portach: Gdańsk, Kołobrzeg, Police, Szczecin, Świnoujście – tabela 3.

Tab. 3.
Przeładunki w morskich portach handlowych w latach 2000 – 2007 (w tys. t.)

Porty	2000	2005	2006	2007	Wzrost/-spadek 2007/2000
Gdańsk	16712	24163	24207	21201	26%
Gdynia	8397	12294	14183	17510	110%
Kołobrzeg	116	173	158	118	1,72%
Police	2481	2619	2446	2384	-4%
Szczecin	11110	10002	9965	9572	-14%
Świnoujście	8942	10018	9242	9153	2,4%
Ogółem	**47758**	**59279**	**60201**	**59938**	**25,5%**

Źródło: opracowanie własne J. T., na podstawie Rocznik Statystyczny Rzeczypospolitej Polskiej, Główny Urząd Statystyczny, ZWS, Warszawa 2008, s. 531.

Funkcjonowanie gospodarki morskiej generuje zewnętrzne koszty społeczne w postaci zanieczyszczenia środowiska. Dla ograniczenia tych kosztów podejmuje się działania właściwe wybranym podmiotom gospodarki morskiej

3. Bezpieczeństwo ekologiczne a gospodarka morska

Nadzór nad procesami ochrony środowiska morskiego na polskich obszarach morskich Bałtyku sprawują urzędy morskie. Koncentrują on swoją działalność na przeciwdziałaniu zanieczyszczeniom wytwarzanym: ze statków, ze źródeł lądowych, z prac pogłębiarskich, z eksploatacji dna, z układania kabli i rurociągów. Jedną z form ochrony środowiska morskiego jest odbiór nieczystości statkowych w portach, w skład których wchodzą: wody zaolejone, ścieki, odpady bytowo-gospodarcze, pozostałości ładunkowe, wody balastowe. Zachętą do zdawania nieczystości jest wprowadzenie organizacji ich odbioru, na zasadzie "bez pobierania szczególnej opłaty". Taki system, obejmujący odbiór wód zaolejonych, funkcjonuje między innymi w portach Darłowo, Kołobrzeg, Łeba i Ustka. Za zdawanie pozostałych nieczystości zapłatę pobiera prowadzący usługę odbioru.

To do zadań Urzędów Morskich należy uzgadnianie i wydawanie pozwoleń wodno-prawnych na wprowadzanie do morza ścieków ze źródeł lądowych m.in. poprzez kanalizację ścieków oczyszczonych, których wylot znajduje się bezpośrednio w morzu. Przykładem takich oczyszczalni są między innymi: Oczyszczalnia Ścieków Grzybowo oraz Zakład Płyt Wiórowych „Alpex Karlino". Inne źródła zanieczyszczeń to np. Stacja Utylizacji Wód Zaolejonych w Ustce.

Odkładanie do morza urobku z pogłębiania dna portów i red podlega procedurze zezwoleń. Wydanie zezwolenia uwarunkowane jest między innymi stanem czystości materiału dennego i osadów, pod względem zawartości substancji szkodliwych dla środowiska morskiego. Wykaz substancji oraz dopuszczalna ich zawartość, przy której można urobek odłożyć do morza znajduje się w załączniku do konwencji helsińskiej o ochronie środowiska Morza Bałtyckiego. Ilość urobku przeznaczonego do zatopienia określa się na podstawie badań batymetrycznych wykonywanych podczas sondaży dna. Tylko część urobku trafia do morza, zaś część odkładana jest również na brzeg.

Na dnie Bałtyku odkryto wiele surowców mineralnych: ropę naftową, gaz ziemny, kruszywa (żwir, piaski), bursztyn i minerały ciężkie. Ropa naftowa i gaz ziemny występują wzdłuż południowo-wschodnich

wybrzeży Bałtyku, na głębokościach od 2 do 6 kilometrów. Poszukiwania ropy wykazały, że najbardziej obiecujące złoża znajdują się w polskiej strefie ekonomicznej w rejonie na północ od Rozewia, gdzie w 1980 roku stanęła pierwsza platforma wiertnicza na Bałtyku. Ropie naftowej towarzyszą złoża gazu. W polskiej strefie odkryto 4 złoża, których potencjał wynosi od 7,5 do 10 mld m^3. Kontrola czystości wód morskich wokół wież prowadzona jest miedzy innymi poprzez obserwacje powierzchni morza z samolotów.

Na dnie morza kryją się również znaczne zasoby materiałów budowlanych: głazów, żwirów, otoczaków i piasków. Są one eksploatowane głównie przez Danię, Szwecję, Finlandię i Łotwę. W polskiej strefie Morza Bałtyckiego znaczne ilości materiałów budowlanych znaleziono na Ławicy Słupskiej, Ławicy Odrzańskiej i w okolicy Koszalina. Prace przygotowawcze do podjęcia eksploatacji przemysłowej na Ławicy Słupskiej trwają 2006. Należy podkreślić, że pozyskiwanie tych surowców z dna morskiego musi podlegać ostrym rygorom bezpieczeństwa, gdyż intensywne prace wydobywcze naruszają równowagę ekologiczną i mogą doprowadzić do zniszczenia cennych zespołów fauny i flory. Przestrzeganie warunków ochrony środowiska polega na ustaleniu obszaru eksploatacji, określeniu ilości kruszywa jaką można wydobyć oraz innych warunków wykonywania prac.

Na dnie Bałtyku układane są między innymi kable i rurociągi. W ostatnim okresie położono np. kabel światłowodowy z Bornholmu do Kołobrzegu oraz kabel energetyczny Szwecja – Polska, wychodzący na ląd w rejonie Ustki i biegnący dalej pod ziemią do stacji przemiennikowej w Wierzbięcinie koło Bierkowa, a stąd linią napowietrzną do sieci energetycznej. Trasę przebiegu kabli na pełnym morzu uzgodniono z Ministrem Transportu i Gospodarki Morskiej, zaś na morzu terytorialnym oraz w pasie nadmorskim z Dyrektorem Urzędu Morskiego w Słupsku. Na obszarze morza terytorialnego oraz pasa nadmorskiego uzgodnienie takie dokonywane jest w drodze decyzji o warunkach zabudowy i zagospodarowaniu terenu. Odrębną dziedziną ochrony środowiska morskiego jest zapobieganie i zwalczanie zanieczyszczeń olejowych na morzu.

Nadzór nad działaniami mającymi na celu zwalczanie zagrożeń i zanieczyszczeń morza, prowadzonymi przez kapitana statku i armatora, sprawują urzędy morskie. Dokonują one oceny sytuacji w celu ustalenia rodzaju i stopnia zanieczyszczenia morza lub zagrożenia zanieczyszczeniem. Biorąc pod uwagę rodzaj i stopień zagrożenia oraz

sposób wykonywania działań przez kapitana lub armatora, urzędy morskie mogą polecić prowadzenie tych działań Służbie SAR (Search and Rescue) lub innej wyspecjalizowanej jednostce. W przypadku, gdy istnieje możliwość zanieczyszczenia brzegu morskiego albo zagrożenia życia lub zdrowia ludności w rejonie nadmorskim, niezwłocznie powiadomiony zostaje wojewoda oraz wojewódzki inspektor ochrony środowiska, którzy maja obowiązek podjęcia odpowiednich działań zapobiegawczych na lądzie.

Gdy krajowe środki do przeprowadzenia skutecznej akcji zwalczania zanieczyszczenia, okażą się nie wystarczające, istnieje możliwość zwrócenia się o pomoc do państw stron Konwencji Helsińskiej. W sytuacji zanieczyszczenia morza przez statek urzędy morskie mają obowiązek niezwłocznie podjąć czynności w celu wykrycia sprawców i zabezpieczenia dowodów. W celu zapobieżenia, usunięcia lub ograniczenia poważnego i bezpośredniego zagrożenia dla polskich wybrzeży, minister właściwy ds. gospodarki morskiej może wydać decyzję o zastosowaniu na polskich obszarach morskich, w stosunku do polskich statków, niezbędnych środków, łącznie z zatopieniem lub zniszczeniem statku.

4. Współpraca międzynarodowa dla bezpieczeństwa gospodarki morskiej

Niebezpieczeństwa i zagrożenia interesów europejskich wymagają kontroli zgodności z morskimi zasadami bezpieczeństwa przeprowadzanych przez władze portowe, poprawienia sprawności i niezawodnego zarządzania ruchem statków. Wiąże się to z likwidacją rozbieżności między systemami prawnymi w poszczególnych państwach członkowskich oraz wdrożenia międzynarodowych instrumentów takich jak kod ISPS.[17] W monitoringu wód UE stosuje się wiele różnych metod: nadzór prowadzony z lądu, obserwacje lotnicze i satelitarne oraz systemy śledzenia statków. Dalsza integracja w tej dziedzinie przyniosłaby dodatkowe korzyści. Zapobieganie niebezpieczeństwom i zagrożeniom mogłoby być skuteczniejsze dzięki działaniom usprawniającym wymianę

[17] W grudniu 2002 roku w Londynie odbyła się Konferencja Dyplomatyczna, której tematem była Ochrona Bezpieczeństwa Morskiego. Przyjęła Międzynarodowy Kodeks Ochrony bezpieczeństwa Statków oraz Obiektów i Urządzeń Portowych (Kodeks ISPS), w celu zidentyfikowania i zapobiegania aktom zagrażającym bezpieczeństwu w sektorze transportu morskiego. www.isps.org.

informacji między państwami członkowskimi, funkcjonowaniu wspólnych zespołów dochodzeniowo śledczych oraz wzmocnienia ochrony najważniejszych elementów infrastruktury w UE.

Zapewnienie bezpieczeństwa na morzu wymaga współpracy międzynarodowej. UE współpracuje z USA w ramach inicjatywy dotyczącej bezpieczeństwa kontenerów(CSI),[18] wprowadzonej po atakach terrorystycznych z dnia 11 września 2001 r.

W celu poprawienia skuteczności reakcji na poważne zagrożenia przekraczające krajowe możliwości reagowania, UE przyjęła dwa wnioski legislacyjne, mające wzmocnić wspólnotowy mechanizm ochrony ludności. W celu zapobiegania wypadkom na morzu i zagrożeniom wynikającym z zanieczyszczenia oraz reagowania na nie, Europejska Agencja Bezpieczeństwa Morskiego (EMSA) pomaga państwom członkowskim w przypadku wypadków powodujących zanieczyszczenie środowiska. Innym ważnym faktorem jest dostępność danych, które pomogą organom publicznym monitorować działania gospodarcze na terenie wód przybrzeżnych. W szczególności potrzebne są lepsze informacje o bieżącym ruchu statków. Informacje takie są nie tylko ważne dla nawigacji, ale mogą być również wykorzystywane do wykrywania działalności przestępczej: przemytu, handlu żywym towarem, działań terrorystycznych czy nielegalnych zrzutów ze statków. Wymiana informacji związanych z bezpieczeństwem i ochroną na szczeblu europejskim odbywa się między właściwymi organami poprzez system SafeSeaNet[19] (opracowany przez Komisję i obsługiwany przez EMSA).

Podkomitet do spraw Radiokomunikacji oraz Poszukiwań i Ratownictwa (COMSAR) IMO ustanowił system identyfikacji i śledzenia dalekiego zasięgu (LRIT) statków i ich pozycji przy wykorzystaniu danych satelitarnych, który może być zarządzany przez regionalne ośrodki danych. Na szczeblu UE taki system regionalny powstaje na podstawie istniejącego systemu SafeSeaNet. Systemy te w coraz większym stopniu będą wykorzystywane zarówno przez

[18] Umowa między UE, a USA o intensyfikacji i rozszerzeniu Umowy o współpracy celnej i wzajemnej
pomocy w sprawach celnych, w celu włączenia współpracy w zakresie bezpieczeństwa kontenerów i kwestii powiązanych (Dz.U. poz. 304 z 30.9.2004).

[19] SafeSeaNet – Wspólnotowy system wymiany informacji morskiej utworzony przez Komisje Europejska we współpracy z Państwami Wspólnoty w celu wdrożenia właściwych Wspólnotowych regulacji prawnych w zakresie bezpieczeństwa i ochrony żeglugi oraz ochrony środowiska morskiego.

wojskowych, jak i cywilnych użytkowników. Koncepcja polega na dążeniu do integracji istniejących systemów, umożliwiającej dostarczanie dla określonego odcinka wybrzeża informacji z różnych źródeł w połączeniu z informacjami z nowych źródeł, takich jak Galileo[20] i systemy obserwacyjne Ziemi z przestrzeni kosmicznej. W wodach UE dodatkowym wymogiem będzie pełna kompatybilność różnych systemów i sektorów w państwach członkowskich. Systemy takie będą musiały zostać utworzone we współpracy z państwami sąsiadującymi z UE. Stopień integracji funkcji rządowych dotyczących wód terytorialnych i wyłącznych stref ekonomicznych różni się pomiędzy państwami członkowskimi. W niektórych przypadkach, indywidualny organ władzy (straż przybrzeżna, policja lub siły zbrojne) jest odpowiedzialny za prawie wszystkie funkcje. W wielu państwach akcje poszukiwawczo-ratownicze, kontrola celna, kontrola graniczna, inspekcja rybołówstwa i kontrole w zakresie ochrony środowiska powierzane są różnym organom władzy. Zwiększenie koordynacji tych działań, jak również działań państw członkowskich, mogłoby pomóc w dalszej integracji i sprzyjać większej skuteczności. W UE istnieją już przykłady podejścia zintegrowango geograficznie. Agencje UE powstały w takich obszarach jak bezpieczeństwo morskie (EMSA), kontrola granic zewnętrznych (FRONTEX – Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej)[21] i kontrola rybołówstwa. Prawodawstwo przyjęte w tych sektorach zachęca państwa członkowskie do współpracy w niektórych działaniach kontrolnych i egzekucyjnych. Pomiędzy państwami członkowskimi oraz agencjami UE istnieje ścisła współpraca. W sprawach celnych propozycje stworzenia elektronicznego środowiska celnego i zmodernizowanego kodeksu celnego zachęcą do dalszej integracji..

W odpowiedzi na postępujący proces zanieczyszczania środowiska morskiego Bałtyku w ramach środków zapobiegawczych opracowano i wcielono w życie wiele konwencji międzynarodowych. Zasadniczo dzielą się one na międzynarodowe porozumienia o zasięgu globalnym i regionalnym. Trzy konwencje bezpośrednio dotyczą zagadnień

[20] GALILEO – europejski system nawigacji i łączności satelitarnej zob. D. Iwen, *Wielokryterialne porównanie systemów nawigacji satelitarnej,* praca dypl. AMW Gdynia, 2005, niepublikowana.

[21] www.europa.eu.int/agencies/community_agencies/frontex/index_en.htm

związanych z ochroną środowiska morskiego przed zanieczyszczeniami pochodzącymi ze statków podczas ich normalnej eksploatacji. Są to:

- Międzynarodowa konwencja o zapobieganiu zanieczyszczaniu morza przez statki 1973 i Protokół 1978 (MARPOL 73/78);
- Konwencja o zapobieganiu zanieczyszczaniu morza przez zatapianie odpadów i innych substancji 1972 (LC 1972);
- Konwencja o ochronie środowiska morskiego obszaru Morza Bałtyckiego – Konwencja Helsińska 1974 oraz nowa Konwencja Helsińska 1992.

Konwencja MARPOL 73/78 jest aktem prawnym o zasięgu globalnym, regulującym sprawy zapobiegania zanieczyszczaniu mórz przez statki. Zakres konwencji obejmuje wszystkie zagadnienia techniczne zawiązane z ograniczeniem zanieczyszczania morza przez statki za wyjątkiem zatapiania odpadów i innych substancji. Dotyczy statków wszystkich typów oraz platform wiertniczych. Nie ma zastosowania do zanieczyszczeń będących następstwem badań i eksploatacji dna morskiego oraz złóż położonych pod dnem.

Na skutek wprowadzenia w życie postanowień działającego w ramach Konwencji Komitetu (MEPC), dokonano wielu znaczących działań w zakresie zmian konstrukcyjnych statków, ich wyposażenia, organizacji postępowania z odpadami, ograniczeniu emisji do atmosfery substancji kontrolowanych oraz tlenków azotu (NO_X) i siarki (SO_X). W wyniku tych działań Bałtyk został uznany jako obszar kontroli emisji tlenków siarki. Zapoczątkowano również inicjatywy, które dały początek dla prac nad Konwencją dotyczącą przenoszenia szkodliwych organizmów w wodach balastowych oraz wyznaczania Szczególnie Wrażliwych Obszarów Morskich. Te dwie inicjatywy są szczególnie ważne dla regionu Morza Bałtyckiego. Bałtyk ze względu na stosunkowo niskie zasolenie wód przejawia znaczną podatność na obce gatunki inwazyjne przenoszone w wodach balastowych z innych rejonów świata. Natomiast, w związku z ekologicznymi, ekonomicznymi, kulturowymi, naukowymi i edukacyjnymi walorami akwenu bałtyckiego, na wniosek wszystkich nadbałtyckich państw europejskich **(**z wyjątkiem Rosji**)**, postanowiono ochronić jego środowisko przed degradacją w wyniku rosnącego natężenia międzynarodowego transportu morskiego, poprzez uznanie go za Szczególnie Wrażliwy Obszar Morski (PSSA). Jest to bardzo pilna sprawa, ponieważ ilość samej ropy transportowanej tylko

przez Zatokę Fińską zwiększyła się w ciągu niespełna 10 lat o 200%. Inną bardzo istotną dla ochrony środowiska inicjatywą było objęcie zakazem stosowania farb przeciwporostowych zawierających związki cynoorganiczne.

Konwencja o zapobieganiu zanieczyszczaniu morza przez zatapianie odpadów i innych substancji, sporządzona w Londynie w 1972 roku, uzupełnia obszar działań chroniących środowisko morskie, wyznaczonych przez Konwencję MARPOL 73/78. Wyznaczyła również wskazania do opracowania Załącznika V Konwencji Helsińskiej.

Konwencja o ochronie środowiska morskiego obszaru Morza Bałtyckiego zwana Konwencją Helsińską podpisana w 1974 roku, odnosi się do regionu Morza Bałtyckiego i poddaje kontroli wszystkie rodzaje zanieczyszczeń.

W 1992 roku przyjęto tzw. Nową Konwencję Helsińską. Zawiera ona 7 Załączników, a podstawowe zmiany w stosunku do Konwencji z 1974 roku odnoszą się do następujących zagadnień:

- do obszaru obowiązywania Konwencji włączono wody wpływające do Bałtyku;
- wprowadzenia wymagań dotyczących określenia szczegółowych kryteriów i środków dla ochrony środowiska Bałtyku, stosowania zamkniętych systemów wodnych w zakładach przemysłowych oraz wydawania zezwoleń zakładom przemysłowym na odprowadzanie ścieków;
- dołączenia listy substancji chemicznych, dla których wprowadzono całkowity zakaz używania lub dopuszczono używanie w ograniczonym zakresie.

W ramach Komisji Helsińskiej (HELCOM), która jest powołanym przez Konwencję Helsińską organem koordynującym, podjęto działania w celu opracowania programów i środków służących ochronie gatunków i siedlisk, które zostały rozpoznane jako zagrożone, zanikające lub wymagające ochrony. Za ważne narzędzie tej pracy zostały uznane morskie obszary chronione (BSSA). Celem jest zbudowanie do 2010 r. spójnej ekologicznie sieci dobrze zarządzanych morskich obszarów chronionych i utrzymanie jej na Morzu Bałtyckim. Pierwsze 62 obszary chronione Morza Bałtyckiego zostały zaproponowane w 1994 r. w ramach Zalecenia HELCOM 15/5 dotyczącego systemu przybrzeżnych i morskich obszarów chronionych Morza Bałtyckiego. Obecnie baza danych HELCOM dotyczących obszarów chronionych Morza Bałtyckiego zawiera informacje o 97 terenach stanowiących

w większości tereny Natura 2000 chronione zgodnie z Dyrektywami „Siedliskową" i „Ptasią" WE.

Ustawodawstwo UE ma na celu ochronę środowiska naturalnego za pośrednictwem „Dyrektywy Siedliskowej" (Dyrektywa Rady 92/43/EWG) i gatunków za pośrednictwem Dyrektywy Ptasiej (Dyrektywa Rady 79/409/EWG).

W obu mowa jest o tworzeniu obszarów chronionych jako środka ochrony. W przypadku ich ustanowienia tworzą one wspólnie sieć znaną jako Natura 2000. Obie dyrektywy zostały zastosowane w środowisku obszarów przybrzeżnych i morskich. Ponadto należy uwzględniać przepisy UE dotyczące jakości wód wpływających do Bałtyku oraz określające dopuszczalne wartości emisji substancji szkodliwych. Do priorytetowych, w tym względzie, należy zaliczyć Ramową Dyrektywę Wodną (2000/60/EC), Dyrektywę o Oczyszczaniu Ścieków Komunalnych (91/271/EWG), Dyrektywę o Azotanach (91/676/EWG) i Dyrektywę dotyczącą wprowadzania do obrotu środków ochrony roślin (dot. m.in. pestycydów) (91/414/EWG). Sprawy ograniczenia emisji substancji kontrolowanych reguluje Rozporządzenie Parlamentu Europejskiego i Rady Europy o substancjach zubożających warstwę ozonową (EC N^{o} 2037/2000). Natomiast Dyrektywa 1999/32/EC określa wymagania w odniesieniu do zawartości siarki w paliwach.

Sytuacja na morzach wydaje się zmierzać w kierunku „wspólnej przestrzeni morskiej UE", rządzonej tymi samymi regułami dotyczącymi bezpieczeństwa i ochrony środowiska. Mogłoby to doprowadzić do zwiększonej efektywności w zarządzaniu wodami terytorialnymi i wyłącznymi strefami ekonomicznymi przez państwa członkowskie i sprawić, że żegluga przybrzeżna znalazłaby się w tej samej sytuacji co transport lądowy między państwami członkowskimi. Miałoby to konsekwencje dla kabotażu w ramach międzynarodowych negocjacji handlowych. Państwa członkowskie nie mają już innej możliwości - przy realizacji niektórych unijnych i ponadgranicznych celów muszą ze sobą współpracować. Znacząca jest ekonomia skali, która staje się możliwa poprzez powierzanie przedstawicielom władz zróżnicowanych obowiązków i wykorzystanie aktywów do zróżnicowanych celów. Niektóre państwa członkowskie wyznaczyły wspólne ośrodki koordynacyjne lub przydzieliły obowiązki jednemu organowi władzy, umożliwiając korzystanie z aktywów podlegających różnym organom władzy. Na przykład we francuskim systemie prefektów morskich pojedynczy organ władzy podlegający premierowi ponosi całkowitą

odpowiedzialność za wszystkie działania władz na określonym obszarze wód przybrzeżnych. Holenderska Straż Przybrzeżna jest przykładem innego rodzaju integracji, w której jeden organ władzy dysponuje drogim wyposażeniem koniecznym do zarządzania wodami przybrzeżnymi, takim jak okręty lub statki powietrzne, i udostępnia te aktywa lub świadczy usługi innym organom na życzenie. Wskazuje to, że może istnieć pożyteczna ekonomia skali, osiągnięta dzięki wspólnemu działaniu i wspólnemu dysponowaniu środkami. Potencjalna ekonomia skali na poziomie UE jest znacznie większa. Państwa członkowskie już to uznały, tworząc całą grupę agencji UE. Rosnąca konieczność identyfikowania, zatrzymywania i osądzania osób zaangażowanych w przemyt, handel ludźmi, nielegalne rybołówstwo, nielegalną imigrację i terroryzm wskazują na pilną konieczność koordynacji istniejących krajowych zasobów i wspólne nabycie nowych. Ocena Agencji FRONTEX pozwoli ustalić, czy agencja ta powinna ściślej współpracować ze służbami celnymi i innymi organami władzy w sprawach bezpieczeństwa dotyczących towarów.

Konwergencja technologii cywilnych i wojskowych, w szczególności przy prowadzeniu obserwacji morza, powinna również pomóc zredukować podwajanie zasobów. Warto również ponownie zbadać możliwość udostępnienia funduszy na działania kontrolne w tych państwach członkowskich, które stanowią najważniejsze „furtki" dla rynku wewnętrznego. Obecny system nie odzwierciedla niewspółmiernego obciążenia niektórych państw członkowskich w zakresie kontroli granicznych.

5. Sektor obronny a bezpieczeństwo gospodarki morskiej

Praktyka wielokrotnie udowodniła, że skuteczny System Obronny Państwa (SOP) jest istotnym warunkiem bezpieczeństwa każdego społeczeństwa i rozwoju gospodarki. W skład tego systemu wchodzą poza podsystemem kierowania obronnością, podsystemy pozamilitarny i militarny. Zależności pomiędzy bogactwem danego kraju, a poziomem wydatków przeznaczonych na obronę nie są stałe. Ich poziom zależał od poziomu napięć polityczno militarnych w Europie i świecie. W ślad za zmianami w jakie dokonały się u schyłku XX wieku, zmianie uległa rola sił zbrojnych RP., w tym Marynarki Wojennej RP (MW RP), w systemie bezpieczeństwa państwa. Dotyczy to również to utrzymania bezpieczeństwa naszych portów i statków.

Przystąpienie Polski do NATO w 1999 roku przełożyło się na nowe zadania MW RP nowych zadań wynikających ze zobowiązań sojuszniczych, z których znacząca cześć jest bezpośrednio związana *z* bezpieczeństwem w portach oraz statków (okrętów w strefie obrony MW RP). Także wzrost zaangażowania Polski na arenie międzynarodowej, związany z przystąpieniem do koalicji antyterrorystycznej, przyniósł w ostatnich pięciu latach zwiększenie zaangażowania sił MW RP w tym obszarze.

Działalność operacyjna sił MW RP prowadzona w strefie obrony i obszarze operacyjnego zainteresowania MW RP jest podstawową sferą aktywności MW RP mającej wpływ na utrzymanie bezpieczeństwa portów i statków. Jest realizowana tak w czasie pokoju jak i kryzysu. Do lej sfery należy także zaliczyć wszystkie działania o charakterze obronnym w odniesieniu do zagrożeń bezpieczeństwa realizowane w ramach narodowego i sojuszniczego systemu bezpieczeństwa. Do sfery tej zaliczymy miedzy innymi:

- udział w ratowaniu życia w polskiej strefie ratownictwa SAR utrzymywanie śmigłowców i okrętów w dyżurach w gotowości do działania na wezwanie;
- zapewnienie bezpieczeństwa żeglugi na polskich obszarach morskich a w tym: eskortowanie statków o dużym ryzyku zagrożenia, NCAGS,[22] utrzymywanie krajowego systemu informacji nautycznej i ostrzeżeń nawigacyjnych, opracowywanie map morskich i publikacji;
- wsparcie Straży Granicznej w ochronie morskiej granicy państwowej i polskiej strefy ekonomicznej;
- demonstrowanie obecności morskiej w strefie zainteresowania państwa (32,8 tys. km^2 Wyłącznej Strefy Ekonomicznej i ponad 140 tys. km^2 obszaru zainteresowania państwa);
- realizacja zadań HNS (Host Nation Suport). czyli wsparcia państwa gospodarza na rzecz sił sojuszniczych realizujących zadania na terytorium RP, a w tym; ochrona portów i jednostek sojuszniczych znajdujących się w portach;
- przeciwdziałanie zorganizowanej przestępczości w zakresie: penetracji ochranianych obiektów, środków bojowych i materiałów wybuchowych;
- udział w ochronie ekologicznej polskich obszarów morskich;

[22] NCAGS (Naval Co-Operation And Guidance For Shipping) Wojskowa Współpraca i Doradztwo dla Żeglugi, szerzej www.ncags.com.

- utrzymywanie w gotowości i wydzielanie słi MW RP do stałych zespołów NATO oraz UE zgodnie ze zobowiązaniami RP;
- utrzymanie wysokiej gotowości bojowej i mobilizacyjnej do realizacji zadań osłony operacyjnej morskiej granicy państwa i polskich obszarów morskich;
- przygotowywanie sił do realizacji zadań w czasie wojny.

Do działań reagowania kryzysowego prowadzonych w kraju i na polskich obszarach morskich w ramach wsparcia instytucji cywilnych (administracji rządowej, samorządowej) w przypadku wystąpienia sytuacji kryzysowych mogących potencjalnie mieć związek z szeroko pojętym bezpieczeństwem portów, obiektów i aglomeracji przyległych oraz statków, zaliczymy szereg działań wydzielonych sił Marynarki Wojennej RP, w tym:

- obrona przed terroryzmem, a w tym do; ochrony obiektów i osób, neutralizacji niebezpiecznych środków oraz akcji przeszukiwania i izolowania terenów zagrożonych działaniami terrorystycznymi, działań specjalnych;
- zapobieganie i likwidacja skutków klęsk żywiołowych związanych z pożarami przestrzennymi, powodziami i zatorami lodowymi, tąpnięciami i osunięciami ziemi oraz huraganami i anomaliami pogodowymi takimi jak obfite opady atmosferyczne;
- akcje ratowniczo-gaśnicze;
- likwidacja skutków katastrof awarii technicznych: obiektów przemysłowych i instalacji morskich, drogowych, kolejowych, lotniczych oraz likwidacji skutków awarii technicznych z toksycznymi środkami przemysłowymi (TŚP) i wypadków radiacyjnych;
- oczyszczanie terenu z przedmiotów wybuchowych i niebezpiecznych;
- akcje poszukiwawczo-ratowniczych w ramach Systemu Poszukiwania i Ratownictwa SAR;
- działania przeciwepidemicznych.

Warto nadmienić, że poza tymi działaniami, siły MW mogą być także wykorzystane do wsparcia działań sił porządkowych w przypadku wprowadzenia stanu wyjątkowego na zasadach określonych w odrębnych przepisach

Przedstawione zadania wynikają z konieczności ochrony interesów Polski na Morzu Bałtyckim, z którym związany jest, tzw. Eurobałtycki

Region Funkcjonalny. W regionie tym leży 9 państw zamieszkałych prze ok. 145 mln. ludności. Każde z nich chroni własnych interesów, a jednocześnie niemalże wszystkie ze sobą współpracują, np. w dziedzinie ochrony ekologicznej. Poza tym udział tego regionu w wymianie handlowej wszystkich państw europejskich wynosi 20%. Na Polskę przypada 15 % powierzchni akwenu, zaś ludność stanowi 26% ludności państw leżących nad tym akwenem[23]. Jest zatem kogo i czego bronić.

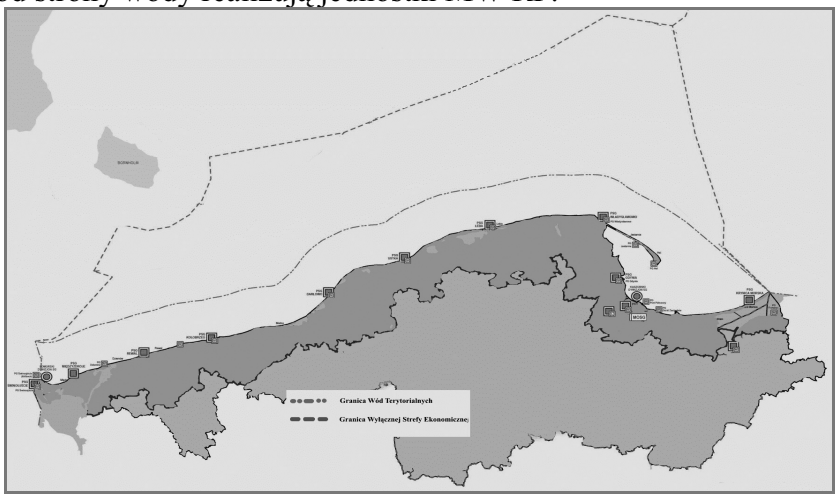
Biorąc pod uwagę fakt usytuowania portów wojennych i cywilnych, ze wspólnymi torami wodnymi, podejściami, wzajemnym wykorzystywaniem nabrzeży oraz współistnienie w tym środowisku dwóch podsystemów ochrony opierających się na zbliżonych założeniach i stworzonych w celu przeciwdziałania podobnym zagrożeniom, logicznym wydaje się konieczność współdziałania i wzajemnej koordynacji działań, jeżeli nie stworzenia wspólnego systemu ochrony, co z pewnością pozwoliłoby na zwiększenie efektywności działania i wykorzystania sił. Powyższe odnosi się w szczególności do ochrony portów od strony wody oraz zagrożeń nawodnych i podwodnych. Ogromnego znaczenia w tym kontekście nabiera współdziałanie i współpraca MW RP ze Strażą Graniczną (MOSG). Z racji uwarunkowań prawnych to właśnie Straż Graniczna dysponuje właściwymi instrumentami prawnymi szczególnie w obszarze wód wewnętrznych i terytorialnych. Te instrumenty oraz posiadane wyposażenie przystosowane do działania na akwenach przybrzeżnych i wewnątrz portów powodują, że Morskiemu Oddziałowi Straży Granicznej jest przypisana wiodąca rola w zakresie ochrony portów. Marynarka Wojenna RP, zgodnie z posiadanymi zadaniami, spełnia rolę wspierającą.

W polskich obszarach morskich można wyodrębnić trzy strefy i przypisać w nich następujące zadania oraz role:

- Strefa zewnętrzna (WSE */EEZ/* Strefa Obrony MW RP) – główne zadania: rozpoznanie i monitorowanie; wiodąca rola MW RP;
- Strefa przybrzeżna (wody terytorialne 12 Mm) – główne zadanie – przechwytywanie; wiodąca rola MOSG, wspierająca MW RP;
- Strefa wewnętrzna (wody wewnętrzne, porty, tory wodne) – główne zadanie to ochrona bezpośrednia; wiodąca rola MOSG, wspierająca

[23] M. Karpiński, *Zagrożenia interesów Polski na Morzu w czasie pokoju, kryzysu i wojny*, w: „Przegląd Morski" nr 2 z 2002 r.

MW RP, wewnątrz portów wojennych ochronę bezpośrednią od strony wody realizują jednostki MW RP.



Rys. 1. Terytorialny zasięg działania Morskiego Obszaru Straży Granicznej
Źródło: opracowanie własne na podstawie www.morski.strazgraniczna.pl/mapa.htm

Wejście w życie „ustaw granicznych" oraz ustawy o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej z dnia 21 marca 1991 r. doprowadziło do zmiany istniejącego systemu ochrony morskiej granicy państwa. Poszerzono go o zadania mające na celu ochronę interesów ekonomicznych i ekologicznych na polskich obszarach morskich. Ważna rola w zapewnieniu bezpieczeństwa naszym rodakom oraz odwiedzającym Polskę gościom, w zakresie infrastruktury materialnej, a mówiąc szerzej bezpieczeństwa państwa, spoczywa na urzędach państwowych, agencjach, inspekcjach i profesjonalnych służbach. Do takich wyspecjalizowanych instytucji należy również Morski Oddział Straży Granicznej. Osiemnaście lat temu, kiedy tworzono Straż Graniczną nie formułowano jeszcze planów instytucjonalnego włączenia Polski w struktury europejskie. Podjęto tylko działania mające na celu gruntowną zmianę istniejącego dotąd systemu ochrony granicy państwowej. Była one odpowiedzią na przemiany polityczno-ustrojowe zachodzące w Polsce i państwach Europy Środkowowschodniej oraz na gwałtowny wzrost przestępczości granicznej, szczególnie o podłożu migracyjnym. W późniejszym jednak czasie poglądy elit politycznych na bezpieczeństwo Polski i jej miejsce w Europie ewoluowały w kierunku NATO oraz wspólnot europejskich.

Z chwilą wstąpienia do Unii Europejskiej, Polska przyjęła odpowiedzialność nie tylko za skuteczną ochronę granicy państwowej naszego kraju i zapewnienie na niej bezpieczeństwa, ale także za duży, liczący blisko 1500 km, jej odcinek granicy zewnętrznej. Istotną rolę w realizacji tych zadań dla gospodarki morskiej spełnia dziś Morski Oddział Straży Granicznej im. płk. Karola Bacza. Rzeczpospolita Polska dokonała szeregu zmian nie tylko w prawodawstwie „granicznym", ale także i całym systemie zarządzania ochroną granicy państwowej.[24]

Ochraniana przez funkcjonariuszy MOSG granica morska liczy 440 km (z czego 395,3 km na 12-milowej granicy wód terytorialnych – długość linii brzegowej polskiej części Bałtyku wynosi 524 km). Ponadto działania oddziału obejmują: 29,5 km odcinek granicy z Republiką Federalną Niemiec na Zalewie Szczecińskim oraz 11,3 km odcinek z Federacją Rosyjską na Zalewie i Mierzei Wiślanej. Ogółem funkcjonariusze MOSG ochraniają 481,3 km, tj. ok. 15% całkowitej długości granicy RP. Natomiast terytorialny zasięg działalności oddziału obejmuje: polskie obszary morskie o powierzchni 36 724 km^2 oraz 60 nadmorskich gmin, które tworzą strefę nadgraniczną. Głównymi zagrożeniami występującymi na morskim odcinku granicy między innymi są:

Morski Oddział Straży Granicznej, jako jedna z 14 jednostek organizacyjnych Straży Granicznej (12 oddziałów i 2 ośrodki szkolenia), realizuje zadania w ochronie granicy państwowej w oparciu o następujące graniczne jednostki organizacyjne:

- 13 placówek w: Elblągu, Krynicy Morskiej, Gdańsku, Gdańsku - Rębiechowie, Gdyni, Władysławowie, Łebie, Ustce, Darłowie, Kołobrzegu, Rewalu, Międzyzdrojach i Świnoujściu;
- 2 dywizjony (Kaszubski Dywizjon SG w Gdańsku i Pomorski Dywizjon SG w Świnoujściu).[25]

Zakończenie

Zaprezentowany rozdział nie wyczerpuje bogatej tematyki dotyczącej roli bezpieczeństwa w stabilizacji i rozwoju gospodarki morskiej. Nie zamyka również procesu badawczego w rozważanym zakresie. W opracowaniu

[24] Plan działania w zakresie wdrożenia dorobku prawnego Schengen w Polsce. *(Poland – Schengen Action Plan), lipiec 2003, www.mswia.gov.pl*

[25] G. Goryński, *MOSG na drodze do Unii Europejskiej*, „Przegląd Morski" 2003 nr 10, s. 9-10.

wykazano, że negatywne zjawiska w gospodarce morskiej pojawiły się już w latach dziewięćdziesiątych minionego stulecia, zatem niezależnie od groźby kryzysu w gospodarce światowej. Za szczególne dotkliwe uznano osłabienie pozycji polskiego transportu morskiego oraz kryzys branży stoczniowej. Permanentny rozwój transportu morskiego, narastające zagrożenia naturalnego środowiska morskiego przemawiają za intensywną współpracą regionalną w rejonie Morza Bałtyckiego. W tym względzie pozytywnie należy ocenić realizację zadań związanych z kontrolą i inspekcją na morzu, dotyczących zapewnienia bezpieczeństwa żeglugi, ochrony środowiska morskiego oraz eksploatacji i ochrony jego zasobów.

Ograniczeniem o charakterze organizacyjnym bezpieczeństwa gospodarki morskiej jest rozproszenie jego elementów składowych systemu bezpieczeństwa w różnych ośrodkach administracji państwowej (Ministerstwo Infrastruktury, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Ochrony Środowiska). Wskazuje to na brak jednego, wyraźnie określonego ośrodka koordynacyjnego systemu oraz ścisłego podziału zadań. Ograniczenie to obejmuje zwalczanie zagrożeń terrorystycznych, rozproszenie zadań kontroli żeglugi (Ministerstwo Infrastruktury) oraz ochrony obszarów morskich (Morski Oddział Straży Granicznej – MSWiA). Aktualne rozwiązanie jest nieefektywne – nie jest ono uzasadnione ani logicznie, ani operacyjnie, a także ekonomicznie z uwagi na konieczność finansowania kilku struktur.

Bibliografia

Druki zwarte

1. Białas T., (red.), „Dylematy i wyzwania współczesnego zarządzania organizacjami publicznymi", W S A i B, Gdynia 2007.
2. Grzybowski M., J Tomaszewski (red.), *Bezpieczeństwo w administracji i biznesie*, WSA i B Gdynia 2007.
3. Kamerschen D. R.,. McKenzie R. B, Nardinelli C., *Ekonomia,* Fundacja gospodarcza NZSS „Solidarność", Gdańsk 1991.
4. Korzeniowski L., Pepłoński A., *Wywiad gospodarczy. Historia i współczesność, EAS,* Kraków 2005.
5. Korzeniowski L. F,. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych,* EAS, Kraków 2008.

6. Kuźniar R., Lachowski Z., (red.), *Bezpieczeństwo międzynarodowe czasu przemian. Zagrożenia- Koncepcje – Instytucje*, Państwowy Instytut Spraw Międzynarodowych, Warszawa 2003
7. *Regulamin działań MW RP,* Gdynia 2003.
8. Rocznik statystyczny Rzeczypospolitej Polskiej, Główny Urząd Statystyczny, ZWS, Warszawa 2008

Materiały niepublikowane

Iwen D., *Wielokryterialne porównanie systemów nawigacji satelitarnej,* AMW Gdynia, 2005.

Periodyki

1. Grzybowski M., Tomaszewski J., *Obronne aspekty funkcjonowania gospodarki morskiej* [w:] „Budownictwo okrętowe i gospodarka Morska", Wyd. Okrętownictwo i Żegluga, Gdańsk 2/1992.
2. Goryński G, *MOSG na drodze do Unii Europejskiej*, „Przegląd Morski" 2003 nr 10.
3. Kaganek K., *Przygotowanie oferty dla osób niepełnosprawnych,* Materiały szkoleniowe z zakresu funkcjonowania biur podróży, Ministerstwo Gospodarki i Pracy, Nowosądecka Organizacja Turystyczna, Warszawa 2004.
4. Kaganek K., *Psychologia pracy w turystyce z osobami niepełnosprawnymi,* w: „Tworzenie i dostosowywanie produktów turystycznych do potrzeb osób niepełnosprawnych", Forum Turystyki Regionów, Szczecin 2007.
5. Kaganek Krzysztof R. Korzeniowski Leszek F.: *Jakość i bezpieczeństwo usług hotelarskich, EAS,* Kraków: 2008.
6. P. Rot, *Ryby płyną do Unii*, w: „Pomorski Przegląd Gospodarczy", IBnGR, Gdynia, 2/2000.
7. M. Karpiński, *Zagrożenia interesów Polski na Morzu w czasie pokoju, kryzysu i wojny,* w: „Przegląd
8. Morski" nr 2 z 2002 r.

Strony internetowe

1. www.europa.eu.int/agencies/community_agencies/frontex/index_en.htm-
2. www.isps.org
3. http://wiadomosci.onet.pl/437529,10,item.html

4. www.mswia.gov.pl Plan działania w zakresie wdrożenia dorobku prawnego Schengen w Polsce. (Poland – Schengen Action Plan), lipiec 2003,

Akty prawne

Umowa między UE, a USA o intensyfikacji i rozszerzeniu Umowy o współpracy celnej i wzajemnej pomocy w sprawach celnych, w celu włączenia współpracy w zakresie bezpieczeństwa kontenerów i kwestii powiązanych (Dz.U. poz. 304 z 30.9.2004).

SECURITY OF MARITIME ECONOMY IN THE FACE OF A THREAT OF THE WORLD ECONOMY CRISIS

Summary

The article presents fundamental problems connected with the security of maritime economy. The maritime security is defined as part of state maritime policy. Basing on statistical examples the authors notice the negative tendencies in maritime economy. They indicate ecological security as an element of security in the Baltic Sea region. The most important international agreements concerning the security of maritime economy are discussed. The authors described the tasks of services and institutions in charge of maritime security including certain links of Polish Defensive System. In conclusion they present the areas and directions of development that currently constitute the prior challenge for the Polish system of maritime security.

Marek Grzybowski*

ROZWÓJ FUNKCJI LOGISTYCZNYCH W PORTACH POLSKICH

Streszczenie

W artykule omówiono rozwój funkcji logistycznych polskich portów jako reakcję na rozwój potrzeb klientów portów oraz zmiany w otoczeniu w regionie Morza Bałtyckiego.

Wprowadzenie

Około53,5 mln mieszkańców regionów położonych nad Bałtykiem stanowi istotne źródło popytu konsumpcyjnego i inwestycyjnego. Funkcjonujące w regionie przedsiębiorstwa i instytucje zapewniają pracę około 25,6 mln osób. Region wytwarza rocznie PKB o wartości około 1400 mld euro[1]. Szybko rosnący popyt krajów skandynawskich i nadbałtyckich został w 2008 r. spowolniony w wyniku światowego kryzysu finansowego. Nie zmienia to jednak faktu, że w regionie coraz więcej się konsumuje i to w dużej mierze towarów z importu. Dodatkowe strumienie ładunków generowane są przez inwestycje podjęte w wyniku napływu środków finansowych z Unii Europejskiej.

2. Zmiany w otoczeniu polskich portów

Na początku tego wieku wyraźnie zaznaczył się trend szybkiego napływu ładunków w kontenerach oraz przewozów ro-ro. W portach położonych nad Bałtykiem powstają nowe terminale kontenerowe, uruchamiane i planowane są kolejne stanowiska do przeładunku ro-ro.

---

* Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.

[1] C. Ketels: The Baltic Sea Region as a Place to Do Business. Baltic Development Forum, Kopenhaga 2007, s. 7.

Rośnie również liczba połączeń żeglugowych, na które wprowadzane są coraz większe i szybsze jednostki.

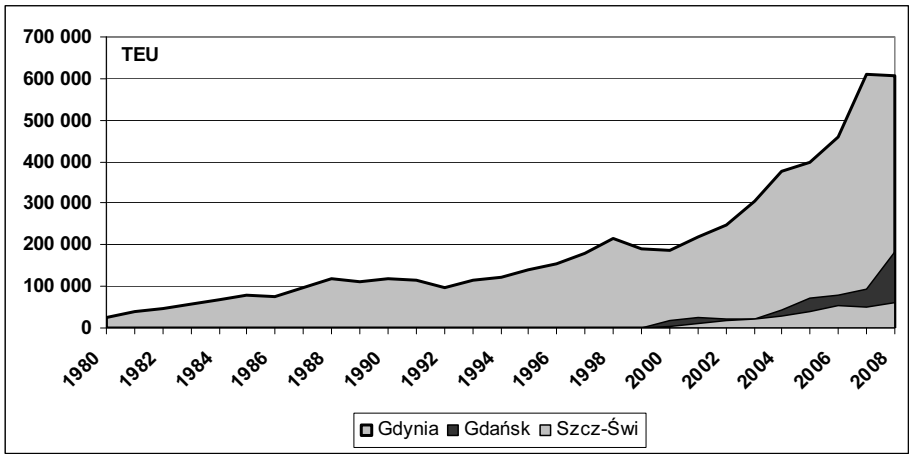
Rocznie w regionie bałtyckim w obrocie wewnętrznym przewozi się morzem około 160 mln ton ładunków. Na Bałtyk wpływa na statkach ponad 60 mln ton towarów, a wywozi się niego ponad 300 mln ton (głównie ropy naftowej). W żegludze regularnej między portami bałtyckimi a europejskimi portami oceanicznymi kilkudziesięciu armatorów utrzymuje ponad 3800 regularnych połączeń. Tylko do nabrzeży portów polskich przybija ponad 17 tys. jednostek rocznie. Coraz więcej wśród nich jest statków z kontenerami i jednostkami ro-ro. W portach bałtyckich przeładowuje się ponad 4 miliony kontenerów rocznie. Każdego roku ich liczba rośnie o około 10%. W 2007 r. w polskich portach przeładowano ponad 760 tys. TEU, a w 2008 r. było prawie 855 tys. TEU[2].

2. Przeładunki kontenerów w polskich portach

Dziś terminale kontenerowe i ro-ro polskich portów dysponują potencjałem przeładunkowym około ponad 2 mln TEU oraz jednostek ładunkowych, a w perspektywie 5 lat ten potencjał ten zwiększy się dwukrotnie. Centra logistyczne stanowić będę niezbędne zaplecze dla szybko rozwijających się morsko-lądowych łańcuchów transportowych.

W portach polskich w latach 2007-2008 roku utrzymała się wysoka dynamika przeładunku kontenerów. Liczba standardowych pojemników w przeładunkach burtowych wzrosła z prawie 506,2 tys. TEU w 2005 r. (449 tys. TEU w 2004 r.) do około 855 tys. TEU. Decydujący wpływ miał ponad 15% wzrost przeładunków w Gdyni, głównie w Bałtyckim Terminalu Kontenerowym, który wciąż jest jednym z liczących się terminali kontenerowych na Bałtyku (rys. 1.). W 2008 r. przeładowano w nim ponad 440,6 tys. TEU. Dobre wyniki osiągnął działający od wiosny 2006 roku Gdynia Container Terminal, w którym przeładowano 167 tys. TEU.

[2] Dane z terminali kontenerowych i zarządów portów z lutego 2009 r.



Rys. 1. Przeładunki kontenerów w portach polskich w latach 1980-2008
Źródło: Dane terminali kontenerowych i zarządów portów ze stycznia 2009.

W Gdańsku w ubiegłym roku w DCT, który rozpoczął działalność w październiku 2007 r. odnotowano wzrost przeładunków kontenerów z około 3,5 tys. TEU do prawie 106,5 tys. TEU, ale w terminalu kontenerowym (GTK) nastąpił spadek obrotów o około 15% (z ponad 91 tys. do prawie około 98 tys. TEU). W Szczecinie ilości kontenerów nie są tak wielkie jak w Gdyni, ale przyrost jest systematyczny. Drobnica-Port Szczecin (obecnie PCC) odnotowała kolejny rok wzrostu przeładowując ponad 38 tys. TEU w 2006 r. i ponad 50 tys. TEU w 2007 r. oraz prawie (obecnie PCC) 62 tys. TEU w 2008 r.

4. Zmiany w infrastrukturze w portach polskich i ich otoczeniu

W otoczeniu konkurencyjnym polskich portów trwają intensywne inwestycje infrastrukturalne. Rozbudowywane jest zaplecze logistyczne. St. Petersburg, Kaliningrad, Kopenhaga, Malmoe, Turku, Trelleborg, Aarhus, Lubeka rozbudowują swoje terminale ro-ro i kontenerowe. Obok nich budowane są centra logistyczne. Od podstaw budują swoje terminale kontenerowe i centra logistyczne Rosja w Ust-Ługa, a Estonia w Sillamäe. Porty bałtyckie starają się nadążyć budując nie tylko terminale o coraz większych możliwościach przeładunkowych, lecz również intensywnie inwestując w infrastrukturę drogową i transport intermodalny oraz centra logistyczne. W zachodniej części Bałtyku intensywnie inwestują Aalborg i Goeteborg, znacznie zmodernizował swoją infrastrukturę portową Trelleborg, gdzie również zbudowano

nowoczesne centrum logistyczne. W portach wschodniego Bałtyku budowane od podstaw i rozbudowywane są terminale przeładunkowe (kontenerowe i ro-ro) i centra logistyczne w St. Petersburgu, Ust-Łudze, Bałtijsku i Kalingradzie, w Helsinkach i Hanko.

W portach polskich zarządy starają się nadążyć za trendami światowymi i zmianami w infrastrukturze portowej i logistycznej w Regionie Bałtyckim. Doskonalona jest infrastruktura drogowa, modernizowane są nabrzeża i drogi wodne, wymienia się wyposażenie terminali przeładunkowych, unowocześnia się dotychczas funkcjonujące i planuje się nowe terminale. Każdy z zarządów portów zaplanował już na swoim terenie centrum logistyczne.

5. Koncepcje rozwoju funkcji logistycznych w polskich portach

Zachodniopomorskie Centrum Logistyczne w Szczecinie zostało wybudowane porcie szczecińskim na terenie o powierzchni 20 ha. Inwestycja została sfinansowana z Europejskiego Funduszu Rozwoju Regionalnego w ramach Sektorowego Programu Operacyjnego Transport 2004-2006 i została ukończona w 2007 roku. W 2005 r. Zarząd Morskich Portów Szczecin i Świnoujście podpisał umowę z konsorcjum firm Calbud ze Szczecina i Interbud-West z Gorzowa Wlkp. na budowę centrum. W ramach inwestycji przewidziano rozbudowę infrastruktury drogowej i kolejowej. Centrum stanowi naturalne zaplecze terminalu przeładunku kontenerów.

Uzbrojenie i wyposażenie terenu zapewnia potencjalnym operatorom logistycznym możliwość inwestowania na terenach dzierżawionych. Centrum zostało powiązane z infrastrukturą drogową i kolejową. Infrastruktura drogowa połączona jest z ulicą Gdańską poprzez most przez Parnicę z ciągiem komunikacyjnym w kierunku na Dolny Śląsk, Poznań i Warszawę. Odległość do prowadzącej do Niemiec autostrady A6 i międzynarodowej drogi E65 to tylko 8 km. Centrum logistyczne w Szczecinie pozwala na budowę zarówno magazynów niskiego jak i wysokiego składowania oraz chłodnie. Na terenie centrum usytuowano parking dla 40 samochodów ciężarowych. Przewiduje się możliwość funkcjonowania punktów obsługi taboru.

Istotną zaletą projektów na Ostrowie Grabowskim jest to, że Zachodniopomorskie Centrum Logistyczne oraz infrastruktura techniczna bazy kontenerowej są dofinansowywane z Europejskiego Funduszu Rozwoju Regionalnego (ERDF). Ich wartość szacuje się na

około 100 mln zł, z czego jedną trzecią przeznaczono na budowę centrum logistycznego, a pozostałą część na terminal kontenerowy[3].

Gdyńskie Centrum Dystrybucyjno Logistyczne zaplanowano w sąsiedztwie Bałtyckiego Terminalu Kontenerowego, Gdynia Container Terminal oraz Terminalu Promowego obsługującego (m. in. za pomocą dwupoziomowej rampy) połączenie promowe Steny Line Gdyni z Karlskroną. Usytuowane po zachodnie stronie Estakady Kwiatkowskiego, centrum sąsiaduje z Baltic Auto Center (centrum dystrybucji samochodów o zdolności obsługi około 30 tys. pojazdów rocznie) oraz licznymi mniejszymi firmami dystrybucyjnymi[4].

Rys. 2. Planowane centra logistyczne rejonie Gdańska i Gdyni
Źródło: Opracowanie na podstawie mapki Suchman & Wakefield (2008-12-01)

[3] Informacja na podstawie materiałów informacyjnych Zarządu Morskiego Portu Szczecin-Świnoujście, 2009-04-27.
[4] M. Grzybowski: *Port morski– budowanie marki firmy na rynku globalnym B2B (na przykładzie portu w Gdyni)*, [w:] MARKETING PRZYSZŁOŚCI. TRENDY, STRATEGIE, INSTRUMENTY. Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 511. Ekonomiczne Problemy Usług nr 26. Uniwersytet Szczeciński, Szczecin 2008. ISSN 1640-6818 [ISSN 1896-382X], s. 63-70.

Natomiast na północny zachód od centrum, na terenie o powierzchni 7 ha zbudowane zostanie Trefl Logistic Center (TCL) – inwestycja firmy Trefl SA. 1 kwietnia 2008 r. został uruchomiony depot, na którym obecnie składuje się około 200 kontenerów. Obecnie trwają przygotowania do budowy magazynów o powierzchni 2,5 tys. m^2[5]. Na działalność logistyczną i dystrybucyjną w ramach centrum logistycznego zarząd gdyńskiego portu zarezerwował 30 ha. Z chwilą zakończenia budowy autostrady A1, dzięki połączeniu Trasy Kwiatkowskiego z obwodnicą Trójmiasta, gdyńskie centrum logistyczne ma szanse stać się jednym z ważniejszych ogniw krajowego systemu logistycznego. Jego pozycję może wzmocnić uruchomienie w Gdyni lotniska cywilnego z terminalem cargo i miejscami do obsługi „general avition"[6].

Centrum Logistyczno-Dystrybucyjne w Gdańsku usytuowane zostanie na powierzchni 130 ha. Formalna decyzja o lokalizacji centrum logistycznego w porcie gdańskim zapadła w styczniu 2005 r. W Urzędzie Miasta Gdańska podpisane zostało trójstronne porozumienie o współpracy dotyczące projektu i budowy centrum logistyczno-dystrybucyjnego w Porcie Północnym. Obok prezesa portu i prezydenta miasta list intencyjny podpisał prezes Deepwater Container Terminal (DCT) Gdańsk SA. Powierzchnia centrum będzie kilkakrotnie większa od projektowanego terminalu kontenerowego dla którego zarezerwowano 32 ha. Gdańskie centrum logistyczne ma stanowić zaplecze terminalu kontenerowego i ro-ro. Według zapowiedzi kierownictwa DCT terminal ruszy już jesienią tego roku, a w pierwszym roku działalności powinien przeładować 200 tys. TEU, by ciągu kilku lat osiągnąć obroty na poziomie 500 tys. TEU[7].

W maju tego roku do tworzenia centrum włączona została Pomorska Specjalna Strefa Ekonomiczna Sp. z o.o. Planuje się, że Centrum Logistyczno-Dystrybucyjne w Gdańsku będzie miało do dyspozycji ok. 134 ha. Na obszarze (którego właścicielem jest obecnie Gmina Gdańsk) lub jego części ustanowiona zostanie specjalna strefa ekonomiczna w rozumieniu ustawy z 20 października 1994 r. o specjalnych strefach

---

[5] L. Stefaniak: *Logistyka na zapleczu*, dodatek LOGISTYKA 2008, „Namiary na Morze i Handel", październik 2008, s. 10.

[6] M. Grzybowski: *Węzeł lotniskowy dla Kaszub*. PORTY, CARGO, USŁUGI LOTNICZE. Polska Gazeta Transportowa. 2008, 2 lipca 2008, nr 27, s. V.

[7] M. Grzybowski: *Klastry logistyczne jako efekt aktywności regionów zorientowanych marketingowo* [w:] Bałtycki rynek żeglugowy [ISBN: 978-83-60585-09-2], Akademia Morska, Szczecin 2008, s. 11-22.

ekonomicznych. Takie rozwiązanie poprawi na pewno atrakcyjność inwestycyjną w pierwszej fazie tworzenia centrum[8].

O atrakcyjności morsko-lądowych centrów logistycznych decyduje nie tylko ich usytuowanie w portach ale przede wszystkim ich położenie w drożnych korytarzach transportowych. Jeśli od strony morza dostęp do terminali przeładunkowych, a wraz z nimi do centrów logistycznych gwarantuje dostawy ładunków, to od strony lądu korytarze transportowe do portów mają ograniczoną drożność.

Jeszcze ważniejszym czynnikiem decydującym o istotnej roli lądowo-morskich centrów logistycznych w zwiększenia udziału polskich portów i przewoźników morskich w zintegrowanych łańcuchach transportowych w ramach morsko-lądowych łańcuchów dostaw jest rozwinięcie w centrach logistycznych wszystkich funkcji i działań niezbędnych do generowania ładunków zarówno w kierunku połączeń lądowych jak i morskich[9].

6. Podsumowanie

Zwiększona dynamika przewozów ładunków w kontenerach wymusza rozwój funkcji logistycznych w portach polskich. W okresach, gdy drobnica była dostarczana do portów w formie ładunków konwencjonalnych, część funkcji logistycznych wykonywana była w poszczególnych terminalach (składowanie, formowanie kontenerów) lub wyodrębnionych jednostkach działających w porcie i jego otoczeniu (magazyny cytrusów, chłodnie składowe, łuszczarnia ryżu itp.). Obecnie klienci wymagają nowej jakości usług, którą zapewnić mogą działania realizowane w ramach zorganizowanych i sprawnie zarządzanych centrów logistycznych.

[8] M. Grzybowski: *Strategie rozwoju portów i żeglugi na Bałtyku u progu XXI wieku,* [w:] Żegluga i porty morskie w procesie integracji europejskiej (red. Henryk Salmanowicz), Zeszyty Naukowe nr 552, Ekonomiczne Problemy usług nr 7, Uniwersytet Szczeciński, Szczecin 2007 (ISSN 1640-6818, ISSN 1869-382X), s. 65-76.

[9] Zob. M. Grzybowski (kierownik projektu): *Znaczenie lądowo-morskich centrów logistycznych w rozwoju żeglugi bliskiego zasięgu w relacjach z portami polskimi*, Wydawnictwa wewnętrzne Instytutu Morskiego w Gdańsku Nr 6418. Gdańsk 2008, s. 58-70.

Bibliografia

1. Ketels C.: *The Baltic Sea Region as a Place to Do Business*. Baltic Development Forum, Kopenhaga 2007, s. 7.
2. Grzybowski M.: *Port morski – budowanie marki firmy na rynku globalnym B2B (na przykładzie portu w Gdyni)* [w:] MARKETING PRZYSZLOŚCI. TRENDY, STRATEGIE, INSTRUMENTY. Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 511. Ekonomiczne Problemy Usług nr 26. Uniwersytet Szczeciński, Szczecin 2008. ISSN 1640-6818 [ISSN 1896-382X], s. 63-70.
3. Grzybowski M.: *Węzeł lotniskowy dla Kaszub.* PORTY, CARGO, USŁUGI LOTNICZE. Polska Gazeta Transportowa. 2008, 2 lipca 2008, nr 27, s. V.
4. Grzybowski M.: *Klastry logistyczne jako efekt aktywności regionów zorientowanych marketingowo* [w:] Bałtycki rynek żeglugowy [ISBN: 978-83-60585-09-2], Akademia Morska, Szczecin 2008, s. 11-22.
5. Grzybowski M.: *Strategie rozwoju portów i żeglugi na Bałtyku u progu XXI wieku* [w:] Żegluga i porty morskie w procesie integracji europejskiej (red. Henryk Salmanowicz), Zeszyty Naukowe nr 552, Ekonomiczne Problemy usług nr 7, Uniwersytet Szczeciński, Szczecin 2007 (ISSN 1640-6818, ISSN 1869-382X), s. 65-76.
6. Stefaniak L.: *Logistyka na zapleczu,* dodatek LOGISTYKA 2008, „Namiary na Morze i Handel", październik 2008, s. 10.

LOGISTICS FUNCTIONS DEVELOPMENT IN POLISH PORTS

Summary

Author presents in the article perspectives logistics functions development in polish ports as factor of new conditions in trade environment in Baltic Region.

Ilona Jacyna*

WYZNACZANIE PRZEPŁYWÓW TOWARÓW W OBIEKCIE MAGAZYNOWYM SYSTEMU LOGISTYCZNEGO

Wprowadzenie

W okresie kilku ostatnich lat pojęcie systemu logistycznego stało się bardzo popularne i coraz powszechniej używane. W literaturze dotyczącej badań systemowych spotyka się imponującą rozmaitość definiowania terminu „system". Przez językoznawców system określany jest jako [11]:

- zbiór jednostek tworzących pewną całość organizacyjną, służącą jednemu celowi układu;
- sposób, metoda wykonywania jakiejś czynności;
- zasady organizacji, ogół przepisów, reguł obowiązujących, stosowanych w danej dziedzinie według których dane zjawisko jest wykonywane;
- uporządkowany zbiór twierdzeń, poglądów tworzących pewną teorię.

Reasumując powyższe rozważania, można powiedzieć, że za system można uważać celowo określony zbiór elementów o określonych właściwościach oraz relacji pomiędzy tymi elementami i (lub) między ich własnościami [3].

W odniesieniu do tak rozumianego pojęcia systemu można sformułować definicję systemu logistycznego jako celowo zorganizowany i zintegrowany – w obrębie danego układu gospodarczego – zbiór zasad sterujących przepływem materiałów i produktów oraz odpowiadających im informacji umożliwiających optymalizację w zarządzaniu łańcuchami dostaw (m.in. przez automatyczną identyfikację towarów, symulację komputerową, kontroling oraz elektroniczną wymianę danych), [2].

* Studia Doktoranckie Wydział Zarządzania Uniwersytet Warszawski.

J. Fijałkowski [5] definiuje system logistyczny jako podsystem w przedsiębiorstwie, który składa się ze środków pracy, tj. maszyn i ludzi potrzebnych do przekształcenia obiektów, przy czym każdy system logistyczny zawiera w sobie charakterystyczny przepływ informacji.

Natomiast A. Korzeniowski w pracy [8] twierdzi, iż procesy logistyczne koordynują przepływ towarów i informacji na całej ich drodze – od producentów poszczególnych towarów poprzez dystrybucję, aż po utylizację odpadów, względnie kasację nieużytecznych pozostałości.

1. Elementy systemu logistycznego

Aby pojąć zasady rządzące systemem logistycznym, należy zapoznać się z głównymi jego cechami, do których należą [7]:

- wysoki stopień spójności – oznacza, że zmiana w jednym podsystemie pociąga za sobą zmiany w pozostałych podsystemach. Wynika to z faktu, iż poszczególne podsystemy są ze sobą silnie powiązane i od siebie zależne;
- elastyczność – wyraża się reagowaniem na wpływ otoczenia ekonomicznego, otoczenia konkurencji, a w związku z tym podatnością na zmiany cen, podatków, a także poziomu inflacji.

Do głównych zadań systemu logistycznego należą [5]:

- zarządzanie przepływem materiałów i towarzyszących im strumieni informacji, od momentu wydobycia surowca aż do chwili dostarczenia do ostatecznego klienta;
- zminimalizowanie nakładów związanych z przepływami towarów;
- dostosowanie działań w przedsiębiorstwie do wymagań obsługi odbiorców.

Pod pojęciem system logistyczny powinniśmy rozumieć zbiór różnych elementów i relacji między tymi elementami (np. środków technicznych, organizacyjnych i ludzkich zdolnych realizować przepływy towarów między producentami a konsumentami). Do takich elementów należy zaliczyć, m.in. [7]:

- infrastrukturę (np. magazyny, place, parkingi, drogi);
- środki transportowe i urządzenia mechaniczne (np. suwnice, wózki, układnice regałowe, pojazdy);
- urządzenia i środki do sterowania przepływem ładunków (komputery, specjalistyczne oprogramowania);
- wyposażenia niemechaniczne (np. regały, palety);
- wykwalifikowani pracownicy.

Zazwyczaj w obrębie wydzielonego obszaru systemu logistycznego, można wyodrębnić następujące elementy [5]:

- Zaopatrzenie – podsystem ten utworzony jest przez dostawców DS_k, gdzie k=1,2,..,K. Firma pozyskuje kosmetyki od trzech różnych dostawców.
- Magazynowanie – w skład tego podsystemu wchodzą obszary, wraz z ich częścią administracyjną BR_g, w których jest składowany towar. Firma dysponuje jednym magazynem regionalnym w g-tym regionie MR_g, gdzie g=1,2,…,G.
- Transport zewnętrzny – podsystem ten obejmuje czynności związanez przemieszczaniem ludzi, ładunków w przestrzeni, poza terenem zakładów przy wykorzystaniu odpowiednich środków transportu. Zbiór tych środków i towarzyszących im czynności tworzą obszar funkcjonalny transportu zewnętrznego w g-tym regionie TZR_g, gdzie g=1,2,…,G.
- Dystrybucję – podsystem ten obejmuje przepływ towarów z magazynów regionalnych MR_g do ostatecznego nabywcy, a tworzą go punkty sprzedaży detalicznej SD_{hg} dla h=1,2,…,H i g=1,2,…,G.
- Centralę – strefa ta określa główną siedzibę firmy, gdzie podejmowane są główne decyzje dotyczące zarządzania firmą i jej zasobami. Przypadku rozpatrywanej firmy dystrybucyjnej centrala CT znajduje się w pobliżu magazynów regionalnych MR_g.

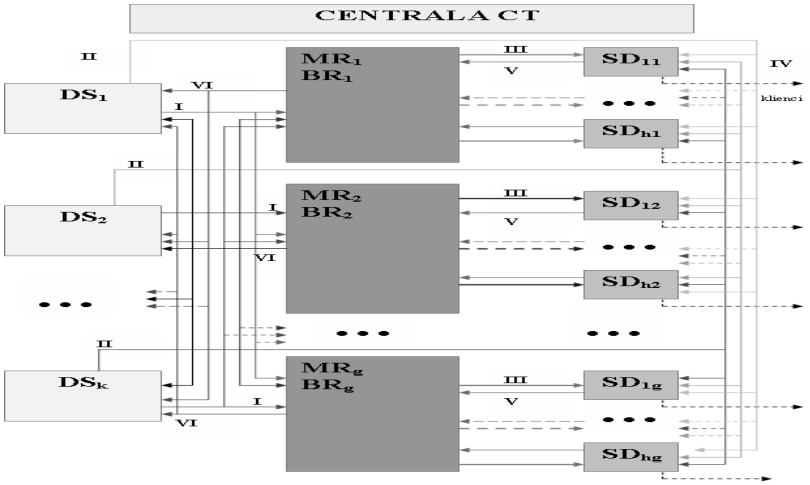
2. Model przepływu ładunków w systemie logistycznym

Model struktury systemu logistycznego natomiast jest graficznym przedstawieniem relacji istniejących pomiędzy obszarami funkcjonalnymi co schematycznie przedstawiłam na rys. 1. Według [5] w systemie logistycznym występują następujące rodzaje relacji transportowych z punktów nadania do punktów odbioru, odnoszących się do dostaw towarów:

- Typ I – transport ładunków od dostawców DS_k do odbiorców MR_g;
- Typ II – transport ładunków od dostawców DS_k do odbiorców SD_{hg};
- Typ III – transport ładunków z magazynów regionalnych MR_g do regionalnych punktów sprzedaży detalicznej SD_{hg};
- Typ IV – jest relacją niesystemową – nie podlega wymiarowaniu (transport indywidualny klientów);
- Typ V – transport ładunków (zwroty i opakowania) z regionalnych punktów sprzedaży detalicznej SD_{hg} do magazynów regionalnych MR_g; liczba relacji typu V w systemie wynosi około 10% relacji typu

III i obejmuje tylko czynności przeładunkowe, gdyż realizowane są w ramach jazd powrotnych;

- Typ VI – transport ładunków (zwroty i opakowania) z magazynów regionalnych MR_g do dostawców DS_k; liczba relacji typu VI w systemie wynosi około 10 % relacji typu I i dalej jak w typie V;
- Typ VII – transport ładunków (zwroty i opakowania) z regionalnych punktów sprzedaży detalicznej SD_{hg} do dostawców DS_k; liczba relacji typu VII w systemie wynosi około 10 % relacji typu II i dalej jak w typie V (nie zaznaczono na rysunku).



Rys. 1. Model graficzny systemu logistycznego firmy z obszarami funkcjonalnymi w postaci bloków DS., MR/BR, SD i strumieni ładunków w TZR

Źródło: [12]

3. Formułowanie zadania logistycznego

Zadanie logistyczne określa zakres przekształceń dokonywanych na strumieniach ładunków. W [5] przedstawiana jest dwuetapowo, tj. etap formułowania oraz etap jego rozwiązania. Formułowanie zadania logistycznego ma na celu uzyskanie odpowiedzi na następujące pytania:

- Co jest przedmiotem transportu?
- Ile towaru zamierzamy przetransportować?
- Skąd towar jest pobierany?
- Dokąd towar będziemy przewozić?
- Kiedy cała transakcja ma nastąpić?

Takie zadanie logistyczne należy sformułować dla obiektu magazynowego pod względem jakościowym jak i ilościowym. Obejmuje ono szereg zadań cząstkowych związanych z przekształceniami strumieni ładunków i związanych z nimi strumieni informacji.

W badanym obszarze magazynowym MR zadanie logistyczne polega na sukcesywnym przekształcaniu strumieni materiałów i związanych z nimi strumieni informacji dostarczanych od dostawców ich transportem do magazynu w strumienie towarów i informacji przeznaczone do sprzedaży. Zazwyczaj dostawcy dostarczają do magazynu towar uformowany w jednostki ładunkowe paletowe jednorodne, natomiast z magazynu towar jest wysyłany zarówno w postaci jednostek ładunkowych paletowych jednorodnych (jłpj), jak i jednostek ładunkowych paletowych skompletowanych (jłpk).

Dodatkowo po wszystkich dostawach zazwyczaj występują zwroty palet. Na przykład przepływ pustych palet (jłpp) może odbywać się z punktów sprzedaży detalicznej do magazynu. Przekształcanie strumieni materiałów zarządzane jest przez strumienie informacji.

Ilościowe ujęcie zadania polega na określeniu warunków brzegowych służących do ukształtowania i zwymiarowania wybranego podukładu systemu logistycznego. Należy w tym momencie określić pewne podstawowe parametry [12]:

- liczba dni roboczych w roku – dr [dni/rok]
- normatyw zapasu – N [dni roboczych]
- przeładunek roczny na wejściu – P^R_{we} [jłpj]
- współczynnik spiętrzeń dobowych na we/wy – $\varphi_{we/wy}$
- stopień komisjonowania – τ
- stopień wypełnienia jłpk – ρ

4. Procedura projektowania systemu logistycznego – określenie zadania logistycznego

Istotnym etapem procedury projektowania obiektu magazynowego w systemie logistycznym jest rozwiązanie zadania logistycznego. W procedurze projektowania systemów logistycznych określa się go jako etap ukształtowania i zwymiarowania. Może on dotyczyć całego systemu bądź wybranego obiektu (podukładu) systemu logistycznego. W artykule szczegółowej analizie został poddany tylko jeden z wielu podukładów systemu logistycznego, a mianowicie wybrany obiekt magazynowy znajdujący się w strefie magazynów regionalnych MR systemu

logistycznego. Dla zwymiarowania badanego obiektu należy sformułować zadanie logistyczne, ale zanim to nastąpi powinno się określić pewne wskaźniki, którymi są [12]:

- Liczba nominalna godzin pracy w roku na zmianę – g_0 [h]
- Liczba zmian pracy w ciągu doby – l_z
- Współczynnik zmiany obszaru pracy – φ_{zo}
- Współczynnik wykorzystania czasu pracy – φ_{tz}
- Współczynnik gotowości technicznej – φ_{gt}
- Wskaźnik kosztów utrzymania wyposażenia niemechanicznego – $\gamma_{W.}$
- Wskaźnik kosztów utrzymania elementów stałych – γ_B
- Wskaźnik amortyzacji urządzeń – α_1
- Wskaźnik oprocentowania kapitału – α_2
- Wskaźnik kosztów przeglądów i napraw urządzeń – γ_{TT}
- Wskaźnik kosztów zakładowych – γ_{Kz}
- Struktura średniej jłpk – w x p [wiersze x pozycje]

Zadanie logistyczne polega na sukcesywnym przekształcanie strumieni ładunków oraz związanych z nimi strumieni informacji dostarczanych przez dostawców DS_k do bazy magazynowej BR-MR_g oraz sieci punktów sprzedaży detalicznej (SD_{hg}) według złożonych wcześniej zamówień, w strumienie informacji i towarów przeznaczonych do sprzedaży w sieci SD_{hg} przy minimalnych kosztach.

Po określeniu powyższych danych można obliczyć liczbę jednostek ładunkowych paletowych jednorodnych, jaka może być składowana w magazynie, [4]:

$$Z_p = \frac{P_{WE}^R \cdot N}{d_r} \quad \text{(jłpj)} \tag{1}$$

gdzie:

Z_p – zapas w magazynie liczony w jednostkach ładunkowych paletowych jednorodnych (jłpj),

P_{WE}^R – przepływ jłpj przez magazyn w ciągu roku (jłpj/rok),

N – normatyw zapasu liczony w dniach;

Na podstawie danych (rodzaj i postać materiałów przeznaczonych do magazynowania) należy uformować jednostki ładunkowe paletowe (np. paleta płaska drewniana o wymiarach 1200x800x130 mm, masie 25 kg). Dla każdego rodzaju magazynowanych materiałów należy zaprojektować jednostki ładunkowe w zależności od postaci opakowań.

Dostarczane opakowania jednostkowe należy odpowiednio zabezpieczyć na palecie przed uszkodzeniami, np. poprzez owinięcie folią termokurczliwą lub stretch. Dodatkowo w celu uniknięcia uszkodzeń asortymentów puste przestrzenie wewnątrz kartonowych opakowań zbiorczych powinny być wypełniane polipropylenowymi woreczkami wypełnionymi powietrzem lub też specjalnym wypełniaczem (celulozowym lub polipropylenowym).

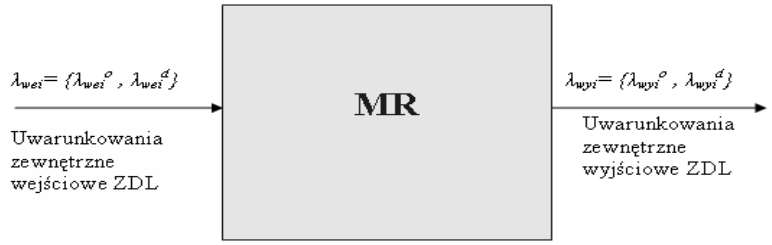
Po zdefiniowaniu warunków brzegowych można przystąpić do określenia wartości dobowych przepływów ładunków w rozpatrywanym obszarze MR_1[12]. Dla bardziej przejrzystego uwidocznienia przepływów wydzielono dwa bloki badanego obszaru – wejścia i wyjścia.

Blok wejścia do magazynu:

$$\lambda_{We}^{D} = \frac{P_{We}^{R}}{dr} \cdot \varphi_{We} \tag{2}$$

Dla obliczonych strumieni wejściowych można stworzyć schemat zadania logistycznego, z uwzględnieniem dobowych przepływów.

$\lambda_{wei} = \{\lambda_{wei}^{o}, \lambda_{wei}^{d}\}$ dla i = 1, 2, …, p $\lambda_{wyi} = \{\lambda_{wei}^{o}, \lambda_{wyi}^{d}\}$ dla i = 1, 2, …, r



Rys. 2. Schemat zadania logistycznego w zakładzie dystrybucyjnym z dobowym zestawieniem strumieni wejściowych i wyjściowych do/z MR

Źródło: opracowano na podstawie schematu zawartego w [5], str. 174.

gdzie:

λ^{i}_{we} – i-ty strumień materiałów na wejściu;

λ_{wyi} – i-ty strumień materiałów na wyjściu;

λ^{o} – opis jakościowy strumienia materiałów;

λ^{d} – opis ilościowy strumienia materiałów;

Blok wyjścia z magazynu

Wartości przepływów jednostek ładunkowych paletowych jednorodnych i skompletowanych **w dobie szczytowej** oblicza się na podstawie niżej zamieszczonych wzorów [5].
Liczba jednostek ładunkowych paletowych na wyjściu z magazynu:

$$\lambda_{Wy}^{D} = \frac{P_{We}^{R}}{dr} \cdot \varphi_{Wy} \tag{3}$$

Liczba jednostek ładunkowych paletowych wychodzących z magazynu w postaci jednostek jednorodnych:

$$\lambda_{Wy(j)}^{D} = \lambda_{Wy}^{D} \cdot (1 - \tau) \text{ jłpj} \tag{4}$$

Liczba jednostek ładunkowych paletowych jednorodnych przeznaczonych do kompletacji:

$$\lambda_{Wy(j->k)g}^{D} = \lambda_{Wy}^{D} \cdot \tau \text{ jłpj/k} \tag{5}$$

Liczba jednostek ładunkowych paletowych wychodzących z magazynu w postaci skompletowanej:

$$\lambda_{Wy(k)}^{D} = \lambda_{Wy}^{D} \cdot \frac{\tau}{\rho} \text{ jłpk} \tag{6}$$

Roczne przepływy jednostek ładunkowych paletowych jednorodnych oraz skompletowanych na wyjściu z magazynu zostały obliczone wg następujących wzorów:

$$P^{R}_{wy} = (\lambda^{D}_{Wy} \cdot d_r)/\varphi_{Wy} \text{ (jłpj/rok)} \tag{7}$$

gdzie:
P^{R}_{wy} – przepływ roczny na wyjściu w jłpj+jłpk;

$$P^{R}_{jłpj} = (1 - \tau) \cdot P^{R}_{WY} \text{ (jłpj/rok)} \tag{8}$$

gdzie:
$P^{R}_{jłpj}$ – przepływ roczny w jłpj,
τ – stopień komisjonowania,

$$P^{R}_{jłpk} = (\tau \cdot P^{R}_{WY})/\rho \text{ (jłpk/rok)} \tag{9}$$

gdzie:
$P^{R}_{jłpk}$ – przepływ roczny jłpk,
ρ – stopień wypełnienia jłpk.

Przyjmując, że zwracane są wszystkie puste palety oraz że są one formowane w jednostkę ładunkową paletową składającą się z 11 pustych palet ułożonych jedna na drugiej to liczba zwrotów pustych palet z punktów sprzedaży detalicznej do magazynów regionalnych w ciągu

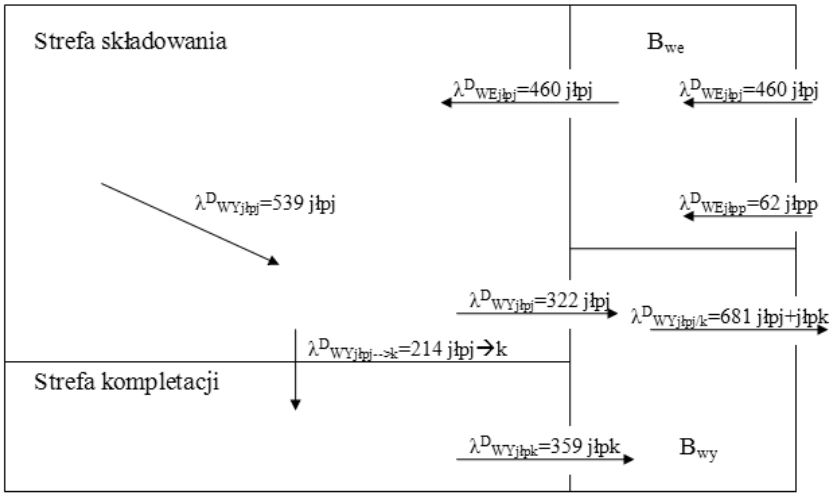
roku ($P^R_{jłpp}$) obliczamy ze wzoru (10) natomiast w ciągu doby szczytowej ($P^D_{jłpp}$) ze wzoru (11):

$$P^R_{jłpp} = P^R_{wy} / 11 \quad \text{(jłpp/rok)} \tag{10}$$

$$P^D_{jłpp} = (P^R_{jłpp} \cdot \varphi_{wy}) / d_r \quad \text{(jłpp/dobę)} \tag{11}$$

Na podstawie dobowych przepływów jednostek ładunkowych obliczyć można strukturę dostaw i wysyłek. Dla przykładu przy założeniu, że przepływ roczny na wejściu do magazynu będzie wynosił 107520jłp i przepływ towarów będzie się odbywał od czterech dostawców poprzez magazyn regionalny MR_1 do czterech odbiorców obliczono przepływ roczne i dobowe (w dobie szczytowej oraz średniej) przepływy jednostek ładunkowych paletowych jednorodnych, skompletowanych i pustych pomiędzy poszczególnymi elementami podsystemu.

Na podstawie poczynionych obliczeń można opracować model graficzny wybranego obszaru z uwzględnieniem przepływów dobowych. Model ten schematycznie (z uwzględnieniem przepływów dobowych między poszczególnymi strefami) będzie prezentował się jak na rys. 3.



Rys. 3. Model graficzny magazynu z podziałem na strefy
Źródło: [12].

Struktura dostaw i wysyłek w omawianym obszarze dobowych miarodajnych przepływ palet na wejściu i na wyjściu magazynu kształtuje się zatem następująco:

λ_{WE}^{D} = 460 jłpj + 62 jłpp,

λ_{WY}^{D} = 322 jłpj + 359 jłpk.

W ciągu doby przyjeżdża 24 samochody z jłpj i jłpk oraz 4 samochody z jłpp.

Podsumowanie

Na podstawie przedstawionego podejścia do obliczania przepływów towarów w obiekcie magazynowym można wyznaczyć wartości przepływów jednostek ładunkowych paletowych między poszczególnymi strefami badanego obiektu. Pomocne jest to przy wymiarowaniu obiektów magazynowych różnych branż.

Wyznaczone wielkości przepływów stanowią również podstawę do obliczania niezbędnych kosztów oraz nakładów, jakie należy ponieść, projektując magazyn, przy zadanych warunkach brzegowych.

Bibliografia

[1]. Abt S., *Logistyka ponad granicami*, Biblioteka Logistyka, Poznań 2000.

[2]. Burnewicz J., *Centra logistyczne jako brakujące ogniwa polskiego systemu transportowego*, Materiały Konferencji Naukowo-Technicznej, Centra logistyczne dla obsługi transportu towarowego. SITK, Poznań 4-5 czerwca 1996.

[3]. Falkiewicz W., *Cybernetyka Ekonomiczna* PWE, Warszawa 1989.

[4]. Fijałkowski J., *Technologia magazynowania*, Oficyna Wyd. PW, Warszawa 1995.

[5]. Fijałkowski J., *Transport wewnętrzny w systemach logistycznych*, Oficyna Wyd. PW, Warszawa 2003.

[6]. Fijałkowski J., *Wybrane zagadnienia projektowania centrów logistycznych w Polsce*, „Logistyka', nr 1/2001, Poznań 2001.

[7]. Jacyna M., *Uwarunkowania techniczne kształtowania centrów logistycznych*,Oficyna Wyd. PW, z. 57, Warszawa 2006.

[8]. Korzeniowski A., *Dystrybucja towarów częstego zakupu*, ILiM, Poznań 1996.

[9]. Krawczyk S., *Metody ilościowe w logistyce*. C. H. Beck, Warszawa 2001.

[10]. Mindur L., *Założenia teoretyczne do organizowania Centrów Logistycznych w Polsce. materiały konferencji naukowo-technicznej* pt. „Centra Logistyczne na Mazowszu", Warszawa 9 października 2003.

[11]. Młynarski S., *Elementy teorii systemów i cybernetyki*, Warszawa 1979

[12]. Praca magisterska pt. „Ocena wariantów projektowych systemu logistycznego na przykładzie centrum logistycznego", Jacyna Ilona, WT PW, Warszawa 2008.

[13]. Rutkowski B., Beier F.J., *Logistyka*. SGH, Warszawa 2004.

[14]. Skowronek C., Saryusz-Wolski Z., Logistyka w przedsiębiorstwie, PWE, Warszawa 1995.

DETERMINING MATERIAL FLOWS FOR WAREHOUSE IN LOGISTIC SYSTEM

Summary

Article presents technical forming of selected logistics system component that is warehouse. In the first part the material flow between functional areas of logistic system are presented. Part second provides logistics task. Paper aims in presenting the ways of determining material flows volumes through warehouse object.

Nebojša Bogojević
Zlatan Šoškić*

VEHICLE DESIGN IN FUNCTION OF SAFETY AND SECURITY OF GOODS IN RAILWAY TRANSPORT

Introduction

It is usually considered that the main drivers of processes of design of railway vehicles are theirs technical (speed, load, energy consumption etc.) and functional (comfort of passengers, ability to adapt to transported goods etc.) characteristics. While security of transported goods is certainly one of aspects considered during design of railway vehicle, it was rarely the case that security aspect was considered as main reason for development of new model or reconstruction of present type of a railway vehicle.

However, nowadays, when challenges to security are increased due to rise of terrorism and, what can be expected, rise of criminal, as consequence of global economic crisis, security aspects are gaining increased attention, and may be the sole reason for changes in design of railway vehicles, and one of more important market requests that is considered by customers. It means that, in conditions of economic crisis, railway vehicles manufacturers should recognize that fact and try to react in an adequate manner so as to keep or improve their market position.

The fact of increased importance of security aspect of railway transport is of particular importance for freight wagons manufacturers, because it is usually considered that the price of freight wagon is the only determining factor that is influencing choice of customers, which, on the other side, restrains manufacturers from investing in research and development in area of freight wagon design. Recognition of importance of security aspects in contemporary environment should lead to increased research in respective area, enabling manufacturers to respond to market requests for more secure freight wagons.

This paper presents an overview of state of security aspect in design of railway vehicles and an example of development of design of freight

* Autorzy są pracownikami University of Kragujevac.

wagons for car transport that was lead by increased requests of Balkan market for security of transported goods as main reason for design changes.

1. Security aspect of design of railway vehicles

Contemporary tendencies of development in transport comprise complying with relevant standards in quality, safety and security. It holds also for railway transport, but, due to immense influence of tradition and heritage in this area, different regulations, different levels of economic development and different levels of application of international standards lead to differences in achieved level of security in railway transport in various European countries.

Security aspects in railway transport comprise today protection against terrorist attacks, security of passengers and goods, security concerning transport of dangerous materials and actions of specialized teams in cases of accidents in transport[1] [2]. As a consequence of increased number of terrorist attacks during the last decade, the attention in transport security was devoted to that aspect. In railway transport, it leads to introduction of anti-terrorist units and teams (Behavior Detection Officers, VIPR Teams Enhance Security at Major Local Transportation Facilities), and development of new security procedures (Employees screening, recommended security action items for the rail transportation of materials poisonous by inhalation, Access Control Security Practices, En-Route Security Practices etc).

All aforementioned measures and activities are to be organized and carried out by railway transport operators or security services. However, theirs successful implementation may be supported by proper design of vehicles, which is responsibility of manufacturers.

The scope and solutions of security-related requests during the design of railway vehicle depend on the kind of the vehicle, being different for locomotives, passenger wagons and freight wagons, but all of them basing on similar security strategy principles[3]:

- Limit the ability to place or hide explosives on or under vehicle;

[1] Safety, Security, Health and Environment Law, Michael Tooma, Federation Press, Australia (2008).
[2] Transportation, Security, Administration, http://www.tsa.gov
[3] Transit Security Design Considerations, US Department of Transportation, http://transit-safety.volpe.dot.gov.

- Improve the ability to see into and out of vehicle;
- Reduce the damage that would result from an explosion;
- Reduce the damage that would result from a fire;
- Reduce the damage that would result from contaminants;
- Enhance emergency egress through doors and windows;
- Protect the driver from physical threat;
- Network the vehicle with the OCC;
- Enable communications between the vehicle operator and passengers;
- Secure the vehicle from theft/unauthorized operations.

These principles affect the design of passenger compartments (doors, windows, seats, ceiling, lighting, public information systems, emergency systems and equipment), operator compartments (door controls, communication systems, train control equipment) as well as the design of car bodies in general.

The solutions that are developed to satisfy the requests are numerous, and, considering large number of railway vehicles present in operation, it is not only important what are the costs of implementation of some security solution in vehicle design, but also if the solutions can be applied to present vehicles or they can be applied only in process of production of new vehicles.

2. Development of design of car transport wagons

As an illustration of railway vehicle design driven by security demands, here will be presented process of changes of design of freight wagons for transport of cars during last two decades in wagon factories "Bratstvo" from Subotica and Wagon Factory Kraljevo from Kraljevo (Serbia).

Basic type for transport of cars in Serbia was Leas wagon that was designed during 1970s (Fig. 1). The wagon consists of two units, each with two platforms, and has three axles. Being that it was developed in the period when aspect of security of transported cars was not considered, its main features were designed considering the fact that weight of transported cars (≈ 18 t) is not high compared to dead weight of the wagon (≈ 27 t). Therefore, it was technically possible to design a wagon structure that was consisting only of beams, so the wagon was open, without front/back or side walls, or even roof. Such structure

requested smaller costs in production material and work force, so applied design was optimal from the point of view of cost of the wagon.

Fig. 1. Leas wagon for car transport

Exploitation of wagons of Leas type has shown that maintenance costs were low and durability of wagon was high, as it was expected in the phase of design. Moreover, the existence of such type of wagon got full economic justification, being that reduced number of wheelsets (three wheelsets for two units, instead of usual four, were possible because of relatively small total weight of wagon) meant lower transportation costs (which are paid according to number of wheelsets and not weight of vehicles), and, hence, increase of profits for operators that used wagons of Leas type.

However, in course of the economic crisis and social changes in Balkan countries during late 1980s and early 1990s, general rise of level of criminal was also reflected at increased level of thefts on railway, and Leas type of wagon, designed without regards to security requests, turned out to be quite inadequate in such social environment. Stealing car parts and burglary acts performed on cars transported on Leas wagons significantly increased and customers become avoiding them. It was also earlier noticed that open sides do not protect transported cars from weather conditions and small flying parts of stones or garbage that occasionally hit cars during transportation.

In order to comply with changed conditions and market requests, wagon factory “Bratstvo” from Subotica (Serbia) made a reconstruction of Leas wagons according to design that comprised closing of wagon structure from front and back side by sliding steel doors, mounting of roof over top platform, and covering lateral sides by transparent steel net

(Fig. 2)[4]. This solution of design of car transport wagon is classified as DDam type of wagon.

Fig. 2. Outside (left) and inside (right) view of DDam type of wagon

DDam type of wagons turned out to be very successful from the point of view of security of goods. Number of thefts is significantly reduced, and also the damages caused to transported cars due to unfavorable weather conditions and other reasons. On the other side, DDam wagon had some problems with derailments caused by the design, because of increased stiffness of wagon structure and increased weight, caused by redesign, influenced negatively safety of ride of the vehicle that has three axles.

On the other side, Wagon Factory Kraljevo, responding to market requests for changes of design of Leas wagon, aware of advantages and drawbacks of DDam solution developed by competition, decided, on request made by a customer, to apply different design, comprising closing of all sides of wagon by steel plates (covering space between units with rubber), and retractable roof (Fig. 3)[5]. The design belongs to Hccrss type of wagons. Reacting to this move, wagon factory "Bratstvo "produced its own wagon of Hccrss type, changing rolling stock so that it had two bodies and four axles, this improving safety against derailment and running behavior of the vehicle, comparing to DDam type.

[4] Technical documentation for DDam wagon, "Bratstvo", Subotica (1995)
[5] Technical documentation for Hccrss wagon, "Wagon factory Kraljevo", Kraljevo, (2006)

Fig. 3. Outside (left) and inside (right) view of Hccrss type of wagon

However, such design of railway vehicle, favorable by technical point of view, because of increased safety of the vehicle, turned out to be inappropriate from security point of view, although security from external influences was complete. During exploitation in Middle East countries, it turned out that transported vehicles were not observable during transport, which enabled increased numbers of thefts and robberies during transportation between stations, due to the fact that criminals operated in closed space, hidden behind the walls of the wagon.

Although application of Hccrss wagons turned out to be favorable solution in cases of transport through areas exposed to influence of highly abrasive materials (like in Middle East deserts conditions), this type of wagon in general had less success on market compared to DDam wagons, because it did not follow one of basic principles of security design of railway vehicles “Improve the ability to see into and out of vehicle”.

Conclusion

The paper presented a short overview of security principles guiding the design of railway vehicles and an example of evolution of the design of one type of freight wagon, demonstrating the importance of security aspect of a vehicle for its success at the contemporary market.

It can be concluded that in contemporary social environment, influenced by consequences of global economic crisis and rise of criminal, violence and terrorism, criteria for success of a product changes, in some cases putting security aspects as primary criterion for estimation of quality of a product.

Acknowledgement

The authors wish to express their gratitude to European Commission for the support to participation to the Conference realized within FP7 project "SeRViCE".

Bibliography

1. Technical Committee CEN, *EN 12663-Railway applications-Structural requirements of railway vehicle bodies*, Brussels, Belgium ,2000.
2. Technical Committee CEN, *Technical Specification for Interoperability relating to the subsystem Rolling Stock – Freight Wagons*, Brussels, Belgium July 2006.
3. ERRAC, *Sustainable rail system for connected Europe*, February 2006
4. Federal Transit Administration, Office of Safety and Security, 400 Seventh Street, SW, Washington, *DC 205902003, 49 CFR Part 659 – Rail Fixed Guideway Systems; State Safety Oversight, Reference Guide*, USA, June 22, 2005.
5. U.S. Department of Transportation Federal Transit Administration, *State Safety Oversight (SSO) Program Annual Report for 2005*, Federal Transit Administration Office of Safety and Security Washington, DC 20590, October 2006.
6. U.S. Department of Transportation Federal Transit Administration, *Rail Transit Safety Action Plan*, Federal Transit Administration Office of Safety and Security Washington, DC 20590, September 2006.

Internet sources

1. http://www.rssb.co.uk/europe/tsi.asp, Technical Specifications for Interoperability
2. http://www.tsa.gov/what_we_do/rail/index.shtm, Rail Security
3. http://europa.eu/scadplus/leg/en/lvb/l24013.htm, European Railway Agency
4. http://www.rff.fr/pages/europe/directives_eur.asp?lg=en, EU directives

Summary

Security and safety of transported goods is one of basic requests in transport of goods. While contemporary procedures and systems for monitoring and control of goods present technical bases for reduction of risk, safety and security of goods can also be improved by changes in design of transport vehicles. This paper presents influence of requests of security of goods on evolution of design of freight wagons for car transport.

Stanisław Piocha[*]
Jerzy Łuć[**]

BEZPIECZEŃSTWO ENERGETYCZNE PRZEDSIĘBIORSTW CIEPŁOWNICZYCH JAKO SKŁADNIK BEZPIECZEŃSTWA EKONOMICZNEGO

Streszczenie

Bezpieczeństwo jako obszar związany z naukami ekonomicznymi posiada swą bogatą tradycję dociekań wielu nauk społecznych, przede wszystkim jednak filozofii, socjologii i prakseologii.

Za interesujący uważamy problem społecznego postrzegania bezpieczeństwa energetycznego jako elementu szerszego zagadnienia. Dotyczy to branży ciepłowniczej na tle energetyki zawodowej, czy gazownictwa z perspektywy dostrzegania ewentualnych skutków braku zapewnienia wystarczającego poziomu tego bezpieczeństwa przez przedsiębiorstwa. Obserwujemy to w kontekście kreowania przez państwo warunków brzegowych umożliwiających zgromadzenie niezbędnych zasobów kapitałowych i ludzkich gwarantujących zapewnienie odpowiednich standardów bezpieczeństwa w tym zakresie.

1. Bezpieczeństwo w polityce ekonomicznej państwa

Bezpieczeństwo jako obszar związany z naukami ekonomicznymi posiada swą bogatą tradycję dociekań wielu nauk społecznych, przede wszystkim jednak filozofii, socjologii i prakseologii. Przedstawiciele tych nauk zarówno głęboko w historii jak i w historii nowożytnej podejmowali w swych rozważaniach problemy bezpieczeństwa, przy tym nie jednolicie interpretowali treść tego pojęcia .

[*] Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.
[**] Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.

Współczesne kierunki dociekań nad bezpieczeństwem, opierając swe postulaty naukowe na dorobku filozofii , nauk wojskowych i prakseologii także ekonomii, postulują rozwijanie sekurologii (nauki o bezpieczeństwie) realizowanej obecnie coraz powszechniej jako „badania nad bezpieczeństwem".

Środowiska podejmujące metodologiczne zagadnienia tworzenia strategii bezpieczeństwa państwa, nie zaprzeczając potrzeby rozwijania nauki, wskazują na konieczność poszukiwania w tym procesie odpowiedzi na dwa zasadnicze pytania[1]: jaka ma być strategia bezpieczeństwa? Jakie są podstawowe cele strategiczne państwa w zakresie bezpieczeństwa?

W ostatniej dekadzie XX wieku pojawiły się na poziomie globalnym i regionalnym nowe procesy oraz ukształtowały się zjawiska, które mają wpływ na rozumienie kategorii bezpieczeństwa i na treść strategii bezpieczeństwa państwa.

Za jedną z podstawowych przyczyn uzasadniających nowe spojrzenie na kategorię – bezpieczeństwo uznać, wydaje się, należy proces globalizacji wielu płaszczyzn funkcjonowania społeczeństwa. W szczególności globalizacja ta posiada odzwierciedlenie w problematyce ekonomicznej, w tym makroekonomicznej, współczesnego świata.

Pojęcie „globalizacja" pojawiło się w ekonomii w połowie XX wieku w ujęciu ówczesnych ekonomistów, charakterystyczną cechą tego procesu było nasilanie centralizacji kapitału przy równoczesnej dekoncentracji produkcji[2].

Współcześnie literatura przedmiotu nadaje nowy wymiar i nową treść dla tego pojęcia. Utożsamiane jest ono z procesem zmiany perspektywy określania zasad i reguł postępowania, zdarzeń, zachowań działań i uznawanych wartości z perspektywy narodowej na ogólnoświatową. W taki sposób identyfikowanej globalizacji ekonomiści przypisują kilka głównych wymiarów:

- konkurencja globalna,
- megakoncentracja własności i kapitału,
- współpraca między przedsiębiorstwami w skali świata,
- nowa polityka innowacyjna,

[1] R. Zięba *Cele polityki Zagranicznej,* W: J. Kukułka R. Zięba (red.) Polityka zagraniczna państwa, UW Warszawa 1992, s. 64.

[2] Por. M. Perczyński *Globalne uwarunkowania bezpieczeństwa ekonomicznego*, Warszawa 1990, s. 12- i dalsze.

- oparcie gospodarowania na wiedzy i kapitale intelektualnym,
- rozwój zaawansowanej technologii w zakresie informacji i telekomunikacji[3].

Przypisywanie takiej treści procesom globalizacji tworzy potrzebę określenia obszarów, w których procesy te przebiegają. Zdaniem wielu ekonomistów, z punktu widzenia makroekonomii i teorii organizacji i zarządzania przejawianie się ich dostrzegać należy przynajmniej w następujących obszarach:[4]

- finansów,
- rynków i strategii (konkurencji),
- technologii,
- stylów życia i modeli konsumpcji,
- pełnienia funkcji regulacyjnych przez administracje rządowe,
- politycznego ujednoliceniu świata.

Tak pojmowanemu procesowi globalizacji towarzyszy przejmowanie w pewnej mierze regulacyjnych funkcji, które tradycyjnie przypisywane były administracji rządowej, prze organizacje gospodarcze, m in. przykładem takich zachowań może być – przypisywanie do misji dużych przedsiębiorstw działań ograniczających skutki ujemnych efektów procesów gospodarczych (przyjazny stosunek do środowiska naturalnego).

Wymienione wyżej procesy megakoncentracji własności i kapitału stanowią wyzwania dla miejsca rządu w gospodarce. Nowego spojrzenia wymaga rozumienie bezpieczeństwa ekonomicznego. Dosyć często z warunkami bezpiecznego rozwoju łączono ochronę przedsiębiorstw krajowych posiadających wiodącą pozycję na rynku i w związku z tym często pozycja ta chroniona była przed konkurencyjnymimportem. Globalizacja rynków tworzy sytuację, w której podmioty te stają się przedsiębiorstwami średniej wielkości na globalnym rynku.

Rola regulacyjna administracji rządowej musi w takich warunkach koncentrować swe decyzje na takich sposobach ochrony konkurencji, aby zasady konkurencji były jednolite w skali międzynarodowej. Oznacza to, że przedsiębiorstwa globalne, natrafią na takie same regulacje, niezależnie od kraju w którym będą prowadzić działalność gospodarczą.

---

[3] Por. G. Gierszewska, B. Wawrzyniak *Globalizacja wyzwania dla zarządzania strategicznego,* Poltext, Warszawa 2001, s.5-8.

[4] *Granice konkurencji, Grupa Lizbońska*, seria Euromanagement, PFPK-Poltex, Warszawa 1996, s.48- 50.

Wyjątkowego znaczenia nabiera ukierunkowanie polityki ochrony konkurencji na sferę dystrybucji i likwidowaniu barier w międzynarodowej wymianie gospodarczej. Taka polityka nie jest możliwa do przeprowadzenia przez rządy poszczególnych krajów. Skuteczność polityki w takich warunkach wymaga decyzji ponad państwowych. Ogromną rolę w prowadzeniu takiej polityki odgrywają międzynarodowe ugrupowania gospodarcze. Dobrze są nam znane efekty związane z procesem włączania naszej gospodarki systemu regionalnego.

W literaturze przedmiotu podkreśla się, iż we współczesnym świecie występują dwa kierunki działań, z jednej strony są to działania zmierzające do zrzeczenia się części władzy przez centralne ośrodki władzy politycznej krajów na rzecz regionalnych lub instytucji ponad narodowych, drugi kierunek to rozwój korporacji transnarodowych, obejmujących często równocześnie różne dziedziny gospodarki.[5]

Przedstawione zjawiska dowodzą, że zdefiniowanie bezpieczeństwa ekonomicznego nie jest łatwe, pojęcie to bowiem jest nieostre i wieloznaczne. Nieostrość pojęcia zawiera się w fakcie, że odnosić go można do bezpieczeństwa poszczególnych gospodarstw domowych, a nawet jednostek całych grup społecznych, różnej wielkości i dziedzin działania podmiotów gospodarczych, poszczególnych państw, układów regionalnych czy też globalnych. W literaturze przedmiotu najczęściej pojęcie bezpieczeństwa ekonomicznego wyprowadza się z definiowanego przez słownik języka polskiego ogólnego pojęcia-bezpieczeństwo – jako stanu „ nie zagrożenia, spokoju, pewności.”[6].

Analitycy problemu często zagrożenia i wyzwania identyfikują jako takie zjawiska, które kojarzą się, choćby intuicyjnie, z poczuciem bezpieczeństwa[7].

Ocena stanu bezpieczeństwa, a co za tym idzie – świadomość istnienia lub braku istnienia zagrożeń, tkwi w psychice człowieka, społeczeństwa lub narodu. Za F. Kaufmannem przyjmuje się często definicję zagrożenia jako możliwości wystąpienia jednego z negatywnie wartościowanych zjawisk.

---

[5] *Międzynarodowe stosunki gospodarcze, praca zbiorowa* pod red. Budnikowskiego A. i Kaweckiej-Wyrzykowskiej E., PWE, Warszawa 1996, s. 17-18.

[6] *Słownik języka polskiego,* pod red. Szymczaka M., PWN Warszawa 1978, s. 147.

[7] Kukułka J.*, Nowe uwarunkowania i wymiary bezpieczeństwa międzynarodowego Polski,* "Wieś i Państwo" nr 1/1995, s. 198.

Interesujący jest przy tym model, opracowany przez R. Ziębę, wyjaśnienia prawidłowego lub fałszywego postrzegania zagrożeń. Zagrożenia powodują stan niepewności, wręcz strachu. W zależności od świadomości społeczeństwa, decydentów, polityków oraz kategoryzacji pojęć w strategii bezpieczeństwa, pojawia się stan braku bezpieczeństwa, stan obsesji w dziedzinie bezpieczeństwa., stan fałszywego bezpieczeństwa, lub też stan rzeczywistego bezpieczeństwa.

U schyłku ubiegłego stulecia obok kategorii „zagrożenia" w badaniach nad bezpieczeństwem, wprowadzona została kategoria „wyzwania". Niektórzy autorzy identyfikują tą kategorię jako niezbywalne potrzeby wymagające sformułowania odpowiedzi i podjęcia stosownych działań. Wskazuje się przy tym, że zagrożenia i wyzwania są trudne do wyraźnego rozróżnienia; między nimi istnieje cienka linia podziału. Jeszcze do niedawna terroryzm tak jak przestępczość zorganizowana, migracje ludności, skażenie środowiska zaliczano do kategorii wyzwań. Uważano, że międzynarodowy terroryzm jest zjawiskiem, któremu można sprostać przez podjęcie konkretnych, dobrze zorganizowanych działań. Takie podejście do walki z terroryzmem jako z wyzwaniem dla bezpieczeństwa można znaleźć w większości strategii bezpieczeństwa. Widać z tego, że pomijając nawet określone wcześniej możliwości przypisania pewnych przydomków (rodzajów) bezpieczeństwa i spojrzenia na problem z punku widzenia makroekonomicznego, trudnym jest o precyzyjną jednoznaczną definicję. Uznaje się przy tym, wzmocnienie tego bezpieczeństwa ekonomicznego jest niezbywalny celem polityki państwa. Osiągnięcie tego celu uzyskuje się poprzez eliminację zagrożeń zewnętrznych i wewnętrznych.

*W znacznej ilości pozycji literatury pojęcie bezpieczeństwo ekonomiczne utożsamiane jest ze zdolnością systemu gospodarczego państwa (grupy państw) do takiego wykorzystania wewnętrznych czynników rozwoju i międzynarodowej współzależności ekonomicznej, które gwarantowały będą jego niezagrożony rozwój.[8]

Ten kierunek myślenia, wydaje się leży u podstaw definiowania bezpieczeństwa i bezpieczeństwa państwa w założeniach polityki bezpieczeństwa w naszym kraju, w których **bezpieczeństwo** utożsamia się ze stanem braku zagrożenia, stan spokoju i pewności.

[8] Z. Kołodziejak, *Kierunki tworzenia bezpieczeństwa ekonomicznego* "Wektory" 1984, nr 4.

Natomiast za **bezpieczeństwo państwa** uznaje się stan uzyskany w wyniku zorganizowanej obrony i ochrony przed możliwymi zagrożeniami, wyrażony stosunkiem potencjału obronnego do skali zagrożeń.[9] Wymienia się następnie cały szereg zagrożeń, które stanowią olbrzymie agregaty działań mogących naruszyć przyjęty stan. Są to obszary na których oparte jest bezpieczeństwo państwa:

1. Zagrożenia polityczne
2. Zagrożenia gospodarcze
3. Zagrożenia psychologiczno-socjologiczne
4. Zagrożenia ekologiczne
5. Zagrożenia ładu i porządku publicznego (wewnętrzne)
6. Zagrożenia militarne

Identyfikując skuteczne kształtowanie bezpieczeństwa przez państwo jako zadanie naczelne określa się często to zadanie jako – jako potrzebę: przetrwania państwa, jego zwartości terytorialnej oraz integracji regionalnej; a także rozwoju ekonomicznego i podnoszenia jakości życia społeczeństwa, a także utrzymania niezależności politycznej i rozwoju demokracji.[10] Takie podejście daje asumpt do formułowania następujących dziedzin działania uznawanych za priorytetowe dla funkcjonowania państwa i narodu:

– bezpieczeństwo polityczne;
– bezpieczeństwo ekonomiczne;
– bezpieczeństwo społeczne;
– bezpieczeństwo kulturowe;
– bezpieczeństwo militarne.

Widać z tego, że naukowcy niezależnie od siebie, w bardzo zbliżony sposób podchodzą do wyodrębnienia czynników bezpieczeństwa. Takie podejście do problematyki bezpieczeństwa w pewnym sensie determinuje kierunki poczynań w procesie tworzenia koncepcji i strategii bezpieczeństwa. Koncepcje takie odnoszą się z reguły do wskazywanej w podejściu wielu państw strategii globalnej, regionalnej oraz narodowej.

Wskazane wyżej zjawiska i procesy, przede wszystkim zaś wzrost powiązań poszczególnych gospodarek (nawet tylko istotnych jej ogniw, np. rynku finansowego), regionów, ugrupowań, dynamiczny rozwój wymiany handlowej, coraz powszechniej obejmujących także usługi oraz

[9] *Polityka bezpieczeństwa i strategia obronna Rzeczypospolitej Polskiej*, 1992, materiał powielony, s. 10.

[10] Kukułka J., *Bezpieczeństwo a współpraca europejska*, Sprawy Międzynarodowe" nr 7/1982, s. 34.

czynniki wytwórcze w tym czynnik – praca, mogą być czynnikiem sprawczym osłabienia suwerenności ekonomicznej poszczególnych krajów. Co często posiada swe odbicie w utracie zdolności kierowania przez państwo sposobem wykorzystania zasobów gospodarczych, szczególnie zasobów naturalnych i rozwojem niektórych działów gospodarczych. Utrata zdolności do spełniania jednej z ważnych funkcji kierowania – kontroli może być tego przyczyną.

Przedstawione określenia sugeruje trafność tez W. Stankiewicza, przypisujących pewną statyczność ujęcia zagadnień bezpieczeństwa ekonomicznego. Już definicja wskazuje (chwila bieżąca i niedaleka przyszłość), że ma się na myśli pewien wyodrębniony stan stosunków międzynarodowych, do którego się przymierza stosunki istniejące lub do których się w krótkim okresie zmierza, uznając postawiony cel za godny realizacji w przyjętej polityce[11]. Tym czasem bezpieczeństwo ekonomiczne faktycznie występuje w przynajmniej trzech płaszczyznach podstawowych: pojedynczego państwa, grupy państw i globalnej. W tym aspekcie za bardzo trafne uznać trzeba sformułowanie, że istotą bezpieczeństwa, jest jego podmiotowość.

To stanowi punkt wyjścia do przyjęcia założenia, że bezpieczeństwo jest zawsze czyjeś, państwa lub grupy państw (sojuszy, koalicji). Ze względu na kryterium podmiotowe rozróżnia się bezpieczeństwo narodowe i międzynarodowe[12].

Równocześnie zdaniem autorów nie uzasadnionym jest zawężanie definicji bezpieczeństwa i co za tym idzie procesów w niej identyfikowanych do jednego z wymienionych (narodowe lub międzynarodowe). Chodzi o to, że gospodarki nie rozwijają się w oderwaniu od otoczenia zewnętrznego.

Trzy wymienione wyżej płaszczyzny tworzą równocześnie trzy pojęcia bezpieczeństwa ekonomicznego i wydaje się bezpieczeństwa w ogóle, które są zbudowane hierarchicznie i są wzajemnie powiązane. Powiązania mogą dodatnio lub ujemnie wpływać na osiągnięcie pozytywnych rezultatów. Wyodrębnienie tych płaszczyzn związane jest między innymi istotnymi różnicami celów w nich występującymi. W pierwszej chodzi o rozwój krajowego systemu gospodarczego, który

[11] W. Stankiewicz *Węzłowe problemy ekonomiki obrony, „*Myśl Wojskowa" 1985, nr 1.
[12] R. Zięba *Kategorie bezpieczeństwa w nauce o stosunkach międzynarodowych. Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, FSM, Warszawa 1997, s. 6.

zapewnia racjonalne ekonomicznie wykorzystanie wewnętrznych czynników rozwoju i skuteczne przeciwstawienie się zewnętrznej ingerencji. Druga płaszczyzna wyznacza integrujące działania gospodarcze grupy państw w celu przyśpieszenia rozwoju gospodarek, a także zapewnienia grupowej (regionalnej) suwerenności ekonomicznej. Dobrym przykładem europejskim jest integracja w ramach Unii Europejskiej. To równocześnie musi uwzględniać pewne rezygnacje z własnej suwerenności ekonomicznej pojedynczego państwa. W płaszczyźnie trzeciej – globalnej o normalizację międzynarodowych stosunków ekonomicznych.

Cechą współczesnej gospodarki światowej jest przede wszystkim znaczne zróżnicowanie form powiązań międzynarodowych. Oprócz wymiany handlowej dynamicznie rozwija się współpraca produkcyjna i inwestycyjna. Oprócz wymiany towarów i usług szybko się zwiększa przepływ czynników produkcji. Jednocześnie zróżnicowaniu ulegają podmioty gospodarki światowej; wzrasta udział podmiotów międzynarodowych i transnarodowych (przedsiębiorstw, organizacji, instytucji).

We współczesnej gospodarce światowej zmienia się także charakter podziału pracy: specjalizacja o charakterze międzygałęziowym ustępuje miejsca specjalizacji wewnątrzgałęziowej, a wymiana wyrobów gotowych – wymianie podzespołów i części wyrobów gotowych. W związku z tym wzrasta znaczenie wzajemnych powiązań gospodarczych w obrębie krajów rozwiniętych gospodarczo i maleje znaczenie powiązań między krajami rozwiniętymi gospodarczo a krajami słabo rozwiniętymi.

System gospodarki światowej rozwijający się współcześnie coraz mniej przypomina swego protoplastę tzn. tradycyjną gospodarkę światową opartą na międzygałęziowym podziale pracy i narodowych podmiotach gospodarczych. Przede wszystkim przestaje ona być sumą gospodarek narodowych, a staje się gospodarką globalną, w obrębie której następuje integracja gospodarek narodowych w jeden organizm gospodarczy.[13] Przejrzyste, łatwe do ilościowego zewidencjonowania powiązania handlowe typowe dla tradycyjnej gospodarki światowej ustępują miejsca różnorodnym powiązaniom trudnym do ujęcia

[13] *Współczesna gospodarka światowa,* red. A. B. Kisiel-Łowczyc, Uniwersytet Gdański, Gdańsk 1994, s. 25.

statystycznego. W coraz większym stopniu uzależniają one gospodarki narodowe od środowiska międzynarodowego.

Podobnie jak w tradycyjnej gospodarce światowej stopniowi malało znaczenie producentów surowców i żywności, tak we współczesnej gospodarce światowej maleje znaczenie rozwoju przemysłowego, wzrasta zaś rola postępu naukowo-technicznego. W takich warunkach funkcjonowania gospodarki światowej koniecznym, wydaje się być, budowanie zaufania ekonomicznego, tworzenie warunków podejmowania globalnych problemów ekonomicznych, eliminację wszelkich przejawów dyskryminacji i wojny gospodarczej. Niestety doświadczenia funkcjonowania współczesnej gospodarki światowej na płaszczyźnie ekonomicznej nie rokuje w najbliższej przyszłości rozwiązania problemu globalnego bezpieczeństwa ekonomicznego. Narzędzia wojny gospodarczej wciąż stanowią główny sposób rozwiązania ważnych problemów politycznych.

Bezpieczeństwo ekonomiczne to tylko jedna z płaszczyzn tworzenia warunków bezpiecznego rozwoju. Płaszczyzna, którą trudno przecenić. Jednak analizując uwarunkowania rozwoju dostrzegać trzeba inne jego płaszczyzny. Podkreślić przy tym należy, iż skuteczność rozwiązywania problemów w tych innych płaszczyznach jest bardzo silnie związana z gospodarką, z jej stanem i sposobem funkcjonowania, zdolnością do przekształcenia określonych zasobów w czynniki kształtujące właściwe relacje w innych płaszczyznach.

W podejmowaniu decyzji w zakresie kształtowania strategii bezpieczeństwa, jak wskazuje literatura specjalistyczna, bierze się pod uwagę wyniki długotrwałych studiów ośrodków naukowych. Mówiąc zatem o systemie bezpieczeństwa, Instytucje naukowe traktować trzeba jako integralny komponent tego systemu.

2. Ciepłownictwo jako ogniwo systemu gospodarczego i społecznego

Wyjaśnienie pojęcia „ciepłownictwo” oraz krótka charakterystyka tego sektora gospodarki pozwoli lepiej opisać jego miejsce w strukturze gospodarki narodowej w relacjach do innych grup przedsiębiorstw, biorąc za podstawę wyodrębnienia podział branżowy i funkcjonalny, a także umożliwi dokonanie oceny zakresu i skali przedmiotu odniesienia dla dalszej analizy.

Definiując pojęcie: „ciepłownictwo” posłużymy się do tego celu unormowaniem prawnym zawartym w rozporządzeniu wykonawczym do

Ustawy z dnia 10 kwietnia 1997 roku – Prawo energetyczne, gdzie czytamy:„ przedsiębiorstwo ciepłownicze – przedsiębiorstwo zajmujące się wytwarzaniem ciepła w eksploatowanych przez to przedsiębiorstwo źródłach ciepła, przesyłaniem i dystrybucją oraz sprzedażą ciepła wytworzonego w tych źródłach lub zakupionego od innego przedsiębiorstwa energetycznego”[14]. Wychodząc z przedstawionej wyżej definicji możemy stwierdzić, że przedsiębiorstwa ciepłownicze tworzą branżę często nazywaną w literaturze, a także w języku potocznym ciepłownictwem, lub sektorem ciepłowniczym.

Dokonując dalszej kwalifikacji terminologicznej należy zauważyć, że sektor ten pojęciowo mieści się jednocześnie w obrębie sektora energetycznego oraz w obszarze gospodarki komunalnej. Cytowana wcześniej Ustawa w art. 3 ust. 12 precyzuje pojęcie przedsiębiorstwa energetycznego w następujący sposób: „przedsiębiorstwo energetyczne – podmiot prowadzący działalność gospodarczą w zakresie wytwarzania, przetwarzania, magazynowania, przesyłania, dystrybucji paliw albo energii lub obrotu nimi.”

Dla utrzymania pełnej jasności terminologicznej w obszarze naszego zainteresowania, nie wchodząc przy tym głębiej w rozważania z zakresu fizyki, warto tutaj dodać, że pojęcie „ciepła” mieści się mieści się w kategorii „energii”. I tak, zgodnie z Ustawą ciepło to: „energia cieplna w wodzie gorącej, parze lub w innych nośnikach”[15].

Badając aspekty funkcjonalne usytuowania branży możemy zaobserwować, że przedsiębiorstwa ciepłownicze będąc jednym z rodzajów przedsiębiorstw energetycznych należy jednocześnie postrzegać w obszarze gospodarki komunalnej. Jest to uzasadnione ze względu na szczególną rolę jaką pełnią one w zabezpieczeniu potrzeb mieszkańców, instytucji publicznych i przedsiębiorstw w zakresie zaopatrzenia tych podmiotów w ciepło.

W praktyce życia gospodarczego pociąga to za sobą taki skutek, że bezpośrednie zainteresowanie ich sprawnym funkcjonowaniem często jest w większym stopniu domeną lokalnych władz samorządowych niż państwowych instytucji centralnych. Ponadto warto też tutaj nadmienić,

---

[14] Por. *Rozporządzenie Ministra Gospodarki z dnia 15 stycznia 2007r. w sprawie szczegółowych warunków funkcjonowania systemów ciepłowniczych,* Dz. U. z 1 lutego 2007 r. Nr 16 poz. 92, & 2 ust.1.

[15] Por. *Ustawa z dnia 10 kwietnia 1997 r. Prawo Energetyczne*, Dz. U. 1997 r. Nr 54 poz. 348, z późniejszymi zmianami, Art.3, ust.2.

że zgodnie z obowiązującymi w Polsce uregulowaniami prawnymi zapewnienie zaopatrzenia w ciepło mieszkańców należy do zadań własnych gminy. Władze centralne skupiają się natomiast bardziej na tworzeniu ogólnych warunków brzegowych rozwoju branży, czemu ma w szczególności służyć kształtowanie treści Prawa energetycznego i polityki energetycznej, a w tym również głównych założeń polityki regulacyjnej oraz realizacji jej treści. To ostatnie zadanie wykonywane jest poprzez określanie obowiązującego w kraju modelu regulacji energetyki oraz wykonywanie określonych przepisami prawnymi zadań za pośrednictwem powołanego specjalnie w tym celu Urzędu Regulacji Energetyki.

Lokalny charakter podstawowych funkcji przedsiębiorstw ciepłowniczych nie oznacza jednak, że mówimy o niewielkim i mało znaczącym sektorze. Wprost przeciwnie, jest to sektor posiadający duży potencjał produkcyjny i ludzki. Istnieje natomiast zjawisko znacznego rozproszenia terytorialnego poszczególnych przedsiębiorstw tego sektora. Ma miejsce też duże zróżnicowanie wielkości przedsiębiorstw ciepłowniczych, ich kondycji finansowej, poziomu nowoczesności stosowanych przez nie rozwiązań technicznych, technologicznych i organizacyjnych, a także funkcjonujących w praktyce struktur własnościowych. Dla potwierdzenia powyższych stwierdzeń wystarczy przytoczyć tutaj niektóre dane faktograficzne, uzyskane z oficjalnych statystyk prezentowanych przez URE.

W roku 2007 w ewidencji Urzędu, jako przedmiot jego regulacji występowały 540 przedsiębiorstwa, w których moc zainstalowana ogółem wynosiła 62 752,3 MW. W tym zarejestrowano 87 przedsiębiorstw o mocy zainstalowanej 10 MW i poniżej i jednocześnie 8 przedsiębiorstw o mocy zainstalowanej powyżej 1000 MW. Najliczniejszą grupę sektora stanowiły przedsiębiorstwa mniejsze niż średnie, o mocy zainstalowanej mieszczącej się w przedziale 25-50 MW, których wówczas było 109. Bowiem średnia moc przypadająca na jedno przedsiębiorstwo w tym roku wynosiła 116,2 MW. Drugą co do liczebności grupę przedsiębiorstw stanowiły podmioty posiadające moc mieszczącą się w przedziale 10-25 MW, których było 99. W badanym okresie przedsiębiorstwa ciepłownicze objęte ewidencją URE zatrudniały średnio 43 311 pracowników. W tym przedsiębiorstwa zorganizowane w formie spółki z o. o. zatrudniały największą liczbę pracowników, wynoszącą 23 278, drugie w kolejności przyjmując za kryterium liczbę zatrudnionych pracowników były spółki akcyjne, które zatrudniały 17 873 pracowników. Zaś pozostali

pracownicy, szeregując podmioty według wielkości zatrudnienia, pracowali w przedsiębiorstwach państwowych, jednostkach samorządu terytorialnego, spółdzielniach mieszkaniowych i w grupie przedsiębiorstw pozostałych. Należy przy tym nadmienić, że na przestrzeni ostatnich kilkunastu lat w sektorze ciepłowniczym silnie zaawansowane zostały procesy prywatyzacyjne, których obraz w sposób pośredni, w dużym stopniu ilustruje liczba spółek prawa handlowego, szacowana w tym okresie na 437 podmiotów[16].

3. Pojęcie bezpieczeństwa energetycznego i czynników wpływających na poziom bezpieczeństwa

Zarówno w publicystyce, opracowaniach naukowych, jak i w ustawodawstwie pojawia się termin „bezpieczeństwo energetyczne". Zgodnie z definicją ustawową tego pojęcia, bezpieczeństwo energetyczne oznacza: „stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska"[17].

Analizując treść zaprezentowanego unormowania, możemy stwierdzić, że pojęcie to odnosi się do całej gospodarki i ma charakter ujęcia dynamicznego oraz kompleksowego. Wskazuje na to podkreślenie w definicji aspektów perspektywicznych oraz powiązanie wymogów bezpieczeństwa z realiami technicznymi, ekonomicznymi i ekologicznymi. W szczególności nawiązanie do ekologii wskazuje na nowoczesny charakter podejścia ustawodawcy, związany z uznawaną obecnie powszechnie zasadą zrównoważonego rozwoju. Odnosząc pojęcie bezpieczeństwa energetycznego do rożnych sektorów energetyki dla potrzeb dalszej analizy przyjmujemy, że dla każdego z sektorów istotę tej kategorii stanowi zapewnienie ciągłości dostaw energii o wystarczającej mocy, określonej odpowiednimi standardami jakości i przy utrzymaniu racjonalnego poziomu kosztów. Niezależnie od przyjętego dla konkretnej branży praktycznego sposobu rozumienia pojęcia bezpieczeństwa energetycznego sam fakt istnienia potrzeby zapewnienia tego rodzaju bezpieczeństwa pozostaje bezsporny, patrząc

[16] Por. *Prezes Urzędu Regulacji Energetyki, Energetyka cieplna w liczbach - 2007,* Warszawa 2008.
[17] Por. *Ustawa*...op. cit., Art. 3 ust. 16.

zarówno z perspektywy przedsiębiorstwa jak i odbiorcy. Niezależnie od tego, obowiązujące przepisy prawne nakładają na przedsiębiorstwa energetyczne obowiązek jego zapewnienia, również celem polityki energetycznej państwa jest zapewnienie bezpieczeństwa energetycznego kraju[18]. Jednakże sposób rozumienia bezpieczeństwa energetycznego, a co za tym idzie mechanizm jego zabezpieczenia w poszczególnych podsektorach energetyki jest w konkretnych warunkach inny. Wynika to przede wszystkim z odmiennych warunków technicznych i ekonomicznych funkcjonowania poszczególnych branż i związanych z tym zróżnicowaniem, przyjmowanych do stosowania w relacjach z klientem standardach jego obsługi.

Zjawiskiem obserwowalnym w obszarze całej energetyki jest różnorodność czynników wpływających na poziom bezpieczeństwa energetycznego. Jednocześnie obserwuje się zmienność natężenia wpływu poszczególnych czynników na bezpieczeństwo w różnych branżach. Także i w poszczególnych przedsiębiorstwach w obrębie jednej branży warunki funkcjonowania są zróżnicowane.

Czynniki mające wpływ na poziom bezpieczeństwa możemy odnieść do różnych obszarów i aspektów funkcjonowania przedsiębiorstwa.

Wydaje się trafnym wyróżnić przede wszystkim:

- aspekty techniczne,
- prawno-własnościowe,
- finansowe,
- ekologiczne,
- zaopatrzeniowo-logistyczne,
- i aspekty bezpieczeństwa pracy.

Dokonując analizy sposobu oddziaływania poszczególnych czynników, mających wpływ na poziom bezpieczeństwa z perspektywy poszczególnych aspektów funkcjonowania przedsiębiorstwa, obserwujemy ich wzajemne powiązanie i uwarunkowanie. Dla przykładu można zauważyć, że aby zapewnić wymagany poziom bezpieczeństwa pracy należy ponieść określone koszty, które w połączeniu z koniecznością równoległego ponoszenia innych kosztów np. na ochronę środowiska, czy też inne cele, mogą wspólnie tworzyć barierę finansową.

Konkretyzując rozważania do sytuacji występujących w branży ciepłowniczej możemy zaprezentować następujące uwagi:

[18] Por. jw., Art. 13.

Aspekty techniczne

Patrząc na problem bezpieczeństwa energetycznego z punktu widzenia zapewniania niezbędnych norm technicznych, należy rozpatrywać dwie grupy zasobów, tj, majątek produkcyjny i zasoby ludzkie. Z punktu widzenia wpływu zasobu majątku produkcyjnego na kwestie bezpieczeństwa istotne znaczenie ma zarówno jakość wykonania tego majątku, jego wiek (stopień dekapitalizacji), jak i poziom nowoczesności zastosowanych rozwiązań. Dla przykładu można wykazać, że w wielu przypadkach instalacje ciepłownicze (sieci przesyłowe) wykonane w starej technologii, a więc rurociągi stalowe, położone w tradycyjnych, betonowych kanałach ciepłowniczych po kilkudziesięciu latach eksploatacji zachowują swoją sprawność techniczną. Objawia się to nie tylko niskim poziomem awaryjności, ale też umiarkowanym poziomem strat ciepła w trakcie jego przesyłu. Jest to możliwe, gdy w czasie realizacji inwestycji stosowano materiały spełniające w pełni obowiązujące normy jakościowe, a także proces realizacji inwestycji przebiegał zgodnie ze sztuką budowlaną. Z drugiej strony można też przytoczyć przykłady, że zastosowanie nowoczesnych technologii przesyłu ciepła w oparciu o wykorzystanie do tego celu rurociągów zbudowanych z sieci preizolowanych nie gwarantuje niezawodności procesu przesyłowego z punktu widzenia występujących w nim ubytków wody, ani też sprawnego monitoringu wycieków cieczy, pomimo istnienia wkomponowanej w rurociągi instalacji, której zadaniem jest sygnalizowanie pojawienia się nieszczelności rurociągów. Z zasady jednak stosowane w praktyce rozwiązania, oparte o nowoczesne technologie powinny zapewniać trwałość, niezawodność i efektywność ekonomiczną systemu, bowiem technologie te zostały zaprojektowane w taki sposób, aby do minimum ograniczyć możliwości powstawania awarii, ułatwiać wykrywanie i usuwanie awarii oraz zapewniać wysoką sprawność jego funkcjonowania. Nowoczesne rozwiązania pozwalają nie tylko na usprawnienie procesu przesyłu energii, jej transformacji na inne dogodne parametry w tzw. węzłach ciepłowniczych, ale również umożliwiają pełne zautomatyzowanie regulacji i nadzoru procesów jego wytwarzania w kotłowniach oraz przetwarzania w węzłach ciepłowniczych. Dzieje się to również na odległość poprzez telemetrię, zapewniającą możliwości zdalnego sterowania procesami wytwórczymi i przesyłowymi.

Nie wymaga większych dowodów teza, że dla potrzeb obsługi nowoczesnych systemów technicznych, bazujących na zaawansowanych

rozwiązaniach z zakresu automatyki, telemetrii i informatyki, krytycznym jest pozyskanie wysokiej jakości czynnika ludzkiego, prezentującego niezbędny poziom kwalifikacji zawodowych. Należy jednak dodać, iż w opisywanej branży niezależnie od spełnienia ww. wymogów kwalifikacyjnych pracownicy zajmujący stanowiska eksploatacyjne muszą spełniać dodatkowe wymogi formalne w postaci posiadania niezbędnych dla danego stanowiska świadectwa kwalifikacyjnego. Wykazanie się przez przedsiębiorstwo dowodami spełnienia tego wymogu, jest warunkiem otrzymania i utrzymania przez przedsiębiorstwo koncesji, które zgodnie z obowiązującymi przepisami prawnymi nadaje URE. Jest to jedna z dróg formalnych zapewnienia bezpieczeństwa energetycznego w branży.

Aspekty prawno- własnościowe

Realizacja inwestycji liniowych w terenie wymaga spełnienia niezbędnych procedur formalno-prawnych, których niedokonanie, lub niewłaściwe wykonanie rodzi niekorzystne skutki prawne. W szczególności istotną kwestią jest uzyskanie wszelkich niezbędnych pozwoleń (pozwolenia na budowę, pozwolenia do użytkowania i inne) oraz odpowiednie respektowanie skomplikowanych niejednokrotnie stanów prawnych w zakresie praw własnościowych. Rezultatem naruszenia tych zasad jest konieczność usunięcia położonych nielegalnie sieci, lub co najmniej ponoszenia znacznych dodatkowych i nie raz nie przewidzianych kosztów, związanych z ustanowieniem służebności lub dzierżaw na rzecz właścicieli terenu. Może to więc, w krańcowym przypadku, skutkować niemożnością kontynuowania działalności na danym obszarze, lub ponoszeniem znacznego ryzyka finansowego związanego z odszkodowaniami.

Ograniczenia i ryzyka finansowe

Prezentowany wyżej przykład, wskazujący na istnienie potencjalnego ryzyka finansowego, związanego z działalnością, dokumentuje, że bezpieczeństwo zapewniania ciągłości dostaw ciepła może w szczególnych okolicznościach być ograniczone względami finansowymi. Zagrożenia takie często mogą dotyczyć skutków dokonań faktycznych z względnie odległej w czasie przeszłości, kiedy realizowano procesy inwestycyjne nie zawsze w sposób konsekwentny zwracając uwagę na należyte udokumentowanie spełnienia wymogów formalnych związanych z realizacją tych procesów. Czasem też, występuje sytuacja,

w której z biegiem czasu odpowiednie dokumenty z różnych względów nie zachowały się. Innym przykładem ryzyka jest niewłaściwe, albo niewystarczające ubezpieczenie ryzyka od odpowiedzialności z tytułu prowadzonej działalności. Zdarza się, że nie spełnienie wymogów bezpieczeństwa może prowadzić do zniszczeń na skutek zalania nieruchomości, co wywołuje z reguły znaczne skutki finansowo-odszkodowawcze. Osobną grupę zagrożeń stwarza odpowiedzialność wobec osób fizycznych związana z wypadkami.

Ochrona środowiska

Stale zmieniające się wymogi z zakresu ochrony środowiska powodują konieczność ponoszenia nakładów na inwestycje modernizacyjne zapewniające wyższy poziom bezpieczeństwa w tym zakresie. Dotyczy to nie tylko wymiany starych skorodowanych rurociągów przesyłowych, zużytych zaworów sekcyjnych, czy też wymiany starych węzłów cieplnych. Czasem istnieje potrzeba montażu zaworów odcinających w miejscach, w których ich dotąd nie było, a ich zamontowanie umożliwia likwidację awarii przy mniejszych stratach wody. W innych przypadkach istotne znaczenie może mieć wymiana izolacji termicznej zapewniająca obniżenie poziomu ubytków energii na przesyle, co pozwoli w ostatecznym rezultacie zmniejszyć zużycie paliwa w źródle ciepła, a co za tym idzie poziom emisji gazów i pyłów do atmosfery. Generalnie możemy stwierdzić, że przestrzeganie wymogów ochrony środowiska pociąga za sobą konieczność ponoszenia stale rosnących kosztów, zaś ryzyko niedotrzymywania standardów zawartych w uzyskanych pozwoleniach powoduje, zagrożenie w postaci wymogu płacenia dotkliwych kar z tego tytułu. W ostatnim okresie, w wyniku wdrażania Unijnego programu obniżania poziomu emisji gazów cieplarnianych do atmosfery w naszym kraju powstało istotne zagrożenie bezpieczeństwa finansowego przedsiębiorstw, wykorzystujących do produkcji ciepła miał węglowy. Polega ono na administracyjnym wykreowaniu przez instytucje publiczne sytuacji niepełnego pokrycia poziomu dokonywanej dotąd przez te przedsiębiorstwa emisji zanieczyszczeń do środowiska przyrodniczego wielkością przyznanych im na ten cel uprawnień. Skutkować to może znacznym wzrostem cen energii, bądź zmniejszeniem jej produkcji, a przede wszystkim koniecznością derogacji niewystarczająco efektywnych w tym względzie kotłów oraz zastąpienia ich nowymi, sprawniejszymi. Tu jednak po raz kolejny pojawia się bariera finansowa

trudna do pokonania przy utrzymaniu obowiązującego obecnie modelu regulacji cen, w powiązaniu z zachowawczą polityką banków handlowych, przyjętą przez nie w obliczu kryzysu finansowego.

Bezpieczeństwo zaopatrzenia w paliwo

Katalog zagrożeń bezpieczeństwa funkcjonowania przedsiębiorstw ciepłowniczych nie kończy się na elementach wskazanych powyżej. Węgiel jako paliwo energetyczne jest w Polsce obecnie i będzie w najbliższych latach paliwem podstawowym. Z jego wykorzystaniem w celach energetycznych wiąże się nie tylko problem emisji CO^2, NOX-ów i pyłów, ale również staje się on dobrem coraz bardziej rzadkim w Polsce, co skutkuje nie tylko rosnącymi cenami jego dostaw, ale często brakiem pewności realizacji kontraktów przez krajowych producentów i dostawców. Powstaje więc konieczność zaopatrzenia w ten surowiec na rynkach międzynarodowych, co kreuje ryzyka związane ze zmianami kursów walut oraz problemy logistyczne. Pośrednim skutkiem opisywanej sytuacji jest też potrzeba tworzenia znacznych, przekraczających normy prawne zapasów miału węglowego, z finansowymi i technicznymi efektami ubocznymi tego zjawiska. Również wykorzystanie gazu jako surowca energetycznego nie poprawia warunków bezpieczeństwa dostaw. W tym obszarze rynku obserwujemy bowiem dużą zmienność cenową, niewystarczający poziom zapasów, a także z względu na brak dywersyfikacji źródeł zaopatrzenia w gaz i zmienność uwarunkowań natury politycznej, bezpieczeństwo ciągłości dostaw tego surowca budzi duże wątpliwości.

Bezpieczeństwo pracy

Energetyka cieplna w swojej technicznej i technologicznej specyfice funkcjonowania ma zakodowane zagrożenia człowieka na stanowisku pracy na poziomie ponad przeciętnym. Wiąże się to z procesami wytwarzania energii, jej przesyłania i transformacji, a także ze specyfiką usuwania awarii. Ze względu na wielość czynników powodujących zagrożenia, jak też zmienność sytuacji w jakich one występują, najbardziej skuteczną metodą zapewniania bezpieczeństwa w tym zakresie jest przyjęcie podejścia systemowego do problemu. Jednym z coraz bardziej powszechnych sposobów radzenia sobie z tym zagrożeniem w branży ciepłowniczej jest wdrażanie norm ISO, w oparciu o wykorzystanie polskiej normy: PN-N 18001 – „Systemy zarządzania bezpieczeństwem i higieną pracy. Wymagania."

Wnioski

Interesującym wydaje się zwrócenie uwagi na społeczne postrzeganie problemu bezpieczeństwa energetycznego branży ciepłowniczej na tle energetyki zawodowej, czy gazownictwa z perspektywy dostrzegania ewentualnych skutków braku zapewnienia wystarczającego poziomu tego bezpieczeństwa przez przedsiębiorstwa. Obserwujemy to w kontekście kreowania przez państwo warunków brzegowych umożliwiających zgromadzenie niezbędnych zasobów kapitałowych i ludzkich gwarantujących zapewnienie odpowiednich standardów bezpieczeństwa w tym zakresie.

Można tutaj zaryzykować twierdzenie, że w tym przypadku istnieje odpowiednio krajowa i lokalna perspektywa, co oznacza nie tylko zróżnicowanie zainteresowania odpowiedniego szczebla władz publicznych kwestiami bezpieczeństwa, ale również uznanie tych kwestii z mniej lub bardziej ważne dla tych władz w zależności od rodzaju branży odniesienia problemu.

Najbardziej jaskrawym przejawem takiego podejścia jest odmienność uregulowań prawnych i realizowana w praktyce polityka regulacyjna w odniesieniu do tych rożnych grup podmiotów w zakresie formalnych i rzeczywistych możliwości kreowania zysku poprzez zwrot z kapitału. Ograniczone drogą administracyjną możliwości ciepłownictwa w tym zakresie powodują, że średnia rentowność sektora jest niska, a znaczna dekapitalizacja majątku dalej się utrzymuje[19]. Nie wróży to najlepiej perspektywom zapewnienia w przyszłości bezpieczeństwa energetycznego w obszarze funkcjonowania sektora ciepłowniczego.

Bibliografia

1. Ansoff H.I., *Zarządzanie strategiczne,* PWE, Warszawa 1985;
2. Belka M., *Wpływ polityki gospodarczej Stanów Zjednoczonych na bezpieczeństwo ekonomiczne krajów trzecich,* Bezpieczeństwo ekonomiczne teoria i praktyka, Wyd. Uniwersytetu Łódzkiego, Łódź 1986;
3. Berkowska M., Gil S., Śleszyński J., *Wskaźnik trwałego dobrobytu ekonomicznego ISEW*, „Ekonomista" 2000, nr 6;

[19] Por. Por. Prezes…, s. 54, tabl. 30, str. 143, tabl. 191.

4. Binnendijk H., *Key Findings. Strategic Assesment* 1999, NDU INSS Waszyngton 1999;
5. Domański H., *Na progu konwergencji,* Warszawa 1999;
6. Gierszewska G., B. Wawrzyniak, *Globalizacja wyzwania dla zarządzania strategicznego,* Poltext, Warszawa 2001;
7. *Energetyka cieplna w liczbach 2007,* Prezes Urzędu Regulacji Energetyki, Warszawa 2008;*Granice konkurencji, Grupa Lizbońska*, seria Euromanagement, PFPK- Poltex, Warszawa 1996;
9. Gwiazda A., *Międzynarodowa współzależność ekonomiczna we współczesnym świecie,* PWN, Warszawa 1985;
10. Kołodziejak Z., *Kierunki tworzenia bezpieczeństwa ekonomicznego* "Wektory" 1984, nr 4;
11. Kowalik T., Współczesne systemy ekonomiczne. Powstanie, ewolucja, kryzys, Warszawa 2000;
12. Koźmiński A.K., Zarządzanie. Analiza systemowa procesów i struktur, Warszawa 1977;
13. Kudliński R., Siwiński W., *Szkice o gospodarce światowej*, PWN, Warszawa 1985;
14. Kukułka J., Zięba R. (red.) *Polityka zagraniczna państwa,* UW Warszawa 1992;
15. Kukułka J., *Bezpieczeństwo a współpraca europejska,* Sprawy Międzynarodowe" nr 7/1982;
16. Kukułka J., *Teoria stosunków międzynarodowych,* Scholar, Warszawa 2000;
17. Mensarovic M., Pastel E., *Ludzkość w punkcie zwrotnym,* PWE ,Warszawa 1977;
18. Michałowski S., *Współzależność ekonomiczna w stosunkach Wschód-Zachód,* Sprawy Międzynarodowe, 1984, nr 10;
19. *Między polityką a strategią*, pod red. Kuźniar R., FSM, Warszawa 1994;
20. *Międzynarodowe stosunki gospodarcze,* praca zbiorowa pod red. Budnikowskiego A. I Kaweckiej- Wyrzykowskiej E., PWE, Warszawa 1996;
21. Moczulski L., *Geopolityka. Potęga w czasie i przestrzeni,* Bellona, Warszawa 1999;
22. *Narodowe oraz sojusznicze aspekty kształtu i użycia sił zbrojnych,* AON, Warszawa 1998;
23. M. Perczyński, *Globalne uwarunkowania bezpieczeństwa ekonomicznego,* Warszawa 1990;

24. *Polityka bezpieczeństwa i strategia obronna Rzeczypospolitej Polskiej,* 1992, materiał powielony.
25. *Rozporządzenie Ministra Gospodarki z dnia 15 stycznia 2007r. w sprawie szczegółowych warunków funkcjonowania systemów ciepłowniczych,* Dz. U. z 1 lutego 2007 r. Nr 16 poz. 92, & 2 ust.1,
26. Stankiewicz W., *Węzłowe problemy ekonomiki obrony*, „Myśl Wojskowa" 1985, nr 1;
27. *Słownik języka polskiego,* t.2, PWN, Warszawa 1988;
28. *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 1996;
29. *Ustawa z dnia 10 kwietnia 1997 r. Prawo Energetyczne*, Dz. U. 1997 r. Nr 54 poz. 348, z późniejszymi zmianami, Art.3, ust.2.
30. *Współczesna gospodarka światowa,* red. A. B. Kisiel- Łowczyc, Uniwesytet Gdański, Gdańsk 1994;
31. Zeszyty Naukowe, Nr 1, Zachodniopomorska Szkoła Bussinesu, Kołobrzeg 1998.

DISTRICT HEATING COMPANIES ENERGY SAFETY AS THE COMPONENT OF THE ECONOMY SAFETY

Summary

Safety matters as the area connected with the economics sciences has its reach tradition coming out of many social sciences scientific research works, first of all from such as the philosophy, sociology and the prakseology. The issue of the social perception of the energy safety, treated as the element of the much wider problem we consider as interesting. It concerns both, the district heating branch in comparison to the electric power production sector and the gas production sector observed from the perspective of perceiving the eventual results of not ensuring sufficient level of safety by the companies.

One can observe it in context of creating by the state limiting conditions, which should enable acquisition of necessary capital and human resources guarantying relevant safety standards in that field.

Piotr Dwojacki [*]

LOGISTYCZNE CZYNNIKI BEZPIECZEŃSTWA ENERGETYCZNEGO POLSKI

Wprowadzenie

Bezpieczeństwo energetyczne kraju traktowane jest jako wielka wartość w państwach, których byt zależny jest od zużycia energii. Zasadniczo – im zimniejszy i ciemniejszy kraj, tym większa zależność od energii. A Polska należy do krajów stosunkowo chłodnych i słabo naświetlonych.

Niniejszy materiał inspirowany jest wiedzą o współczesnych problemach energetyki w Polsce i Europie. Równocześnie, dla potrzeb artykułu, wykorzystano wiedzę i wybrane materiały dotyczące kształtowania wizji energetyki w przyszłości. Odwołano się zarówno do „twardej", strategicznej analizy łańcuchów kooperacyjnych w sektorze paliw i energii, jak i do „miękkich" metod kreatywnego przewidywania przyszłości i kształtowania wizji.

1. Podstawowe zagadnienia bezpieczeństwa energetycznego

Przez **bezpieczeństwo energetyczne** rozumie się niezawodność dostaw energii w określonym czasie, przy zapewnieniu wymaganych ilości i parametrów. Bezpieczeństwo energetyczne kraju oznacza, że dostarczana energia zaspokaja potrzeby w stopniu niezbędnym dla ciągłego, sprawnego funkcjonowania państwa.

Zakłócenia dostaw są to odchylenia od wymaganych ilości i parametrów bądź niezgodności momentu dostawy w stosunku do zapotrzebowania. Zakłócenia mogą występować lokalnie i być krótkotrwałe. W skali państwa zakłócenie występują wtedy, gdy dostępu

[*] Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.

do energii pozbawione są rozległe połaci kraju lub istotne ośrodki miejskie lub przemysłowe.

Zagrożenie bezpieczeństwa energetycznego występuje wówczas, gdy istnieje prawdopodobieństwo wystąpienia zakłóceń. Na poziomie państwa zagrożenie jest tym bardziej dotkliwe, im większych obszarów i większej ilości ośrodków może dotyczyć. Jeżeli zagrożenia się urzeczywistniają, stan ten nazywamy **katastrofą energetyczną**.

2. Logistyczne aspekty bezpieczeństwa

Logistyczne aspekty bezpieczeństwa energetycznego wiążą się natomiast z dwoma rodzajami zagadnień. Po pierwsze, znacząca jest kwestia infrastruktury logistycznej, tj. sieci i urządzeń transportowych, oraz magazynów nośników energii bądź paliw gotowych. Po drugie, istotne jest bezpieczeństwo techniczne obiektów energetycznych, związane z zarówno ze sprawnością (bezawaryjnością) funkcjonowania, jak i ochrony przed ryzykami zewnętrznymi, takimi jak katastrofy naturalne czy zagrożenia wojenne bądź terrorystyczne. Po trzecie, kolosalne znaczenie ma fizyczny dostęp do źródeł energii i jej nośników, tj. do złóż surowców, miejsc ich przetwarzania oraz miejsc wytwarzania bądź magazynowania paliw gotowych i energii finalnej.

3. Polityczno-historyczne czynniki bezpieczeństwa energetycznego

Polska bezpieczna pod względem energetycznym to przedmiot publicznej debaty, w której ważne znaczenie mają polityczne oceny ryzyk. Krytyczne znaczenie mają tutaj oceny związane z:

- historią kraju jako położonego między Rosją a Niemcami, czy też, jak chcą niektórzy, na wschodnich rubieżach Unii Europejskiej,
- pożądanym stopniem autarkii (samowystarczalności) bądź uczestnictwa w globalnym rynku energii i jej nośników,
- „patriotycznym" bądź „ustrojowym" charakterem niektórych surowców energetycznych.

Do polityczno-historycznych czynników wpływających na energetykę należą w XXI wieku również nasilające się oczekiwania dotyczące minimalizacji środowiskowych skutków pozyskiwania i wykorzystania energii. Kontekst polityczny wyraża się tu przede wszystkim:

- istnieniem ruchów społecznych i ugrupowań politycznych dążących do promocji bądź narzucenia rozwiązań o charakterze ekologicznym; ruchy te, występujące silnie w Europie Zachodniej, miały w różnych krajach wpływ na kierunki inwestowania w energetykę, w tym np. na decyzje o rozwoju (lub nie) energetyki jądrowej,
- nasilającą się regulacją środowiskową związaną np. z pożądanym udziałem energii ze źródeł odnawialnych, dopuszczalnej emisji dwutlenku węgla do atmosfery, wpływu inwestycji energetycznych na środowisko przyrodnicze, krajobraz, warunki życia społeczności; przejawem takiej regulacji są np. Protokół z Kyoto czy wiążące dla Polski regulacje Unii Europejskiej.

Kontekst polityczny przekłada się często na praktyczne rozwiązania techniczno-ekonomiczne, preferowane za pomocą instrumentów polityki fiskalnej bądź dotacji ze środków publicznych. Do takich rozwiązań należą zarówno rozwiązania prymitywne, jak stawki akcyzy na paliwa i energię, ale i wyrafinowane, jak rynek handlu prawami do emisji dwutlenku węgla.

4. Energia finalna i jej nośniki

Specyfika branży paliwowo-energetycznej (sektora paliw i energii)[1] jako przedmiotu analizy wiąże się z jej wewnętrzną różnorodnością i złożonością. Różnorodność dotyczy w pierwszej kolejności kwestii techniczno-technologicznych, odmiennych dla różnych nośników energii. Nakłada się na to zróżnicowany stopień pionowej i poziomej integracji biznesu paliwowo-energetycznego, zależny tak od spraw technicznych, jak i od strategii firm i regulacji państwowych. Do tego należy brać pod uwagę wymienione w pkt 3 czynniki o charakterze polityczno-historycznym.

Najczęściej w kontekście bezpieczeństwa energetycznego mówi się o surowcach mineralnych: ropie naftowej, gazie ziemnym, węglu kamiennym i brunatnym.

[1] Brak nawet jednolitej, powszechnie przyjętej definicji branży / sektora czy subsektorów. Np. potocznie sektorem energetycznym zwie się elektroenergetykę, dzieloną na podsektory wytwarzania, przesyłu, dystrybucji – uzupełnione funkcją (branżą?) obrotu energią.

Ropa naftowa jest wydobywana w miejscach geograficznie odległych od Polski, przetwarzana w większości na terenie kraju, zaś jej produkty (przede wszystkim paliwa) są wykorzystywane praktycznie na całym terytorium Polski przez bardzo szerokie spektrum odbiorców. Surowiec ten wszelako nie jest niemal wykorzystywany dla potrzeb produkcji energii elektrycznej. System dostaw ropy naftowej jest w zasadzie stabilny i podlega bardziej ryzykom cenowym, niż zagrożeniom o charakterze logistycznym[2]. W zasadzie zagrożenie dostaw dotyczy rafinerii w Płocku – w wypadku katastrofy technicznej rurociągu „Przyjaźń" lub załamania relacji politycznych Polska-Rosja (mało prawdopodobne w związku z bezpośrednim zainteresowaniem Niemiec ciągłością dostaw tą drogą). Warto mieć na uwadze fakt, że skutki logistyczne nawet katastrofy wielkich rozmiarów mogą zostać (technicznie) zniwelowane przez substytucyjne dostawy paliw gotowych transportem drogowym bądź kolejowym. Nie bez znaczenia będą też pojemności magazynów paliw, sukcesywnie zwiększane – głównie przez podmioty krajowe.

Gaz ziemny dla potrzeb Polski wydobywany jest głównie w Rosji, zaś około trzecia część krajowego zapotrzebowania pokrywana jest ze złóż krajowych. Surowiec ten konsumowany jest przez przemysł (głównie chemiczny) oraz gospodarstwa domowe. Wytwarzanie energii elektrycznej stanowi dla sektora gazowego margines.

Logistyka nafty, paliw ropopochodnych i gazu ziemnego obejmuje różne możliwości transportowe, pośród których dominuje w Polsce transport rurociągami (lądowe rurociągi naftowe i produktowe, gazociągi), zaś niewielkie znaczenie ma transport drogą morską (terminale przeładunkowe). Wyzwaniem logistycznym jest zapewnienie pojemności magazynowych dla zapewnienia buforu bezpieczeństwa dostaw. W sferze dostaw gazu ziemnego dość dramatycznym zagrożeniem dla bezpieczeństwa Polski było wznowienie dostaw gazu z Rosji do Europy przez Ukrainę (luty 2009). Paradoksalnie, styczniowy „kryzys ukraiński"[3], gdy odcięte zostały dostawy do wielu krajów Europy południowo-wschodniej, ominął Polskę – znacznie silniej były

[2] Nie są rozpatrywane w tym miejscu przedsięwzięcia wydobywcze podejmowane prze polskie firmy w rejonie Morza Północnego, Konga czy Azji Środkowej (np. Kazachstan) i Południowo-Wschodniej.

[3] Zaprzestanie dostaw gazu ziemnego z Rosji prze terytorium Ukrainy, styczeń 2009.

zagrożone kraje takie, jak Czechy, Austria, Słowenia, Włochy czy Chorwacja (nie mówiąc już bezpośrednio poszkodowanych: Słowacji, Rumunii, Węgrach, Serbii, Bułgarii i Grecji. Natomiast wznowienie dostaw – z uwagi na nowo ustanowione relacje handlowe – wiązało się z ryzykiem znaczącego ograniczenia dostaw dla polskiego sektora chemii ciężkiej (Puławy, Płock, Tarnów).

Z punktu widzenia powyższych uwarunkowań istotne dla bezpieczeństwa zaopatrzenia Polski w gaz stają się przedsięwzięcia dywersyfikacyjne, związane z budową lądowej i morskiej infrastruktury logistycznej – niekoniecznie na terytorium Polski. Wśród tych przedsięwzięć wymienić należy:

- projekty budowy gazociągów przesyłowych z basenu Morza Północnego, dyskutowane w Polsce od niemal 20 lat,
- projekt budowy gazociągu Nabucco, potencjalnie włączającego Czechy i Polskę w system dostaw z basenu Morza Kaspijskiego,
- wciąż dyskusyjny, choć przesądzony podjęciem prac legislacyjnych projekt budowy terminalu gazowego w wybranym porcie morskim (wybór polityczny dokonany w Polsce dotyczy Świnoujścia, bez uwzględnienia istotnych przesłanek logistycznych związanych z budową infrastruktury morskiej – terminal, ale i lądowej – magazyny i rurociągi oraz kierunek przesyłu gazu pozyskanego drogą morską[4]).

Węgiel kamienny pochodzi głównie ze złóż rodzimych i konsumowany jest przede wszystkim dla potrzeb związanych z wytwarzaniem energii elektrycznej i cieplnej. Ten nośnik energii jest szczególnie zakorzeniony w polskiej tradycji i obficie reprezentowany politycznie. W zasadzie eksploatacja złóż nie podlega kryteriom ekonomicznym, zaś przedsięwzięcia restrukturyzacyjne nie cieszą się jednomyślnością ani na gruncie społecznym, ani analiz eksperckich. W sferze logistyki kluczowe znaczenie ma transport kolejowy w granicach kraju. Nie bez znaczenia pozostają, podlegające wszelako turbulencjom, dostawy drogą morską (z geograficznie odległych miejsc eksploatacji) oraz kolejowe (z Rosji i Ukrainy). **Węgiel brunatny** z kolei w całości pochodzi ze źródeł krajowych, a jego podstawowym zastosowaniem jest produkcja energii elektrycznej. Jest to surowiec, którego wydobycie i użytkowanie wiąże się z najmniejszą złożonością

[4] Patrz głosy w dyskusji na temat lokalizacji terminalu LNG [4] i [5].

logistyczną: miejsce wydobycia i spalenia jest właściwie to samo, nie ma istotnych problemów związanych z magazynowaniem oraz transportem – praktycznie nie występuje konieczność (ani ekonomiczne uzasadnienie) przewożenia surowca na większe odległości. Surowiec ten wszelako jest w Polsce najbardziej dyskusyjny pod względem społeczno-środowiskowym i ma w związku z tym ograniczone możliwości ekspansji – pomimo występowania wielkich, niezagospodarowanych złóż w Polsce środkowej i środkowo-zachodniej.

Energia elektryczna dla potrzeb krajowych wytwarzana jest głównie w oparciu o węgiel kamienny i brunatny. Co ważne z perspektywy bezpieczeństwa energetycznego: energia elektryczna na polskie potrzeby wytwarzana jest w Polsce, praktycznie nie podlega też możliwościom tradycyjnie rozumianego magazynowania. Z logistycznego punktu widzenia do niedawna kluczowe wydawały się kwestie sprawności technicznej sieci wysokich i średnich napięć, ulegające od lat 80 systematycznej dekapitalizacji bądź nawet fizycznej dewastacji. Na poziomie lokalnym może to owocować ponawianiem się lokalnych zakłóceń dostaw o potencjalnie katastrofalnych skutkach (por. całkowity brak zasilania Szczecina w kwietniu 2008 roku). Na poziomie bezpieczeństwa kraju, z perspektywy roku 2009 można stwierdzić dość autorytatywnie, że Polska w sferze elektroenergetyki jest krajem autarkicznym, czego skutkiem mogą być niedobory mocy w systemie energetycznym jako całości. Sytuacja ta stawia politykę gospodarczą przed wyzwaniami:

- włączenia infrastruktury krajowej w międzynarodowy system dostaw,
- budowy nowych mocy wytwórczych.

Z perspektywy relacji międzynarodowych kluczowe znaczenie mają przedsięwzięcia integrujące polski system elektroenergetyczny z systemem ukraińskim oraz systemem Unii Europejskiej. W pierwszej sferze rzecz dotyczy odbudowy zdewastowanych połączeń bądź budowy nowych z elektrowniami w miejscowościach Chmielnicki i Równe. W drugim przypadku mowa jest na razie głównie o „łączniku" Polska-Litwa w kontekście rozbudowy elektrowni jądrowej w Ignalinie. Nie bez znaczenia będą także przedsięwzięcia związane z bałtyckim pierścieniem energetycznym oraz zwiększaniem możliwości przesyłu w relacjach Polska-Czechy-Niemcy.

Inne źródła energii. Powyżej przedstawiono zarys uwarunkowań logistycznych związanych z zaopatrzeniem w energię – głównie

w kontekście paliw kopalnych. Odniesiono się nieznacznie do połączenia polskiego systemu elektroenergetycznego ze źródłami energii jądrowej Ukrainy i Litwy. Pozostaje jednak istotna kwestia zaopatrzenia w energię z innych źródeł. Nowe zdolności w sferze wytwarzania energii elektrycznej wiążą się z:

- jednym, względnie skonkretyzowanym projektem rządowym – budową elektrowni jądrowych w Żarnowcu i Klempiczu,
- jednym projektem o nie przesądzonym jeszcze charakterze prawnym (rekomendowane jest partnerstwo publiczno-prywatne) – budowy elektrowni wodnej w Ciechocinku,
- coraz bardziej licznymi inicjatywami związanymi z budową nowych mocy wytwórczych w oparciu o gaz ziemny i węgiel, w tym budowy elektrowni i elektrociepłowni o parametrach źródeł systemowych,
- polityką Unii Europejskiej, a w efekcie polskich regionów, w odniesieniu do energii z rozproszonych źródeł odnawialnych.

Równolegle do sfery wytwórstwa podejmowane są inicjatywy związane z nowym wykorzystaniem węgla kamiennego – przez budowę instalacji zgazowania. Polska ma pod tym względem szansę stać się pionierem rozwiązań w skali globalnej, tak w sferze technologii chemicznej – pozyskiwania gazu (substytucyjnego wobec gazu ziemnego), jak i logistyki magazynowania dwutlenku węgla. Projekty, współfinansowane w znacznym stopniu przez instytucje Unii Europejskiej, mogą jednak okazać się chybionym kierunkiem badań. W każdym razie – biorąc pod uwagę wskazane wcześniej uwarunkowania „patriotyczno-historyczno-polityczne" na rzecz podjęcia tego kierunku działań uformowało się bardzo silne lobby, do którego należą liczni polscy parlamentarzyści, tak związani ze Śląskiem, górnictwem, jak i przemysłem chemicznym. Pomijając zatem kwestie możliwych do oszacowania kosztów i ryzyk, wysoce prawdopodobne jest podjęcie przez Polskę tego kierunku rozwoju, łącznie z uczynieniem z tego zagadnienia hasłem przewodnictwa polskiego w Unii Europejskiej w 2011 roku.

Wszystkie wymienione powyżej projekty wiążą się z ryzykami o charakterze społeczno-systemowym. Niemal każde z przedsięwzięć będzie przedmiotem publicznej debaty i da asumpt do licznych protestów na tle politycznym i ekologicznym – w tym kwestionowane są lub będą przedsięwzięcia związane z pozyskiwaniem energii ze źródeł odnawialnych (stopień wodny na Wiśle, farmy wiatrowe na Pomorzu). Ale wszystkie te kierunki będą wiązać się z wyzwaniami o charakterze

logistycznym. W przypadku przedsięwzięć dużych należy oczekiwać przebudowy w ciągu 15-20 lat znacznej części infrastruktury dostaw paliw i energii, jak również magazynowania paliw. Ale kolosalne znaczenie może mieć też segment działań związanych z rozwojem drobnych, rozproszonych źródeł energii, budowanych w oderwaniu od obecnie istniejącego systemu logistycznego.

5. Przewrót w logistyce zaopatrzenia w energię?

W Polsce zużycie energii na mieszkańca jest czterokrotnie niższe, niż w rozwiniętych społeczeństwach Europy Zachodniej. Obecne źródła energii, w momentach szczytowego zapotrzebowania, z ledwością wystarczają na pokrycie potrzeb krajowych. Wzrost gospodarczy, aby „dogonić" Zachód, wiąże się z oczekiwanym wzrostem zapotrzebowania na energię. Nie do pomyślenia w Polsce jest tzw. „wzrost zeroenergetyczny", tzn. oparty na rozwoju i zmianie struktury gospodarki w kierunku nie wymagającym dodatkowego „wsadu" w postaci paliw i energii finalnej. Co więcej, zaburzenia klimatyczne rodzą nowe wymagania związane z pogodzeniem globalnego ocieplenia klimatu z regionalnym oziębieniem, oczekiwanym np. w basenie Morza Bałtyckiego. Prognozowanie zapotrzebowania na energię w skali makro staje się zatem coraz bardziej ryzykowne – i obarczone jest wielkim marginesem błędu. To **pierwsze przewartościowanie** myślenia o energetyce w XXI wieku.

Drugie z przewartościowań wiąże się z energetyką na poziomie lokalnym. Energetyka lokalna w Polsce to przede wszystkim kotłownie i ciepłownie zaopatrujące miejskie sieci ciepłownicze. W większych miastach występują źródła kogeneracyjne (elektorociepłownie), w których ubocznym produktem wobec ciepła sieciowego jest energia elektryczna dostarczana do systemu krajowego. Taka struktura wydaje się oczywista z punktu widzenia zwyczajów panujących w wielu państwach i społeczeństwach, jak również w wielu firmach energetycznych. **Drugie przewartościowanie** energetycznego myślenia wiąże się z rozwojem nowych technik pozyskiwania energii oraz technologii energooszczędnych – właśnie na poziomie lokalnym. Niemal niezauważalnie, „tradycyjnymi" źródłami energii stały się elektrownie wiatrowe, źródła geotermalne czy kotłownie opalane słomą. Tego rodzaju przedsięwzięcia nie są już traktowane jako innowacyjne, bowiem dobrze znane są techniki i technologie z nimi związane, jak również

przyjmowane rozwiązania organizacyjno-handlowe. Ale hasło „gminy samowystarczalnej energetycznie" nie upowszechniło się jeszcze, co więcej, traktowane jest nieco z przymrużeniem oka.

Jeszcze mniejsze znaczenie przywiązuje się do rozwiązań o poziom bardziej lokalnych, towarzyszących pojedynczym gospodarstwom rolnym i domowym. Tym bardziej, że rozwiązania domowe czy przydomowe wymykają się kryteriom racjonalności ekonomicznej, szczególnie wśród osób względnie majętnych. Z lekceważeniem można traktować mały, przydomowy wiatrak bądź panel słoneczny, szczególnie w kraju tak mało nasłonecznionym, jak Polska. Zresztą – kiedyś z lekceważeniem można było podchodzić do furtki Tomasza Edisona, będącej wszak napędem dla domowej „elektrowni". Tym niemniej taki rozwiązania są coraz częstsze, choćby ze względów estetycznych. A są one zaledwie wierzchołkiem góry złożonej z rozwiązań w rodzaju dom pasywny czy pompa ciepła, związanymi już z technologiami budowlanymi, wentylacyjnymi, termoizolacyjnymi – popartymi rachunkiem ekonomicznym. I – idąc jeszcze dalej – z coraz poważniej traktowanymi przedsięwzięciami związanymi z zagospodarowaniem odpadów i odchodów (np. biogazownie).

Drobne przedsięwzięcia energetyczne traktowane są w rezultacie jako margines wobec źródeł tradycyjnych. Ale **trzecie przewartościowanie** w myśleniu o energetyce może dotyczyć właśnie rozwiązań drobnych, opartych na innowacjach, na myśleniu „w poprzek" energetycznej tradycji wieku XX. Skutkiem tego przewartościowania może być na przykład rezygnacja ze scentralizowanych źródeł energii – takich jak elektrownie systemowe. Rezygnacja z sieci wysokich napięć. Rezygnacja z gazociągów przesyłowych. Powrót do lokalnego zaopatrywania się w energię, od którego cywilizacja „odzwyczaiła się" w wieku XX.

Zakończenie

Bezpieczeństwo energetyczne Polski wymaga potężnych inwestycji w infrastrukturę energetyczną i około energetyczną. Zarówno inwestycji w moce wytwórcze, jak i zdolności transportowe, przeładunkowe i magazynowe.

Decyzje inwestycyjne podejmowane są na miarę współczesnej wiedzy, w oparciu o ekstrapolację trendów występujących w XX wieku. Na decyzje wpływ mają też czynniki polityczno-historyczne, działanie

lobby i inne, nie mających wiele wspólnego z rachunkiem ekonomicznym.

Tymczasem – niepostrzeżenie – następuje szybki rozwój innowacji i drobnych, lokalnych przedsięwzięć, których łączna skala może – w przyszłości – znacząco zaważyć na wielkości i strukturze zasobów energetycznych wykorzystywanych w biznesie i życiu prywatnym. W rezultacie energetyka ma szansę na pełzający przewrót technologiczny o globalnych skutkach.

Bibliografia

1. Dwojacki P. *Firma z wizją*, "Personel", Nr 10/1998.
2. Dwojacki P. *Innowacyjna ENERGA. Warunki Rozwoju innowacji energetycznych*, CBR Energa, 2009.
3. Hlousek J. *Zarządzanie innowacjami. Propozycja modelu dla ENERGA S.A.*, GFKM, 2008.
4. *Terminal w Gdańsku albo wcale*, rozmowa ze Stanisławem Corą, „Dziennik Bałtycki", 25.01.2009.
5. Tyszecki A. *Terminal LNG tylko w Gdańsku,* „Dziennik Bałtycki", 5.02.2009.
6. *Ustawa o inwestycjach w zakresie terminalu regazyfikacyjnego skroplonego gazu ziemnego w Świnoujściu*, projekt z dn. 27.03.2009, Ministerstwo Skarbu Państwa, materiał powielany .

LOGISTIC FACTORS OF ENERGY SAFETY IN POLAND

Summary

The presented study is a short review of factors influencing energy industry in Poland. Current technical elements and dependence on logistic factors were described – especially in oil and gas industry. Coal as dominant energy raw material in Poland was taken under consideration, including future innovations in coal-based technologies. Paper covers also electro-energy industry as an area of changes, especially in power-grid and energy generation development. The challenge for Polish economy is: to undertake great infrastructural projects.

Historical and social habits were taken into account. But the study contains some future circumstances: radical changes in energy sources demand and market structure are expected. So dynamic and changing environment may determine future shape and vision of energy industry – including decrease of demand on logistic services and lowering responsiveness of energy industry to logistic factors of safety.

Krzysztof Ficoń[*]

LOGISTYCZNE ASPEKTY BEZPIECZEŃSTWA ENERGETYCZNEGO POLSKI

Streszczenie

W pracy przedstawiono logistyczną koncepcję kształtowania bezpieczeństwa energetycznego Polski w XXI wieku, w odniesieniu do paliw płynnych. We wstępie omówiono pojęcie i narodową strategię bezpieczeństwa energetycznego oraz przedstawiono aktualny bilans energetyczny Polski. W dalszej części omówiono zasadnicze kierunki dywersyfikacji dostaw paliw płynnych do Polski, akcentując rolę i znaczenie logistycznych systemów transportowych. Zwrócono uwagę także na dominującą rolę strategii geopolitycznych w budowaniu optymalnych systemów dostaw surowców energetycznych do Polski. W zakończeniu sformułowano podstawowe zasady optymalizacji logistycznych łańcuchów dostaw surowców energetycznych do Polski.

1. Pojęcie i różne wymiary bezpieczeństwa energetycznego

Najczęściej pojęcie bezpieczeństwa jest definiowane dość kategorycznie jako stan braku zagrożeń dla realizowanej misji i linii rozwojowej danego systemu. Jest to określenie dość względne, albowiem bardziej właściwe definiuje bezpieczeństwo jako pewien stan stabilny, w którym poziom zagrożeń jest akceptowany i pozostaje pod świadomą kontrolą organów odpowiedzialnych za gwarantowanie tego bezpieczeństwa. Ta uwaga wynika z faktu, że każdy wielki system społeczno-polityczno-gospodarczy, w szczególności taki jak instytucja państwa pozostaje pod ciągłą presją różnorodnych zagrożeń generowanych przez nieskończone spektrum źródeł zewnętrznych, wewnętrznych oraz celowych i losowych, a także naturalnych,

[*] Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu w Gdyni.

cywilizacyjnych, klimatycznych itp. W systemie bezpieczeństwa narodowego można wyróżnić trzy zasadnicze filary (podsystemy):

- bezpieczeństwo zewnętrzne (polityczne, militarne, międzynarodowe),
- bezpieczeństwo wewnętrzne (publiczne, społeczne, zdrowotne, edukacyjne),
- bezpieczeństwo gospodarcze (finansowe, komunikacyjne, energetyczne).

Bezpieczeństwo gospodarcze dotyczy tzw. strategicznych sektorów gospodarczych, których udział w gospodarce narodowej jest dominujący i bezpośrednio rzutuje na standardy cywilizacyjne i poziom bezpieczeństwa ogólnonarodowego. W dalszej części zajmiemy się jedną z zasadniczych form bezpieczeństwa gospodarczego, jakim jest bezpieczeństwo energetyczne rozumiane jako bilansowanie się w skali państwa globalnego strumienia przepływu energii czyli popytu (zapotrzebowania) i podaży (zużycia). Warunek bilansowania oznacza pełne pokrycie krajowych potrzeb energetycznych (społecznych, przemysłowych) przez odpowiednio zorganizowany i utrzymany system dostaw dystrybucyjnych nośników energii do końcowych ogniw konsumenckich.

Zgodnie z ustawą „Prawo energetyczne" pojęcie bezpieczeństwa energetycznego oznacza stan gospodarki umożliwiający pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa i energię, w sposób technicznie i ekonomicznie uzasadniony, przy zachowaniu wymagań ochrony środowiska"[1]. Tak rozumiane pojęcie bezpieczeństwa energetycznego może być sprowadzone do kategorii bilansu energetycznego państwa, którego dodatnie saldo wskazuje na spełnienie warunków formalnych nakładanych na strategiczny sektor paliwowo-energetyczny. Warunkami dostatecznymi tego bezpieczeństwa są gospodarcze kryteria efektywności ekonomicznej, posługiwanie się odpowiednio sprawną technologią oraz spełnienie wymagań ochrony środowiska naturalnego.

Jak wynika z tabeli 1 formalne bezpieczeństwo energetyczne większości krajów Unii Europejskiej jest zadawalające i cechuje się statystyczną nadwyżką mocy produkcyjnych nad krajowym zapotrzebowaniem. Aktualnie Polska posiada nadwyżkę mocy produkcyjnych najbardziej syntetycznej energii elektrycznej rzędu 33%

[1] *Ustawa z dn. 10 kwietnia 1997r. – Prawo energetyczne.* Dz. U. nr 54 / 1997, art. 3 § 16 z późn. zm.

ponad potrzeby gospodarki narodowej. Średnia dla badanej grupy krajów UE jest też dość wysoka i wynosi ponad 28%, co pozwala na elastyczne konfigurowanie krytycznych zapotrzebowań poszczególnych krajów członkowskich UE.

Teoretyczna definicja bezpieczeństwa energetycznego całkowicie pomija jego aspekt praktyczny i fizyczną stronę realizacji tego zaopatrzenia, która odbywa się za pomocą współczesnych sieci i technologii logistycznych. Fizyczne przepływy surowców, materiałów czy produktów z jednego punktu czasoprzestrzeni od innego, to istota procesów logistycznych, przebiegających we wszystkich wymiarach – mikroskali (przedsiębiorstwa), mezoskali (sektora energetycznego), makroskali (kraju, państwa) i wreszcie w skali globalnej np. Unii Europejskiej czy światowej. Dlatego z całą pewnością można powiedzieć, że o poziomie naszego bezpieczeństwa energetycznego decyduje logistyka – jej systemy infrastrukturalne i sieci przesyłowe oraz towarzyszące tym przepływom fizycznym transakcje handlowe, w tym zwłaszcza zakupy zaopatrzeniowe, a bardziej konkretnie biznesowy wybór dostawców rynkowych, czyli źródeł zaopatrzenia. Niestety monopolistyczna pozycja strategicznych, światowych dostawców surowców energetycznych, głównie Rosji sprawia, że rynkowe kryteria ekonomiczne i biznesowe standardy funkcjonowania logistycznych łańcuchów dostaw ustępują miejsca kryterium geopolitycznym i skupionym wokół nich strukturom oligarchii paliwowo-energetycznych. Krystaliczną strukturę bezpieczeństwa energetycznego Polski zasadniczo komplikują obowiązujące także w tym sektorze standardy gospodarki rynkowej, które prawnie obligują państwa i ich rządy do demonopolizacji i prywatyzacji wszystkich dziedzin działalności gospodarczej. Praktycznie we wszystkich sektorach gospodarczych powinny dominować zasady otwartej, wolnorynkowej gry biznesowej, ukierunkowane na uzyskanie maksymalnej efektywności ekonomicznej, a tym samym wysokiej konkurencyjności rynkowej, w otwartym światowym systemie gospodarki globalnej.

Krystaliczną strukturę bezpieczeństwa energetycznego Polski zasadniczo komplikują obowiązujące także w tym sektorze standardy gospodarki rynkowej, które prawnie obligują państwa i ich rządy do demonopolizacji i prywatyzacji wszystkich dziedzin działalności gospodarczej.

Tab. 1.

Bilans potrzeb i możliwości energetyki europejskiej – 2005r.

LP	Kraj UE	Zapotrzebowanie szczytowe na moc (GW)	Moce zainstalowane netto [GW]	Nadwyżka mocy [5]
1.	Dania	6,2	12,42	50,1
2.	Francja	72,4	115,41	37,3
3.	Portugalia	7,1	10,96	35,2
4.	Włochy	49,2	75,51	35,1
5.	Hiszpania	35,3	53,25	33,7
6.	Polska	22,3	33,42	33,3
7.	Niemcy	84,0	119,47	29,7
8.	Luksemburg	0,9	1,25	28,0
9.	Finlandia	12,4	16,26	23,7
10.	Holandia	15,2	19,56	22,3
11.	Irlandia	3,8	4,71	19,3
12.	Wlk. Brytania	64,2	79,12	18,9
13.	Grecja	9,1	10,91	16,5
14.	Szwecja	26,0	30,89	15,8
	Średnia UE	**29,15**	**41,65**	**28,49**

Źródło: Biuletyn Informacyjny PGNIG 2007r.

Praktycznie we wszystkich sektorach gospodarczych powinny dominować zasady otwartej, wolnorynkowej gry biznesowej, ukierunkowane na uzyskanie maksymalnej efektywności ekonomicznej, a tym samym wysokiej konkurencyjności rynkowej, w otwartym światowym systemie gospodarki globalnej. Podstawą udanej integracji europejskiej były rynkowe kryteria ekonomiczne, które programowo stymulują rozwój przedsiębiorczości, gospodarności i wysoką konkurencyjność biznesową wszystkich podmiotów gospodarczych, tj. firm, przedsiębiorstw, korporacji a także regionów, narodów i państw.

2. Bilans energetyczny Polski

Sytuacja surowcowa Polski w zakresie własnych źródeł surowców energetycznych nie jest wcale aż tak niekorzystna jak wygląda to w obiegowych opiniach i komentarzach medialnych. Bilans energetyczny Polski opiera się przede wszystkim na węglu kamiennym i brunatnym, które zaspokajają krajowe potrzeby energetyczne na poziomie 65%.

Tab. 2.
Zużycie i produkcja nośników energetycznych w Polsce w roku 2005

Nośnik energii	Produkcja krajowa		Import	
	[jm]	%	[jm]	%
Ropa naftowa	0,8 [mln t.]	4 %	16,6 [mln t.]	96 %
Gaz płynny	277 [tys.t.]	16 %	1.493 [tys. t.]	84 %
Gaz ziemny	8,7 [mln m3]	32 %	4,1 [mln m3]	68%
Paliwa płynne	1,5 [mln t.]	88 %	11 [mln t.]	12%
Węgiel kamienny	100,6 [mln t.]	100 %	-	-
Węgiel brunatny	60,5 [mln t.]	100 %	-	-
Energia elektryczna	150,8 [TWh]	100 %	-	-

Źródło: Biuletyn Informacyjny PGNIG 2007r.

Udział paliw płynnych szacuje się na poziomie 22%, natomiast udział gazu w krajowym bilansie energetycznym to ok. 12% ogólnego zapotrzebowania. Niestety udział pozostałych tzw. alternatywnych źródeł energii w ogólnym bilansie energetycznym Polski jest marginalny i formalnie biały węgiel, czyli hydroenergetyka partycypuje w produkcji energii elektrycznej na poziomie ok. 1%, a notowania pozostałych źródeł – energii wiatrowej, geotermalnej i bioenergii są wręcz symboliczne nie przekraczające łącznie 1%. Wyjątkowym ewenementem polskiego systemu energetycznego jest całkowity brak energetyki jądrowej i totalne oparcie się na brudnej energii pochodzącej ze spalania węgla, co w dłuższej perspektywie generuje bardzo niekorzystne trendy i konsekwencje ekonomiczne, społeczne i ekologiczne[2].

Praktycznie cała polska elektroenergetyka bazuje na krajowych zasobach węgla kamiennego (100 mln ton / rok) i brunatnego (60 mln ton /rok), dlatego w produkcji energii elektrycznej jesteśmy samowystarczalni, a zainstalowane moce produkcyjne pozwalają na swobodny eksport energii elektrycznej do wspólnej sieci europejskiej.

[2] Obecnie na świecie działają 442 elektrownie jądrowe, pokrywające ponad 16% ogólnoświatowego zapotrzebowania na energię elektryczną. Około 80% z nich ma reaktory działające ponad 15 lat. W budowie jest 28 nowych obiektów, z których wiele ma zastąpić elektrownie starszych typów, w naturalny sposób wycofywanych z eksploatacji. Polska jest „białą plamą" na mapie Europy, będąc otoczona krajami dysponującymi „prądem z atomu".

Polska posiada też znaczące zasoby gazu ziemnego, które wprawdzie nie gwarantują nam samowystarczalności w zakresie niebieskiego nośnika, ale pokrywają potrzeby krajowe na poziomie 30-35%. Prowadzone są intensywne badania geologiczne nad pozyskaniem nowych źródeł gazu ziemnego, gdyż produkcja krajowa jest najtańsza i najbardziej bezpieczna. Krajowe wydobycie gazu ziemnego osiąga obecnie poziom ok. 6 mld m^3 rocznie, co sukcesywnie coraz bardziej uniezależnia nas od importu. Zupełnie w śladowych ilościach wydobywamy z własnych źródeł ropę naftową, aktualny poziom wydobycia to ok. 850 tys. ton rocznie, co wobec potrzeb rzędu 16-17 mln ton jest wkładem symbolicznym. Krajowe badania i prognozy geologiczne są bardziej korzystne dla dalszego pozyskiwania nowych źródeł gazu niż ropy naftowej.

Aktualnie najbardziej bezpieczna i stabilna jest sytuacja w elektroenergetyce, gdzie własne krajowe duże elektrownie oraz dobrze rozwinięte linie przesyłowe gwarantują produkcję prądu na wymaganym poziomie i sprawny jego przesył do końcowych odbiorców. O efektywności krajowych systemów elektro-energetycznych decyduje ich sprawność produkcyjna i zaawansowanie technologiczne. Sprawność coraz starszych polskich elektrowni jest niezadawalająca, co wynika z prostego rachunku ekonomicznego, mówiącego o tym, że ok. 6-8% wyprodukowanej energii elektrycznej jest zużywane bezpośrednio do jej wytworzenia przez danego producenta. W miarę starzenia się polskiej energetyki – 75% bloków energetycznych w polskich elektrowniach ma ponad 20 lat, ta sprawność będzie sukcesywnie się obniżać, a koszty nowych inwestycji w sektorze energetycznym są wyjątkowo wysokie[3]. Perspektywicznym problemem polskiej energetyki są głównie źródła surowcowe i trwający bez końca monopol węgla kamiennego, gwarantujące pracę i produkcję energii elektrycznej na coraz wyższym poziomie dostaw.

Relatywnie większe bezpieczeństwo panuje w sektorze naftowym niż gazowym, co wynika przede wszystkim z usytuowania i przepustowości logistycznych sieci dostaw, których krytycznymi elementami są pierwotne źródła dostaw, czyli zakontraktowane i realizowane wielkości dostaw odpowiednio ropy naftowej i gazu ziemnego. Większe

[3] Na rok 2008 potencjał produkcyjny polskiej energetyki tworzyło: 20 elektrowni przemysłowych i 57 dużych elektrociepłowni, których moc użyteczna wynosiła łącznie 35 tys. MW, przy średnim zapotrzebowaniu rzędu 22 MW w skali roku. Na łączną liczbę funkcjonujących 57 bloków 120 MW wiek prawie 1/3 przekracza 40 lat.

bezpieczeństwo rynku paliwowego w Polsce wynika przede wszystkim z lepiej i bardziej racjonalnie zorganizowanej i zdywersyfikowanej logistycznej sieci dystrybucji ropy naftowej. Paradoksalnie krajowe, eksploatowane pokłady ropy naftowej są kilkakrotnie mniejsze niż zasoby gazu ziemnego, a sytuacja rynkowa jest zupełnie odwrotna. Zarówno w przypadku ropy naftowej, jak też gazu ziemnego jesteśmy w dominującym stopniu uzależnieni do naszego rosyjskiego dostawcy i jego mieszanych polityką standardów biznesowych.

Ropa naftowa jest dostarczana do Polski transkontynentalnym rurociągiem „Przyjaźń", który z powodzeniem obsługuje potrzeby importowe Polski, częściowo zaspokaja zapotrzebowanie gospodarki niemieckiej oraz sprawnie realizuje pokaźny eksport ropy rosyjskiej przez Port Północny. Wysoką sprawność rurociągu Przyjaźń i bezpieczeństwo dostaw tego strategicznego surowca gwarantuje przede wszystkim północna jego odnoga łącząca rafinerię Płock z rafinerią Gdańsk i dalej Portem Północnym. Rurociągiem Pomorskim można przesłać rocznie ok. 30 mln ton ropy, a co najważniejsze w obu kierunkach południe-północ i północ-południe. Gdyby więc zaistniała pilna konieczność można sprowadzić do Naftoportu w Porcie Północnym praktycznie dowolne ilości importowanej ropy naftowej i częściowo przetwarzać ją w Rafinerii Gdańsk, częściowo tłoczyć do drugiej największej Rafinerii Płock[4]. W ten sposób można byłoby całkowicie uniezależnić się od chimerycznych dostaw partnera rosyjskiego i drogą morską pokryć niemal 100% zapotrzebowanie Polski, szacowane rocznie na poziomie 18-19 mln ton surowca. Oczywiście problemem strategicznym pozostają zakupy rynkowe tak wielkich ilości ropy, gdyż jeśli nie były wcześniej kontraktowane odpowiednimi umowami długoletnimi ich cena rynkowa jest znacznie wyższa.

Wyjątkowym problemem logistycznym jest transport drogą morską tej ropy oraz dostępność wymaganej liczby tankowców, co przy skromnych 10 mln ton rocznie oznacza np. 100 rejsów tankowcami o ładowności 100 tys. ropy, czyli średnio co 3 dni należałoby rozładować jeden 100 tysięcznik w Porcie Północnym. Jak dotychczas rurociąg Pomorski jest wykorzystywany przede wszystkim do intensywnego przepływu ropy rosyjskiej do Gdańska, a do rzadkości należą przepływy

[4] Rafineria Płock była projektowana i jest dostosowana, głównie do przerobu ciężkiej ropy rosyjskiej, dlatego masowe przetwórstwo importowanej, zamorskiej ropy głownie arabskiej, zaliczanej do kategorii lżejszej, wymagałoby kosztownej modernizacji niektórych ciągów technologicznych.

zamorskiej ropy z Gdańska do Płocka. Wszystkie te czynniki sprawiają, że Gdański Naftoport i rurociąg Pomorski są strategicznymi elementami polskiej infrastruktury energetycznej i dlatego stanowią bardzo atrakcyjny obiekt dla inwestorów, zwłaszcza rosyjskich.

Tab. 3.
Udział nośników energii w produkcji energii w roku 2005

Kraj	Węgiel [%]	Gaz [%]	Ropa [%]	Energia wodna [%]	Energia atomowa[%]
Unia Europ.	15	20	40	14	11
Polska	65	12	22	1	0
Ukraina	29	46	10	13	2

Źródło: Biuletyn Informacyjny PGNIG 2007r.

Aktualnie możemy odczuwać satysfakcję, z tego że krajowe zasoby węgla zwłaszcza kamiennego zapewniają nam bezpieczeństwo energetyczne i niezależność od dostaw z importu. Jednocześnie należy być świadomym światowych tendencji w zakresie ograniczenia emisji gazów cieplarnianych, głównie dwutlenku węgla CO^2, co zmusi przede wszystkim Polskę do ograniczenia wydobycia i spalania tego surowca dla potrzeb energetycznych.

Nowoczesne technologie ekologicznie czystej gazyfikacji węgla są ciągle zbyt kosztowne i ekonomicznie nieopłacalne w ogólnym bilansie państwa. Polska jest w skali całej Unii Europejskiej osamotnionym potentatem w zakresie wydobycia węgla i produkcji z tego surowca energii elektrycznej, dlatego coraz trudniej będzie nam zachować dotychczasowy parytet węgla w krajowym bilansie energetycznym.

Przepisy Unii Europejskiej wymagają, aby kraje członkowskie miały rezerwy paliw i zapasów ropopochodnych co najmniej na 90 dni pokrycia zapotrzebowania krajowego, a docelowo poziom ten powinien być odniesiony do 120 dni. Krajowe możliwości przechowywania zapasów ropopochodnych szacowane są na poziomie 70 dni i wbrew zaleceniom UE, struktura tych zapasów jest niekorzystna, gdyż aktualne prawo polskie dopuszcza w tej strukturze aż 80% zapasów czystego

surowca, czyli ropy naftowej[5]. Z punktu widzenia bezpieczeństwa energetycznego państwa powinniśmy magazynować znacznie więcej wysoko przetworzonych produktów ropopochodnych, niż czystego surowca[6].

3. Logistyczne kierunki dywersyfikacji dostaw paliw płynnych

Zasadniczym zagrożeniem dla bezpieczeństwa energetycznego Polski, głównie paliwowego i gazowego jest jednokierunkowy i monopolistyczny system zakupów zaopatrzeniowych, zorientowany od lat na największego potentata surowcowego świata, którym jest Rosja, z jednej strony bliski geograficznie sąsiad Polski, z drugiej trudny, historycznie i mocarstwowy gracz rynkowy, który do wolnej gospodarki rynkowej brutalnie włącza instrumenty walki politycznej.

Praktycznie wszystkie nośniki energii, począwszy od najbardziej zaawansowanego technologicznie prądu elektrycznego poprzez masowe surowce, takie jak ropa naftowa, czy gaz ziemny, a skończywszy na produktach i paliwach ropopochodnych, muszą być przesyłane w strukturach logistycznych łańcuchów dostaw obejmujących wieloetapowe, binarne procesy logistyczne, czyli dynamiczny transport i statyczne magazynowanie. Do realizacji tych łańcuchów potrzebne są przede wszystkim pierwotne źródła dostaw i zaopatrzenia oraz odpowiednie sieci i instalacje przesyłowo-magazynowe, które warunkują końcowe dostawy dystrybucyjne do poszczególnych odbiorców. Infrastrukturę logistyki sektora paliwowo-energetycznego tworzą przede wszystkim sieci energetyczne do przesyłania energii elektrycznej, rurociągi i naftociągi do transportu ropy naftowej oraz gazociągi do przesyłania gazu, głównie ziemnego. Warunkiem sprawnego funkcjonowania tych instalacji są kosztowne systemy i urządzenia techniczne takie jak stacje transformatorowe, rozdzielnie mocy, tłocznie i przepompownie a przede wszystkim odpowiednie magazyny i obiekty do składowania i przechowywania niezbędnych rezerw i zapasów.

---

[5] *Ustawa z dn. 16 lutego 2007r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa,* Dz. U. nr 52 / 2007, poz. 343.

[6] Taki stan wynika z koniunkturalnych interesów wiodących firm paliwowych, które skorzystały z okazji i w wyeksploatowanych kawernach solnych pod Inowrocławiem zgromadziły duże ilości surowej ropy naftowej, bo przetworzonych produktów paliwowych np. benzyn w takich warunkach nie można przechowywać.

Szczególnie niebezpieczna jest nasza jednokierunkowa zależność od dostaw rosyjskiego gazu ziemnego, który jest istotnym składnikiem bilansu energetycznego Polski – prawie 65% gazu LNG importujemy z Rosji, ciągle bez jakichkolwiek alternatywnych kierunków dostaw. Do Polski gaz ziemny jest transportowany przede wszystkim gazociągiem Jamał, którego techniczna przepustowość jest całkowicie wystarczająca, a jedynym krytycznym punktem jest wypełnienie go po stronie rosyjskiej odpowiednim medium oraz tranzyt przez terytorium Białorusi, co jak wykazują doświadczenia zimy 2004 i 2005 generuje polityczne problemy bezpieczeństwa i niezawodności dostaw.

Nieudaną próbą dywersyfikacji dostaw gazu ziemnego jest będący ciągle w sferze zamierzeń planistycznych 160 km gazowy bajpas (w tym 30 km na naszym terytorium) gazociąg Bernau-Szczecin łączący polskie sieci gazowe z otwartym i zdywersyfikowanym systemem zachodnio-europejskim. Blokowany od wielu lat decyzjami politycznymi gazociąg Bernau – Szczecin, pomimo strategicznych zalet i ekonomicznych korzyści ciągle nie może doczekać się praktycznej realizacji. W nieodległych czasach był on konkurencją dla forsowanych przez pewne siły polityczne budowy podmorskich sieci przesyłowych łączących Polskę z gazociągami duńskimi, szwedzkimi i norweskimi. Aktualnie istnieje niewielkie połączenie z siecią niemiecką koło Zgorzelca, ale jego wydajność nie przekracza 1 mld m^3 gazu w skali roku, co wobec 14 mld konsumpcji jest dość symboliczne.

Kolejnym, realnym kierunkiem dywersyfikacji dostaw gazu ziemnego są dostawy transportem morskim w postaci gazu skroplonego, co wymaga ogromnych inwestycji infrastrukturalnych i transportowych. Aktualnie w Porcie Północnym w Gdańsku istnieje pojedynczy pirs do przeładunku gazu skroplonego, ale jego wydajność jest wysoce niewystarczająca, jak na potrzeby różnych sytuacji kryzysowych. Stąd realna koncepcja budowy nowoczesnego gazoportu na redzie w Świnoujściu, jako wielkiego bałtyckiego terminala do rozładunku gazu skroplonego, transportowanego za pomocą wysoce zaawansowanych technologicznie statków-gazowców[7]. Jeszcze innym alternatywnym

[7] Gazoport, czyli terminal portowy do odbioru tankowców ze skroplonym gazem LNG, ma powstać w Świnoujściu i w pierwszym etapie mógłby odbierać do 2,5 mld m^3 rocznie (tzn. ok. 20% krajowego zużycia). W założeniach przyjęto, że po rozbudowie moce terminalu mogłyby zostać potrojone. Koszty pierwszego etapu tej inwestycji oszacowano na mniej więcej 450 mln euro, a oddanie inwestycji do eksploatacji przewiduje się na 2013 r.

źródłem zwiększenia bezpieczeństwa zaopatrzenia Polski w błękitne paliwo jest rozbudowa krajowego systemu składów i magazynów gazu ziemnego, z wykorzystaniem przede wszystkim naturalnych, geologicznych struktur do jego gromadzenia. Polska posiada korzystne warunki do stworzenia takich naturalnych magazynów, ale ich pojemność jest oczywiście też ograniczona i mogą być traktowane jedynie jako strategiczne składy buforowe na wypadek większego kryzysu energetycznego[8].

Elementem szczególnej gry rynkowej w sektorze paliwowym są też różne zabiegi biznesowe czynione wokół polskich Naftobaz, czyli dużych magazynów, w których składowane są znaczne ilości produktów ropopochodnych. Formalnie na straży strategicznych interesów państwa stoją rządowe programy restrukturyzacji branży paliwowej, ale niektóre firmy prywatne usiłują różnymi drogami pozyskać odpowiednie pakiety kontrolne i uzyskać prawa własności do najważniejszych obiektów infrastruktury magazynowej. Utrzymanie tych strategicznych inwestycji paliwowych pod kontrolą geopolityczną państwa polskiego leży w żywotnym interesie bezpieczeństwa energetycznego kraju i zostało odpowiednio wyartykułowane w rządowych Założeniach Polityki Energetycznej Państwa do roku 2020. Niestety sytuacja najbardziej krytycznego elementu tej strategii, czyli Naftoportu jest dość złożona, gdyż aktualnie jest on współwłasnością kilku firm, w tym sprywatyzowanego Orlenu oraz prywatnej spółki J&S, a o przejęcie pakietu kontrolnego walczy państwowa firma PERN zarządzająca siecią krajowych rurociągów naftowych.

Sygnalizowane w tytule podejście logistyczne oznacza w tym przypadku spełnienie, oprócz nadrzędnych kryteriów sprawnych technicznie i bezpiecznych przepływów, także postulatu efektywności ekonomicznej, co implikuje minimalizację łącznych kosztów dostaw nośników energetycznych we wszystkich ogniwach łańcucha logistycznego. Z uwagi na znaczący udział globalnych kosztów dostaw nośników energii w budżecie każdego państwa warunek minimalizacji tych kosztów jest istotnym czynnikiem optymalizacji jego strategii

[8] Aktualnie w Polsce funkcjonuje 6 dużych podziemnych magazynów gazu – Wierzchowice (558 mln m3), Mogilno (372 tys. m3), Husów (374 mln m3), Strachocina (133 mln m3), Swarzów (82 mln m3), Brzeżnica (62 mln m3) zlokalizowanych na bazie wyeksploatowanych złóż gazu ziemnego i odpowiednio przygotowanych kawern solnych. Nowo planowane lokalizacje to: Daszewo, Bonikowo i Kosakowo oraz rozbudowany Strachocin.

gospodarczej. W przypadku dostaw nośników energii i przesyłu samej energii decydującym składnikiem kosztów tych strumieni są koszty utrzymania logistycznych łańcuchów dostaw w odpowiedniej sprawności i gotowości technicznej, organizacyjnej i funkcjonalnej, a przede wszystkim pozyskanie wymaganych źródeł zaopatrzenia (zakupu) gwarantujących rytmiczne i odpowiednio intensywne przepływy fizyczne poszczególnych mediów energetycznych.

Formalnie logistyczny łańcuch dostaw nośników energetycznych obejmuje pewien chronologicznie zbudowany ciąg operacji technologicznych i procesów logistycznych, na który składają się takie czynności jak np. pozyskanie, utrzymanie i eksploatacja źródeł pierwotnych, przetwórstwo wstępne i przygotowanie do transportu, fizyczny transport lub przesył nośników energetycznych za pomocą specjalistycznej z reguły infrastruktury transportu przesyłowego (rurociągi, naftociągi, gazociągi, taśmociągi), gromadzenie i składowanie nośników na różnych etapach ich transportu oraz rozdział i dostawy dystrybucyjne do końcowych ogniw konsumenckich. Zasadniczym problemem związanym z utrzymaniem tych łańcuchów jest z reguły duże rozproszenie przestrzenne sieci dystrybucyjnej, jej wielka rozległość terytorialna wynikająca z punktowych źródeł naturalnego wydobycia i niezwykle rozczłonkowanej sieci dystrybucji. Dodatkowe trudności, głównie natury politycznej i handlowej implikuje transgraniczny system transportu przesyłowego obejmujący najczęściej wiele państw i krajów leżących na trasie przepływu tych surowców strategicznych.

4. Wyższość polityki nad ekonomią i logistyką

Problematyka bezpieczeństwa energetycznego Polski jest od początku naszej demokracji traktowana zdecydowanie bardziej w kategoriach politycznych niż ekonomicznych czy gospodarczych. Praktycznie od 20 lat wszystkie rządy Rzeczypospolitej w tej strategicznej dla kraju sprawie kierują się partykularnym interesem politycznym, ambitnie generują mniej lub bardziej sensowne plany zagwarantowania bezpieczeństwa energetycznego kraju, po czym demokratycznie wybrani ich następcy natychmiast totalnie krytykują swoich poprzedników i obwieszczają nowe autorskie koncepcje i narodowe strategie bezpieczeństwa energetycznego Polski. Tą niekonsekwencje strategiczną i totalny zamęt na szczeblu operacyjnym z całą premedytacją wykorzystują nasi zagraniczni partnerzy rynkowi –

dostawcy i pośrednicy i lansują wygodne dla siebie rozwiązania biznesowe, coraz wyraźniej zabarwione kryteriami geopolitycznymi. Panaceum w postaci dywersyfikacji dostaw nośników energetycznych podgrzewa wszystkie polskie umysły i gremia decydenckie na różnych poziomach władzy politycznej, kierowania i zarządzania gospodarczego, a efekty tej narodowej gorączki są raczej niewielkie, żeby nie powiedzieć kompromitujące. Najlepszym przykładem tej tezy jest częściowe przyczynienie się Polski do rezygnacji przez Rosję z budowy wielkiego transkontynentalnego gazociągu Jamał 2 biegnącego pierwotnie przez terytorium Polski i Białorusi, a dziś projektowanego w postaci gazociągu Północnego na dnie Morza Bałtyckiego[9]. Tej dziejowej szansy politycznej podniesienia bezpieczeństwa energetycznego kraju i szansy ekonomicznej wynikającej z międzynarodowego tranzytu przez nasze terytorium ogromnych mas surowcowych raczej już nie odzyskamy, a działania niektórych organów politycznych nastawione na konfrontacyjną politykę z Rosją niweczą ją ostatecznie i całkowicie.

W energetycznych transakcjach rynkowych Rosja świadomie i bardzo zręcznie posługuje się ekonomicznymi kryteriami zysku i dlatego zarówno ropa naftowa, jak też gaz ziemny są sprzedawane m.in. Polsce po cenach zawsze nieco niższych niż aktualne notowania światowe. W ten sposób podnosi konkurencyjność swojej oferty i pozyskuje strategicznych odbiorców związanych korzystnymi, wieloletnimi umowami handlowymi z poszczególnymi państwami. Sprzedawana dla strategicznych odbiorców europejskich rosyjska ropa naftowa jest zawsze tańsza o 3-5% od ropy arabskiej, jeszcze większe dysproporcje występują w przypadku gazu ziemnego importowanego ze złóż norweskich, czy niemieckich na Morzu Północnym. W ten sposób większość krajów Europy Wschodniej musi rozwiązać dylemat, czy zaopatrywać się z różnych źródeł i różnymi kanałami dywersyfikując swoje dostawy i podnosząc własne bezpieczeństwo energetyczne, czy pozostać w ścisłych relacjach handlowych i biznesowych z monopolistycznym dostawcą. Czynnikiem decyzyjnym jest rachunek

[9] Gazociąg Północny to planowana przez międzynarodowe konsorcjum Nord Stream, z pakietem kontrolnym rosyjskiego Gazpromu, budowa gazociągu morskiego mającego służyć do transportu gazu ziemnego z Rosji do Niemiec. Według planów, ma przebiegać dnem Morza Bałtyckiego, omijając Polskę i republiki bałtyckie. 29 sierpnia 2006 Rosyjski Gazprom oraz niemieckie E-ON-Ruhrgas i BASF podpisały w Moskwie porozumienie końcowe dotyczące budowy Gazociągu Północnego, którego wstępne koszty szacowane są na poziomie 13 mld $. Kraje skandynawskie z Polską na czele wysuwają intensywne kontrargumenty, głównie natury ekologicznej.

ekonomiczny, który wskazuje na stałe i korzystne partnerstwo rynkowe, z drugiej strony istotne jest bezpieczeństwo strategiczne i niezależność polityczna od praktyk monopolistycznych. Należy także pamiętać, że wysokie ceny energii to wyższe koszty wytwarzania produktów, usług i funkcjonowania całej gospodarki, a tym samym niższa jej konkurencyjność na globalnych rynkach światowych. Ryzyko politycznej zależności konkurujące w tym przypadku z ryzykiem kosztów ekonomicznych musi być wzajemnie relatywizowane i odpowiednio kalkulowane, co w skali państwa nie jest rzeczą ani łatwą, ani jednoznaczną.

Polska leżąca na trasie dwóch wielkich szlaków transportowych – rurociągu Przyjaźń (przez nasz kraj płynie 30% eksportu rosyjskiej ropy) i gazociągu Jamał jest atrakcyjnym partnerem biznesowym Rosji, który za wszelką cenę dąży do monopolizacji pewnych transakcji, a zwłaszcza systemów infrastruktury przesyłowej nośników energetycznych. Polska dodatkowo dysponuje dwoma nowoczesnymi rafineriami Płock i Gdańsk, dużym dobrze zlokalizowanym naftoportem „Port Północny" oraz licznymi naftobazami i specjalistycznymi składami do gromadzenia i magazynowania zarówno surowców energetycznych jak też ich przetworów. Nasze największe koncerny paliwowo-energetyczne takie jak Orlen, Lotos czy wreszcie PGNIG (Polskie Górnictwo Naftowe i Gazownictwo) znajdują się pod ciągłą presją rosyjskiego giganta Łukoil, który za wszelką cenę stara się zdobywać zagraniczne obiekty infrastrukturalne europejskiego sektora paliwowo-energetycznego. Rosyjskie koncerny paliwowo-energetyczne, a stojące za ich plecami najwyższe władze polityczne na Kremlu w dużej części kontrolują rynki byłych republik radzieckich i coraz natarczywiej atakują narodowe koncerny pozostałych krajów tzw. bloku wschodniego, w tym Polski, a ostatnio bardzo intensywnie Ukrainy. Wzorem światowych gigantów paliwowych takich jak BP, Shell czy ExxonMobile rosyjskie koncerny chcą kompleksowo zajmować się wszystkim, od wydobycia surowca, poprzez jego transport i dystrybucję, a także przetwarzanie aż do detalicznej sprzedaży na stacjach benzynowych. Ta monopolistyczna tendencja ma swoje źródła w koniunkturalnych wahaniach światowego rynku paliwowo-energetycznego – raz zarabia się lepiej na wydobyciu surowca, innym razem największe zyski przynosi jego przetwórstwo, a jeszcze innym sprzedaż produktów gotowych. Światowe koncerny paliwowe poszukują zagranicznych rynków zbytu nie tylko na surową

ropę czy gaz ale przede wszystkim na ich gotowe produkty, głównie paliwa.

Monopolistyczna i mocarstwowa pozycja Rosji w całym sektorze energetyczno-paliwowym wynika przede wszystkim z jej ogromnych zasobów naturalnych, zarówno ropy naftowej, a przede wszystkim gazu ziemnego (ok. 60% rozpoznanych światowych złóż gazu znajduje się na terytorium Rosji) jakimi dysponuje w skali całego świata. Pozycję światowego lidera i monopolisty Rosja broni różnymi sposobami przede wszystkim skutecznie zwalczając konkurencję, zwłaszcza na kierunku wschodnim. Efektem tej rynkowo-politycznej gry jest skuteczne zablokowanie alternatywnego kierunku dostaw ropy naftowej do Europy południowo-wschodniej tzw. gazociągiem Nabucco[10], który miał obsługiwać dostawy ropy kaspijskiej z byłych republik środkowo-azjatyckich. W efekcie ukraińska część rurociągu Odessa-Brody, którym miała płynąć konkurencyjna do rosyjskiej ropy – ropa kaspijska znalazła się pod kontrolą koncernów rosyjskich, a projektowa rozbudowa do Polski na kierunku Brody – Płock stała się mało bezpieczna rynkowo, gdyż Rosjanie zagrozili Polsce, że w tym przypadku skoro zamierzamy kupować droższą ropę kaspijską, to widocznie rosyjska jest zbyt tania sensownym będzie rewizja dotychczasowych umów i podniesienie ceny na dostawę ropy w rurociągu „Przyjaźń”[11].

Wnioski i uwagi końcowe

1. Bezpieczeństwo energetyczne Polski należy do strategicznych kierunków bezpieczeństwa gospodarczego i musi być programowo kontrolowane i stymulowane przez rząd, jako przedmiot najwyższych kompetencji i szczególnej odpowiedzialności.

[10] Planowany gazociąg Nabucco o długości ok. 3,3 tys. km i szacowanych kosztach 6 mld $ miał posłużyć do transportu gazu ziemnego z Iranu, Azerbejdżanu, Rosji i wschodniej Turcji do Austrii przez Bułgarię, Rumunię i Węgry. Projekt Nabucco został włączony do programu Trans-European Energy Network współfinansowanego na poziomie 20-30% kosztów przez Bank Centralny UE.

[11] Wyraźny cień na aspektach biznesowych tych relacji kładą rosyjskie służby specjalne na czele z Władimirem Afganowem i tajemniczym rosyjskim biznesmen Siergiejem Gawriłowem. W te wielkie interesy wplątanych jest także cały szereg polskich nazwisk i biznesmenów, którym trudno udowodnić jakąś wyraźną winę. Sprawy te były rozpatrywane m.in. podczas pracy słynnej sejmowej komisji specjalnej tzw. Komisji Orlenowskiej.

2. Aktualny (2008r.) stan bezpieczeństwa energetycznego Polski jest zadawalający, a bilans energetyczny korzystny i spełniający ogólne standardy Unii Europejskiej (+33,3%).
3. Wyjątkowo specyficzna jest struktura bilansu energetycznego Polski, w której wyraźnie dominują bogate, krajowe surowce kopalne czyli węgiel kamienny i brunatny (65%).
4. Utrzymanie w dłuższej perspektywie czasowej „węglowej" struktury bilansu energetycznego Polski jest niemożliwe i dlatego należy:

- albo zmniejszyć dotychczasowy udział węgla,
- albo wykorzystać potężne zasoby tego surowca za pomocą nowoczesnych, ekologicznych technologii np. gazyfikacji węgla.

5. W dążeniu do poprawy bezpieczeństwa energetycznego Polski należy optymalnie dywersyfikować źródła i kierunki dostaw nie paląc dotychczasowych, strategicznych mostów logistycznych łączących Polskę z największym zagłębiem surowcowym świata, którym jest Rosja.
6. Najbardziej krytycznym i kryzysogennym nośnikiem energii jest aktualnie gaz ziemny, którego 70% zapotrzebowania musimy pokryć w drodze międzynarodowego importu.
7. Strategicznych kierunków dywersyfikacji gazu ziemnego jest stosunkowo dużo, a do najbezpieczniejszych i najbardziej efektywnych ekonomicznie należą:
   – budowa nitki gazociągu Bernau – Szczecin (30 km po stronie polskiej),
   – budowa gazoportu Świnoujście (3 mld PLN) i mało realne kontraktacje dostaw gazu skroplonego,
   – technologiczne, morskie podłączenie do Gazociągu Północnego (bardzo trudne),
   – restauracja projektu Jamał-2 (najmniej prawdopodobna).
8. Bezpieczeństwo energetyczne Polski ma wymiar zewnętrzny – geopolityczny i wspólnotowy (UE) oraz wewnętrzny – ekonomiczno-gospodarczy i handlowy.
9. Realne bezpieczeństwo zewnętrzne jest pochodną skomplikowanych relacji biznesowych i politycznych światowych, koncernów paliwowo-energetycznych, w tym rosyjskich i polskich i dlatego należy ostrożnie budować wszelkie narodowe strategie bezpieczeństwa.
10. Bezpieczeństwo zewnętrzne należy widzieć kompleksowo jako zintegrowany system bezpieczeństwa energetycznego całej Unii

Europejskiej i nie próbować rozgrywać indywidualnie karty polskiej ze stroną rosyjską.

11. Bezpieczeństwo wewnętrzne to również efekt skomplikowanych relacji biznesowo-politycznych tworzony przez państwowe i prywatne podmioty gospodarcze prowadzące rynkową grę o znaczące zyski i wielkie dochody korporacyjne.
12. Fizycznym determinantem bezpieczeństwa zewnętrznego i wewnętrznego są logistyczne łańcuchy dostaw obejmujące: pierwotne źródła zakupów, sieci i systemy przesyłowe, systemy magazynowania i składowania, sieciowe urządzenia techniczne oraz logistyczne węzłyi sieci dystrybucji rynkowej.
13. Strategiczną kontrolę nad bezpieczeństwem energetycznym Polski powinien sprawować Rząd RP, przy pełnej akceptacji i zgodności z polityką energetyczną Unii Europejskiej i całkowitej solidarności wszystkich państw członkowskich.

Kraje starej Unii dawno odkryły, że trzy razy tańsze i znacznie bardziej perspektywiczne są inwestycje w ograniczanie i redukcję zużycia wszelkiej energii przez poszczególnych konsumentów niż inwestowanie w nowe moce produkcyjne, czy nowe źródła pozyskania nośników energetycznych. W dużej części wynika to z faktu, że do momentu odkrycia i eksploatacji złóż podmorskich na Morzu Północnym, były one praktycznie pozbawione znaczących źródeł własnych, a w dominującej części uzależnione były od światowego importu, głównie ropy naftowej i gazu ziemnego.

Bibliografia

1. Cohen A., *Rury bojowe,* Wprost nr 14 kwiecień, 2007.
2. Grzeszak A., *Krótki kurs gazownictwa*, Polityka nr 3 (2688), 2009.
3. Grzeszak A., *Iwan i gazrurka. Raport*, Polityka nr 50(2482), 2004.
4. Grzeszak A., *Na falach trój morza*, Polityka nr 22 (2656) / 2008.
5. Ilnicki M., Kubiak K., Mickiewicz M., *Morski transport ropy naftowej i gazu w warunkach zagrożeń aktami przemocy,* WN DSWiE, Wrocław 2006.
6. Kochanek E., *Bezpieczeństwo energetyczne Polski*, Kwartalnik. Bellona 1/2008.
7. Kuczyński W., *Maczuga energetyczna*, Polityka nr 49 (2481) / 2004.
8. Nowakowski J.M., *Miotacz gazu,* Wprost nr 1205 / 2006.
9. Orłowski W.M., *Płynne prognozy*, Polityka nr 22 (2656) / 2008.

10. Traynor I., *Nabucco pełne snów*, Forum nr 2 / 2009.
11. Winiarski W., *Bezpieczeństwo energetyczne i węgiel,* Biuletyn Górniczy 1-2 (79-80) styczeń – luty 2002.
12. Zerka M., *Bezpieczeństwo energetyczne. Filary europejskiej polityk,.* Nafta i Gaz Biznes, grudzień 2004.

LOGISTIC ASPECTS OF POLISH ENERGY SECURITY

Summary

The paper presents the development of the logistics concept of energy security in the twenty-first century in Poland, with respect to liquid fuels. In the introduction is discussed the concept and a national strategy for energy security and a current polish energy balance. Next are presented the essential lines of diversification of supply of liquid fuels to Poland, and the importance of the role of transport logistics systems. Also is characterized the dominant role of geo-political strategy in building the best system of energy supplies to Poland. At the end are described the basic principles of optimization of energy supply logistic chains to the Poland.

Konrad Zaręba [*]

SKUTECZNA STRATEGIA WYKORZYSTANIA ODNAWIALNYCH ŹRÓDEŁ ENERGII SZANSĄ NA POPRAWĘ BEZPIECZEŃSTWA ENERGETYCZNEGO

Streszczenie

W artykule podjęto próbę charakterystyki skutecznej strategii wykorzystania odnawialnych źródeł energii stwarzającej szansę na poprawę bezpieczeństwa energetycznego kraju. Ukazano również czynniki determinujące jej skuteczność, korzyści i ryzyko związane z wykorzystaniem źródeł energii odnawialnej. Zwrócono uwagę również na strategiczne cele projektu wykorzystania zasobów odnawialnych.

Wstęp

Dyskusje i polemiki wywołane odcięciem i ograniczeniem dostaw rosyjskiego gazu dla państw Unii Europejskie przywrócił temat bezpieczeństwa energetycznego naszego kraju. Enigmatycznie wspominano o alternatywnych rozwiązaniach zmierzających do wykorzystania odnawialnych źródeł energii, ograniczając się do tematu dywersyfikacji dostaw gazu.

Łączenie terminu „bezpieczeństwa energetycznego kraju" z kolejnymi rozgrywkami nie służą dobrze zrozumieniu istoty problemu przez społeczeństwo i uwypukleniu charakteru jego zagrożeń oraz ostatecznie wypracowaniu skutecznej strategii.

Dokonane badania mówią, że 30% zużywanej przez nas energii pochodzi z surowców importowanych, które obarczone są „politycznymi rozgrywkami". Dlatego dywersyfikacja surowców energetycznych powinna opierać się na zastąpieniu ich surowcami, bądź takimi źródłami energii, które będą bezpieczne i odporne na polityczne zawirowania.

[*] Autor jest Pracownikiem Uniwersytetu Ekonomicznego w Krakowie.

Zapewnienie krajowi bezpieczeństwa energetycznego powinno prowadzić do podejmowania działań szerszych i bardziej spektakularnych, zmierzających do zagwarantowania dostępności do różnorodnych nośników energii i zapewnienia ciągłości ich dostaw, a także stworzenia niezawodnej infrastruktury do przesyłu energii od dostawców do ich odbiorców.

Po przystąpieniu Polski do Unii Europejskiej jesteśmy częścią układu – jak w naczyniach połączonych, który niesie ze sobą wiele pozytywów, ale również pewne ryzyko. Uświadamia nam to prawdę, że nie zawsze to, co dobre dla innych jest równie dobre dla nas.

Cykl inwestycyjny w polskiej energetyce wymaga tworzenia długookresowej strategii bezpieczeństwa energetycznego, w tym trafnego prognozowania koniunktury gospodarczej w okresie dwóch, trzech dekad.

Ciągłe podkreślanie, że ze względu na posiadane zasoby węgla Polska skazana jest na jego priorytet w strukturze źródeł pierwotnych, wymagają analizy i odpowiedzi czy rzeczywiście z punktu widzenia bezpieczeństwa gospodarczego powinno tak być ?.

2. Czynniki determinujące skuteczną strategię energetyczną

W aspekcie politycznym zapewnienie bezpieczeństwa energetycznego sprowadza się obecnie w znacznym stopniu do wyeliminowania lub ograniczenia możliwości wykorzystania przez podmioty zewnętrzne ich statusu dostawcy energii, w celu wywierania nacisków politycznych. Aspekt gospodarczy tego bezpieczeństwa obejmuje głównie koszty uzyskania energii, a nie fizyczne zapewnienie dostaw[1].

Aspekt ekologiczny jako znaczący czynnik wpływający na podejmowanie strategicznych decyzji, zaczął być zauważalny dopiero od niedawna. Ciągle jeszcze jednak jest pomijany i nie uwzględniany w gospodarczych działaniach strategicznych. Potrzeby energetyczne Polski kształtują się obecnie na poziomie około 30 % średnich potrzeb starej Unii Europejskiej[2].

---

[1] Jemioło T., *Polityczno-gospodarcze aspekty bezpieczeństwa energetycznego Polski*, Materiały Konferencyjne: pt.: Bezpieczeństwo narodowe i zarządzanie kryzysowe w Polsce w XXI wieku – wyzwania i dylematy. Warszawa 2008.

[2] Polityka energetyczna Polski do 2025r. Dokument przyjęty przez RM RP 25.01.2005.

Kontynuowanie rozbudowy systemu energetycznego w naszym kraju według dotychczasowych technologii ogranicza wielkość produkcji energii elektrycznej do wysokości nieco ponad 200 TWh brutto rocznie. Zatem większa produkcja wymusza potrzebę radykalnej zmiany struktury wykorzystania paliw i źródeł energii. Przewiduje się, że do 2020 roku zapotrzebowanie na energię znacznie przekroczy tę granicę.

Podstawową przyczynę ograniczenia wykorzystania węgla w przyszłości stanowi nieuniknioną konieczność ograniczenie emisji dwutlenku węgla do atmosfery. Ciągła wizja rozwoju technologii pozyskiwania surowców wynika z przekonania o „niewyczerpywalnych" zasobach własnych surowców energetycznych.

W działaniach mających na celu wykreowanie wizji przyszłości strategii energetycznej (w analizie i planowaniu) warto zwrócić uwagę na projekt typu Foresight. Tworzy on bowiem język debaty społecznej i kulturę budowania wizji przyszłości. Tego typu projekty, analizy i oceny przeprowadzane są przy szerokim udziale różnych grup społecznych, a ich celem jest badanie możliwych prawdopodobnych i preferowanych wizji przyszłości w okresach średnio i długoterminowych. Należy podkreślić, że Foresight przedstawia wizję, która może być inna niż panujące trendy. Często nazywany jest próbą spojrzenia w przyszłość, a nie jej przewidywania[3].

Główne czynniki, które w krótkim okresie czasu mogą przyczynić się do opracowania skutecznej strategii energetycznej to:

- uregulowana sytuacja prawno – organizacyjna w energetyce,
- utworzenie forum naukowo – eksperckiego,
- patronat i wsparcie rządu oraz dobry klimat społeczny,
- zaplecze badawczo – naukowe.

Aby mówić o rozwoju nowoczesnej strategii energetycznej, trzeba stworzyć organ państwowy, który będzie wyposażony w odpowiednie uprawnienia, kierowany przez wykwalifikowaną, fachową kadrę oraz posiadający odpowiednie środki finansowe i techniczne.

3. Jak zapewnić elastyczność systemu elektroenergetycznego kraju ?

Myśląc o bezpieczeństwie energetycznym Polski należy mieć na uwadze, że wydobycie węgla będzie eliminowane narastającymi

[3] Kuciński J., *Organizacja i prowadzenie projektów „Foresight" w świetle doświadczeń międzynarodowych*, IPPT PAN, Warszawa 2006.

restrykcjami ekologicznymi, a ceny ropy naftowej będą podatne na wahania ze względu na konflikty zwłaszcza na Bliskim i Środkowym Wschodzie. Efektywna strategia energetyczna wykorzystania odnawialnych źródeł energii powinna zapewnić elastyczność systemu elektroenergetycznego.

Głównymi czynnikami zapewniającymi elastyczność systemu energetycznego kraju są:

- szeroki dostęp do pierwotnych nośników energii na poziomie pozwalającym zaspokoić popyt, z uwzględnieniem technologii transportu nośników pierwotnych,
- technologie przemiany nośników pierwotnych w nośniki użytkowe,
- technologie długodystansowego transportu nośników użytkowych,
- mechanizmy finansowania działalności i rozwoju sektorów energetycznych[4].

Zapewniając elastyczność systemu elektroenergetycznego kraju należy zadbać o: uniezależnienie się od surowców importowanych, liberalizację rynku energetycznego, ciągłe obniżanie energochłonności gospodarki, modernizację i budowę nowej infrastruktury energetycznej zapewniającą odbiór nośników z różnych kierunków i łatwość zmiany tych kierunków, niezawodność dostaw i strukturę zapewniającą wysoką produktywność, zmniejszony udział węgla w bilansie energetycznym na rzecz odnawialnych źródeł energii, opracowanie programów antykryzysowych, włączenie do przedsięwzięć energetycznych przedstawicieli wszystkich struktur administracyjnych państwa – poczynając od samorządów.

4. Korzyści związane z wykorzystania odnawialnych źródeł energii

W obecnej sytuacji geopolitycznej rzetelny program wykorzystania odnawialnych źródeł energii jest możliwy do wcześniejszej realizacji niż projekt Amber, zarzucony wraz z konkretyzacją budowy gazociągu północnego, czy gazociągu Sarmacja, którego planowanie jest w fazie wstępnej. Program ten zapewniałby: uniezależnienie od importowanych nośników energii, powszechną do nich dostępność, wypełnienie

[4] Kowalak T., *Bezpieczeństwo energetyczne zaklęcie, wytrych czy realna kategoria ?*, www.ure.gov.pl

zobowiązań dotyczących redukcji emisji substancji zanieczyszczających atmosferę i zobowiązań dotyczących OZE w produkcji energii, mniej awaryjną pracę instalacji, poprawę stanu środowiska naturalnego, rozwój krajowego rynku wysokich technologii, edukację ekologiczną społeczeństwa.

Obecnie kwestią zasadniczą jest tempo dochodzenia do pożądanego stanu i koszty jego osiągnięcia. Problemy te rozstrzyga polityka energetyczna państwa. Należy sobie uświadomić, że kryzys nie jest powodem dla, którego te działania można odkładać w czasie, gdyż nieskuteczna strategia energetyczna może go tylko pogłębiać.

5. Ryzyko związane z nowymi rozwiązaniami

Wieloaspektowość pojęcia „bezpieczeństwa energetycznego" powoduje szerokie spektrum zagrożeń, jakim podlega, a to z kolei wymusza rzetelne działania na rzecz ich wyjaśnienia. Nie jest to zadanie proste, gdyż odpowiedzialność za bezpieczeństwo energetyczne nie skupia się na jednym podmiocie życia społecznego, ale wymaga skoordynowanych działań podejmowanych na różnych jego szczeblach.

W naszym kraju ciągle jeszcze niedostatecznie rozpowszechniona jest wiedza na temat odnawialnych źródeł energii, które traktuje się jako niepewne i nieopłacalne źródło dostarczania energii. Brakuje odpowiedniej edukacji społeczeństwa i promocji korzyści pozyskiwania energii ze źródeł odnawialnych.

Dotychczasowy rozwój energetyki odnawialnej następował bez wsparcia państwa i jego angażowania się w jej propagowanie.

Ogólnospołeczne obawy i brak akceptacji dla wielu przedsięwzięć z tej dziedziny wynikają z braku wiedzy i nieznajomości tematu. Po części dotyczy to również, ludzi zainteresowanych „czystą" energią. Ich niepokój budzą: mało skuteczne rozwiązania formalnoprawne, brak grup ekspercko – doradczych, skomplikowana procedura pozwoleń i pomocy finansowej, możliwości spłaty długów i dofinansowań, wysokie koszty inwestycyjne, eksploatacyjne. jak również rozwiązania techniczno-technologiczne, mała dostępność do urządzeń i serwisów. W społeczeństwie pokutują również uprzedzenia minionego wieku obarczone złymi doświadczeniami jak choćby w przypadku spalarni odpadów.

Trudne natomiast do przewidzenia w krótkim czasie są skutki ekologiczne i zaburzenia krajobrazu obecnie podejmowanych

przedsięwzięć. Niepokój budzi bezpowrotna degradacja istniejącego systemu pozyskiwania i przetwarzania konwencjonalnych nośników energii (zamykanie kopalń, redukcja etatów).

To wszystko wymaga sensownych rozwiązań i wyjaśnień.

6. Strategiczne cele projektu wykorzystania zasobów odnawialnych

Bezpieczeństwo energetyczne kraju jest zapewnione wtedy, gdy państwo jest pod tym względem samowystarczalne. Do takiego stanu Polsce daleko, chociaż posiadamy znaczne zasoby surowców oraz energii odnawialnej. Istnieją znaczne rozbieżności w ocenie tych zasobów, potencjału technicznego oraz geograficznego ich rozkładu. Dlatego opracowanie skutecznej strategii wykorzystania odnawialnych źródeł energii wymaga od jej twórców rzetelnej wiedzy, kreatywności i dalekowzroczności oraz społecznej odpowiedzialności.

Projektowanie zintegrowanego systemu rozwiązań zaopatrzenia w energię elektryczną musi obejmować:

- uaktywnienie rządu (stosowanych pracowników, stosownych agent, banków, urzędów regulacji na rzecz tworzenia zintegrowanego systemu),
- hierarchizacje działań operacyjnych,
- szerokie badania rynku,
- prognozy efektów w skali mikro i makro,
- dobór firm w zakresie doradztwa i audytu,
- opracowanie koncepcji rynków globalnego i lokalnego,
- określenie uwarunkowań ekonomicznych i ekologicznych przedsięwzięć,
- planowanie zintegrowanych działań w zakresie zabezpieczenia energii w sytuacji awaryjnej,
- projektowanie koncepcyjne i inżynieryjne,
- budowa instalacji technologicznej i technicznej,
- programy efektywności dla odbiorców finalnych,
- określenia sposobów finansowania i produkcji,
- zbudowania systemów magazynowania energii,
- plany dostępu do dodatkowych rynków,
- możliwości remontu i diagnozy technicznej urządzeń,
- tworzenie zintegrowanego systemów oceny jakości wytwarzanej energii,

– opracowanie systemu synchronizacji z elementami starego systemu energetycznego.

Projekt wykorzystania zasobów energii odnawialnej powinien zapewnić:

- bezpieczeństwo energetyczne kraju,
- dostęp do niewyczerpywalnych źródeł energii,
- uniezależnienie się od surowców importowanych,
- jakość i stabilność legislacyjną, regulującą zasady ich wykorzystywania,
- sprawny system ich pozyskiwania i funkcjonowania,
- zdolność do rzetelnego prognozowania rozwoju technologii,
- zdolność do przenoszenia sygnałów wynikających z elastyczności popytu na rynkach,
- narzędzia regulacyjne w stosunku do konkurencji.

Właściwa ocena potencjału źródeł odnawialnych energii, skoordynowane. Działania instytucji rządowych i polityki energetycznej może skuteczne przyczynić się nawet do samowystarczalności energetycznej kraju.

Podsumowanie i wnioski

Należy zdawać sobie sprawę, że bezpieczeństwo energetyczne kraju nie jest uzależnione tylko od jego gospodarki, ale jest wypadkową wielu zewnętrznych uwarunkowań i jej funkcjonowania.

Działania w zakresie bezpieczeństwa energetycznego w kraju powinny być oddane w ręce fachowców, ekspertów i doradców naukowych, a pozostawać poza wpływem rozgrywek politycznych i partykularnymi interesami.

Zasoby surowcowe w kraju powinny być traktowane jako rezerwa strategiczna.

Państwo o tak dużym potencjale zasobów energii odnawialnej jak Polska, nie może ich nie dostrzegać , a winno wykorzystywać z korzyścią dla gospodarki i środowiska.

Skuteczna strategia wykorzystania naszych zasobów odnawialnych przyczyni się do zapewnienia bezpieczeństwa energetycznego, a tym samym stabilności gospodarczej.

Warto zainwestować w budowę sieci magazynowania energii, która w sytuacji kryzysowej może pokryć minimum kwartalne

zapotrzebowanie na nią.

Prognozuje się, że spośród różnych źródeł energii odnawialnych w naszym kraju największe znaczenie będą miały biomasa i paliwa alternatywne (odpady), wiatr, energia spadków wód, energia geotermalna. Uważa się jednak, że energia wiatrowa, słoneczna, pływów morskich ze względu na uwarunkowania geograficzne mogą odgrywać mniejszą role[5].

Wybór technologii kluczowych nie oznacza wizji przyszłości, zdaniem ekspertów należy określać kilka wizji przyszłości i wybrać spośród nich najbardziej prawdopodobną i racjonalną.

Bibliografia

1. Jemioło T., *Polityczno – gospodarcze aspekty bezpieczeństwa energetycznego Polski*, Materiały konferencyjne pt.: Bezpieczeństwo narodowe i zarządzanie kryzysowe w Polsce w XXI wieku – wyzwania i dylematy. Warszawa 2008.
2. Kowalak T., *Bezpieczeństwo energetyczne zaklęcie, wytrych czy realna kategoria ?* www.ure.gov.pl.
3. Kuciński J., *Organizacja i prowadzenie projektów „Foresight" w świetle doświadczeń międzynarodowych*, IPPT PAN, Warszawa 2006.
4. Leszczyński W.M. *Proekologiczne źródła energii odnawialnej*, WNT, Warszawa 2002.
5. Polityka energetyczna Polski do 2025r. Dokument przyjęty przez RM RP 25.01.2005.

Summary

This article attempts to characterize an effective strategy of the use of renewable energy sources that would lead to the improvement of national energy security. It presents the factors which determine the effectiveness of the strategy, and benefits as well as risks related to the use of renewable energy sources. Additionally, strategic goals of the project of renewable resource use have been scrutinized.

[5] Leszczyński W.M., *Proekologiczne źródła energii odnawialnej*, WNT, Warszawa 2002.

Janusz Gierszewski[*]

BEZPIECZEŃSTWO BIZNESU. FIRMY OCHRONY, JAKO PODMIOTY ZARZĄDZANIA BEZPIECZEŃSTWEM

Wprowadzenie

Temat badawczy jest interesujący z uwagi na zderzenie z jednej strony problemu bezpieczeństwa biznesu, którego ochroną zajmują się firmy, będące przedsięwzięciem biznesowym (for-profit). Czy interes firmy (zysk) jest dla nich jedynym elementem strategii firmy czy mają poczucie pewnego rodzaju misji, zakładającej pracę na rzecz szeroko rozumianego bezpieczeństwa państwa, społeczeństwa czy obywateli. Czy w podobny sposób prognozują potrzeby klientów i budują struktury organizacyjne? Ważne jest usystematyzowanie pojęć, jak i podjęcie próby przedstawienia różnych aspektów funkcjonowania firm ochrony w warunkach gospodarki rynkowej.

1. Definicja bezpieczeństwa

Bezpieczeństwo (security, securitas) jest synonimem pewności (safety), brakiem strachu czy obaw. Jest to pojęcie polisemantyczne. Paweł Tyrała uważa, że bezpieczeństwo podlega prawom prakseologii, a dyscypliną zajmującą się tym systemem jest securitologia[1]. Bezpieczeństwo biznesu to pewność w dokonywaniu kontraktów pomiędzy partnerami biznesowymi w niezagrożonym środowisku wewnętrznym. Charakter zagrożeń jest wieloaspektowy i dotykać może sfery zewnętrznej i wewnętrznej przedsiębiorstwa (personel). Nosi w sobie element podmiotowości i niestabilności. Podmioty ochrony podlegają tym samym zagrożeniom bezpieczeństwa biznesu, co

---

[*] Autor jest pracownikiem Powszechnej Wyższej Szkoły Humanistycznej Pomerania w Chojnicach.

[1] Por. P. Tyrała, *Bezpieczeństwo wymaga kompetencji. Na drodze do securitologii*, Teraz, 2002 r., nr 31, 32, 33.

ochraniane przez nich podmioty gospodarcze. Zagrożenie może pojawić się w samym otoczeniu firmy, zachowań pracowniczych czy w obszarze bezpieczeństwa pozaekonomicznego.

2. Bezpieczeństwo w firmie

W tym ostatnim kontekście można postawić pytanie: jakie (oprócz ustawowych) wdrożyły u siebie firmy ochrony systemy bezpieczeństwa w zakresie bezpieczeństwa wewnętrznych informacji, lojalności personelu czy pospolitej przestępczości. W jaki sposób wdrożyły optymalny system bezpieczeństwa i wyeliminowały potencjalne zagrożenia?

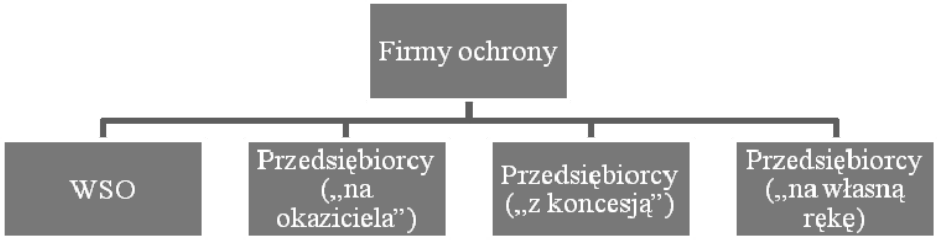
Rys. 1. Istotne (wspólne) elementy w organizacji przedsiębiorstwa

Działalność agencji ochrony mają na celu zlikwidowanie zagrożeń wewnętrznych oraz zewnętrznych i zapewnienie akceptowalnego systemu bezpieczeństwa. Ocena funkcjonowania skupia się przede wszystkim na wyniku finansowym niż na prewencyjnej ocenie skuteczności działań. Bezpieczeństwo powinno stanowić czynnik stabilizacji i rozwoju firmy. Bezpieczeństwo biznesu nosi w sobie wymiar ekonomiczny ukierunkowany na przedsiębiorczość i innowacyjność. Czy w takim otoczeniu jest miejsce na budowanie etosu zawodu jak dzieje się to w instytucjach non profit (np. zasady etyki policjanta). Coraz częściej przedsiębiorcy obok bezpieczeństwa ekonomicznego, ekologicznego, zdrowotnego zauważają potrzebę

budowania bezpieczeństwa osób i mienia. Współczesne zagrożenia mają różnorodny wymiar.

3. System ochrony firmy

Każda firma powinna dokonywać analizę ryzyka w formie akceptowalnej, transferowej i neutralizowanej. Najlepszy wydaję się system mieszany. Pozwala on na rozproszenie ryzyka.

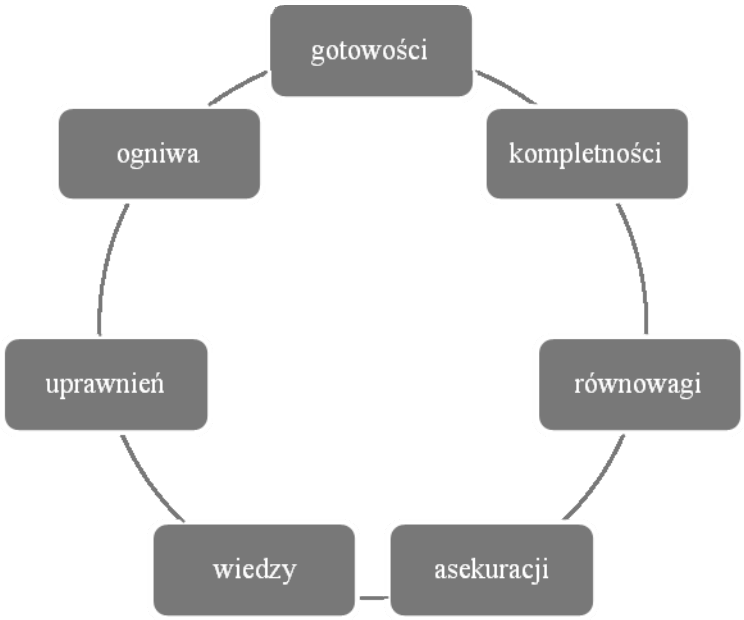


Rys. 2 Wybór „ścieżki" ochrony.

Najczęściej podmioty gospodarcze wybierają zewnętrzną firmę ochrony, przerzucając niejako odpowiedzialność za bezpieczeństwo i ewentualne skutki na inny podmiot. W tym miejscu można przypomnieć zasady polityki bezpieczeństwa.

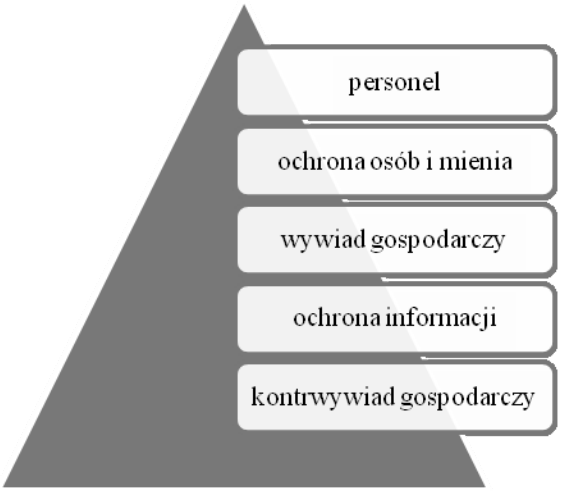
Ustawa daje możliwość działania na rynku również firmom bez koncesji i zatrudniania pracowników bez licencji. Uprawnienia wynikają z Ustawy o ochronie osób i mienia, gdzie swoboda gospodarcza została ograniczona koncesją[2]. Samo sporządzenie takiego planu powinno przynieść korzyść, gdyż brak polityki świadczyć może o nieudolnym zarządzaniu przedsiębiorstwem i narazić je na straty. Zagrożenie może być związane z przedmiotem działalności przedsiębiorstwa. Bezpieczeństwo biznesu to też eliminowanie zagrożeń kryminalnych, które mogą zagrozić funkcjonowaniu różnego rodzaju instytucji.

[2] Zob. Kubiński P., *Koncesjonowanie działalności gospodarczej w zakresie ochrony osób i mienia jako forma reglamentacji publicznoprawnej ministra spraw wewnętrznych i administracji.* Raport z badań, [w:] Przegląd Policyjny nr 4 (88).



Rys. nr 3 Schemat zasad polityki bezpieczeństwa firm.

Analiza zagrożeń wskazuje, że głównym celem jest pozyskanie mienia. Głownie narażone są podmioty podlegające obowiązkowej ochronie takie jak placówki bankowe oraz obiekty handlowe. Obok zagrożeń kryminalnych na znaczeniu zyskują zagrożenia o charakterze gospodarczym, w tym związane z bezpieczeństwem elektronicznym czy nieuczciwą konkurencją. Bezpieczeństwo biznesu nosi w sobie wiele realnych zagrożeń, a tam gdzie może wystąpić niebezpieczeństwo, powinna nastąpić analiza i organizacja systemu bezpieczeństwa w formie instytucjonalnej. Powinna ona zapewnić odpowiedni poziom bezpieczeństwa dla przedsiębiorstwa. Zagrożenia dla firmy mogą być prawdopodobne i rzeczywiste.



Rys. 4. Przedmiot bezpieczeństwa biznesu

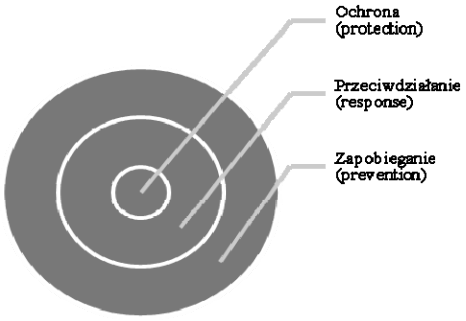
4. Etapy budowy bezpieczeństwa

Budowanie systemu bezpieczeństwa to minimalizowanie ryzyka. Składa się ono z kilku etapów takich jak analizowanie, rozpoznawanie, określanie prawdopodobieństwa wystąpienia zagrożenia czy ewaluację. Trzeba przecież pamiętać, że bezpieczeństwo jest procesem nietrwałym. Każda firma działa w pewnym systemie związków i uzależnień.

Zagrożenia możemy podzielić na geograficzno-topograficzne (duże miasta, osiedla,), obiektywne (niezależne), subiektywne (z winy człowieka), naturalne i ikonowe (kantory, banki). Firmy ponoszą coraz większe straty związane z cyberprzestępczością. W 2005 roku FBI oceniło straty ponoszone przez przedsiębiorstwa na 67 mld $[3].

Coraz więcej firm widzi potrzebę zarządzania bezpieczeństwem i powołuje w tym celu stanowiska do koordynacji tego typu zadań.

[3] http://www.securitystandard.pl/news/104195/Wspolna.obrona.warta.miliardy.html



Rys. 5. Warstwy bezpieczeństwa

Warstwowy system bezpieczeństwa zapewnić powinien niezawodność systemu. Oprócz bezpieczeństwa przemysłowego istotna jest ochrona informacji samego przedsiębiorstwa. Czynem nieuczciwej konkurencji jest przekazanie, ujawnienie, lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża istotnym interesom przedsiębiorstwa.

5. Personel a bezpieczeństwo

Tajemnica przedsiębiorstwa jest dobrem niematerialnym o charakterze majątkowym. Zabezpieczenie polega na zastosowaniu środków technicznych i organizacyjnych zapobiegających dostępowi do chronionych informacji osób nieupoważnionych, zabraniu ich przez osoby nieupoważnione oraz uszkodzeniu lub zniszczeniu[4]. Wyznaczony administrator prowadzi ewidencję osób uprawnionych, kontroluje dane wprowadzane do podległego mu zbioru, kontroluje krąg osób, którym udostępniane są dane.

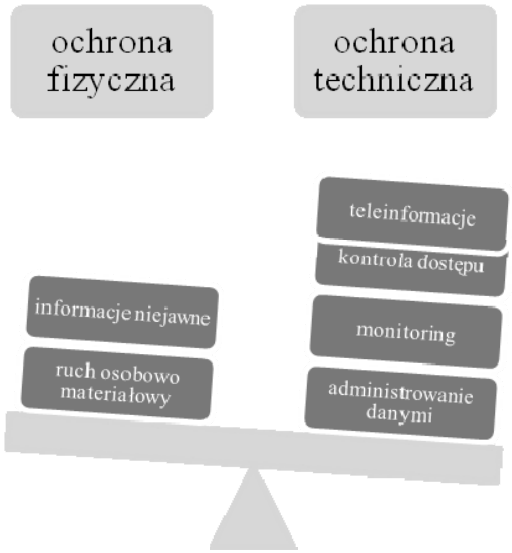
Źródłami ryzyka personalnego są warunki panujące w otoczeniu i we wnętrzu organizacji, metody i style podejmowania decyzji personalnych oraz cechy osób podejmujących decyzje.

Jedna z form ryzyka personalnego ryzyko selekcyjne obejmuje:

- ryzyko wyboru nieodpowiedniej metody różnicującej kandydatów,

[4] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz. U. nr 11, poz. 95 z późn. zmianami

- ryzyko niskiej jakości informacji o kandydacie,
- ryzyko nietrafnej interpretacji informacji dotyczącej kandydata.



Rys. 6. Wybrane zadania menadżera bezpieczeństwa

Osoba odpowiedzialna za bezpieczeństwo powinna charakteryzować się nie tylko niezbędnymi kwalifikacjami (licencje ochrony fizycznej i technicznej), ale wiedzą z zakresu ochrony danych osobowych, tajemnicy przedsiębiorstwa, informacji niejawnych, bezpieczeństwa teleinformatycznego czy zarządzania personelem. W tym miejscu warto się zastanowić jakich narzędzi doboru do pracy w pionie ochrony stosuje przedsiębiorca. Czy po zatrudnieniu monitoruje jego lojalność wobec firmy? Czy tworzony jest obraz koncepcji kandydata, kwestionariusz biograficzny, badane są dokumenty autoprezentacyjne, referencje, testy sprawności fizycznej czy stosuje się może testy uczciwości? To przecież człowiek jest najsłabszym elementem systemu ochrony. Pracownik ochrony to osoba posiadająca licencję pracownika ochrony fizycznej lub licencję pracownika zabezpieczenia technicznego i wykonująca zadania ochrony w ramach wewnętrznej służby ochrony albo na rzecz przedsiębiorcy, który uzyskał koncesję na prowadzenie działalności

gospodarczej w zakresie ochrony osób i mienia, lub osoba wykonującą zadania ochrony w zakresie nie wymagającym licencji[5].

6. Cele ochrony

Cele ochrony są zawarte w Ustawie o ochronie osób i mienia i sprowadzają się do:

a) zapewnienie bezpieczeństwa życia, zdrowia, nietykalności osobistej chronionych osób,
b) zapobieganie przestępstwom i wykroczeniom przeciwko mieniu, przeciwdziałanie powstawaniu szkód wynikających z tych zdarzeń, a także niedopuszczenie do wstępu osób nieuprawnionych na teren chroniony[6]

Pracownika ochrony wyróżniają nie tylko zadania, ale prawo do stosowania różnorodnych środków przymusu.

Swoje zadania realizuje poprzez następujące formy pełnienia służby:

a) Posterunki (stałe, doraźne).
b) Obchody.
c) Patrole.
d) Grupy interwencyjne.
e) Konwoje.
f) Ochronę osób.
g) Dozór sygnałów.
h) Bezpieczeństwo imprez masowych.

[5] Obok definicji ustawowej, Zgodnie z Międzynarodowym Standardem Klasyfikacji Zawodów ISCO-88 oraz Rozporządzeniem Ministra Gospodarki i Pracy z dnia 8 grudnia 2004 r. w sprawie klasyfikacji zawodów i specjalności dla potrzeb rynku pracy oraz zakresu jej stosowania (Dz. U. nr 265 z 2004 r., poz. 2644): pracownik ochrony mienia i osób - to zawód o symbolu klasyfikacyjnym 515902 w grupie usług osobistych i sprzedawców,

[6] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, DzU nr 114, poz. 740 z późn. Zmianami.

Tab. 1.
Środki, które może stosować pracownik ochrony

Środków porządkowych	Środków przymusu bezpośredniego	Broni palnej
a) Legitymowania, b) Wezwania do opuszczenia, c) ustalenia uprawnień, d) ujęcia.	a) siły fizycznej, b) kajdanek, c) psa obronnego, d) paralizatora,, e) broni gazowej, f) ręcznego miotacza gazu,	a) krótkiej, b) gładko-lufowej, c) sygnałowej d) KM.

7. Rynek usług bezpieczeństwa w Polsce

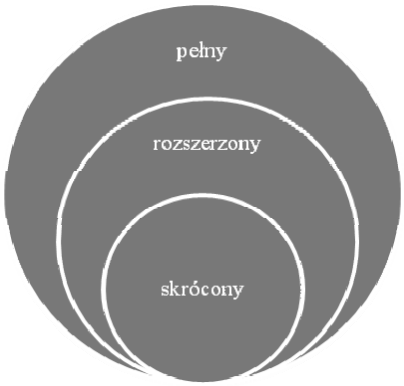
Rynek usług bezpieczeństwa rozwija się dynamicznie od czasów liberalizacji polskiej gospodarki, a więc od początku lat 90. Od tej pory powstało wiele firm ochrony, z których część przekształciła się w rynkowych liderów, część działa w niezmienionej formie małych firm ochroniarskich, niektóre znikły z rynku lub zostały wchłonięte przez inne. Udział pierwszej dziesiątki liderów nie przekracza 25% ogółu rynku[7]. Rozdrobnienie decyduje o konkurencyjności, ale i wysokości marży. Biorąc pod uwagę, że cena a nie jakość jest najistotniejszym elementem przy wyborze firmy ochrony, stawia się na byle jakość. Tak dochodzimy do początku rozważań czyli do istotnych elementów decydujących o sprawności przedsiębiorstwa (rys. 1) i potrzebie prowadzenia świadomej polityki bezpieczeństwa poprzedzonej dogłębną analizą zagrożeń i potrzeb. Niektóre z firm dostrzegają specyfikę bezpieczeństwa biznesu (Safety & Risk Consulting) i proponują audyty bezpieczeństwa, sporządzanie planów ochrony, szkolenia, konsultacje, analizy i zarządzanie ryzykiem, zarządzanie kryzysowe (Business Continuity & Crisis Management), bezpieczeństwo informacyjne (Information Security) czy Działania przeciw nielegalnemu handlowi i fałszerstwom produktów (Anti Illicit Trade & Anti Counterfeit). Coraz

[7] Za K. Rudnickim, dyrektorem strategii i rozwoju firmy „Konsalnet".

modniejszy staje się rynek korporacyjny z uwagi na jego potencjał. W celu dokonania właściwego wyboru firmy ochrony należy sprawdzić jej potencjał organizacyjno-prawny (koncesja, liczba pracowników na umowę o pracę, poziom płac, kwalifikacje, logistyka, bilans, referencje), a potem faktyczny (procedury, szybkość reakcji, certyfikaty, audyt wewnętrzny).

8. Audyt bezpieczeństwa

Po dokonaniu wyboru firmy należy dokonać weryfikacji usługi z analizą zagrożeń, opisem aktualnego systemu bezpieczeństwa i uwagami. Pomocne mogą być pisane oceny i bieżące raporty. Stąd pojawia się potrzeba kształcenia w specjalnościach takich jak: zarządzanie bezpieczeństwem, bezpieczeństwo biznesu, informacji, teleinformatyczne itd. Politykę bezpieczeństwa można kreować w wymiarze operacyjnym i ekonomiczno-organizacyjnym. Coraz częściej firmy decydują się na powołanie pełnomocnika do zarządzania bezpieczeństwem (security menager). Do jego obowiązków należy również audyt bezpieczeństwa, który ma na celu ocenę procesów związanych z bezpieczeństwem w tym regulacji prawnych i standardów.



Rys. 7. Poziomy audytu.

Istotnym elementem dla audytu jest określenie kluczowych wskaźników bezpieczeństwa i ocena istniejącego systemu zabezpieczeń (budowlanych, mechanicznych, technicznych, fizycznych czy organizacyjno-prawnych). Poziomy audytu różnią się częstotliwością i obszarem badawczym. Zagrożenia bezpieczeństwa zawiązane są

z działalnością biznesową firm. Może to być zagrożenie, jak wspomniano, kryminalne, gospodarcze czy terrorystyczne czy teleinformatyczne. Możliwość zapewnienia podmiotowi akceptowalnego przez niego stanu bezpieczeństwa wymaga, między innymi, wiedzy a priori: o naturze zagrożeń i możliwościach ich rozpoznawania za pomocą aktualnie dostępnych środków.

9. Polityka bezpieczeństwa

Załącznik A do normy zabezpieczeń PN-ISO/IEC 27001:2007 uwzględnia m.in. politykę bezpieczeństwa, organizację bezpieczeństwa informacji, bezpieczeństwo osobowe, bezpieczeństwo fizyczne i środowiskowe, kontrolę dostępu czy zarządzanie incydentami związanymi z bezpieczeństwem informacji. Ta międzynarodowa norma ma zapewnić bezpieczeństwo informacji, ale wskazuje na ogólne elementy działań organizacji mające na celu zminimalizowanie zagrożeń[8].

Na tej podstawie można budować zasadnicze zależności koncepcji ochrony. Przedsiębiorstwa ochrony osób i mienia dobrze radzą sobie z rynkowymi potrzebami w tym ustawowym zakresie. Jednym z podstawowych zadań zawsze będzie przeprowadzona analiza bezpieczeństwa z właściwie określonym stopniem zagrożenia i określeniem nakładów rzeczowo-finansowych[9]. Projekty normy europejskiej przewidują 12 kategorii (dla obiektów budowlanych), dla których ustala się współczynnik ryzyka (od 0 do 5). Pracownik ochrony fizycznej sporządzając plan ochrony powinien posiadać znajomość zabezpieczeń technicznych.

Znając rodzaj zagrożeń musimy znaleźć właściwą koncepcje ochrony w oparciu o zabezpieczenia:

a) architektoniczno-budowlane, „zniechęcające”(lokalizacja, konstrukcja, oświetlenie),

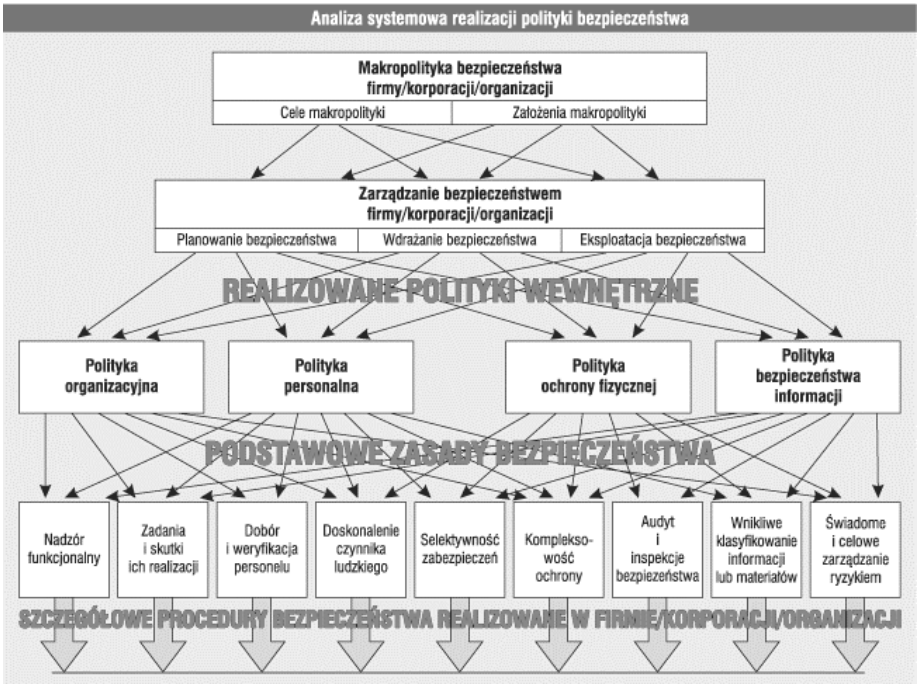
b) mechaniczne, „opóźniające”(zamki, okucia, kłódki, blokady, sejfy, szyby specjalne, folie, siatki, rolety),

[8] Norma PN-ISO/IEC 27001:2007 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, Warszawa, PKN 2007.

[9] Polska norma PN-93/E-8390/14 wyróżnia 4 kategorie zagrożonych wartości (od Z1 do Z4), a do ich szacowania można posługiwać się wielokrotnością N średniego rocznego dochodu pracownika w 5 podstawowych działach gospodarki

c) elektroniczne, „wykrywające" (systemy alarmowe, telewizja przemysłowa, systemy kontroli dostępu),

d) organizacyjno-taktyczne.



Rys 8. **Makropolityka bezpieczeństwa jako strategia wieloetapowego i wielopoziomowego działań.** ***(za M. Blim, Teoria ochrony informacji, Zabezpieczenia, nr 3/2007)***

Są to środki „zaradcze" mające na celu zminimalizowanie zagrożenia. Do nich też zaliczyć można wspomnianą wyżej ochronę fizyczną, politykę bezpieczeństwa, bezpieczeństwo informacji i danych

Znając rodzaj zagrożeń, oczekiwania firm i ich możliwości finansowe można przystąpić do modyfikacji struktury organizacyjnej w zakresie doboru ludzi i szeroko pojętej logistyki. Wszystkie firmy różnią się podatnością (rodzaj wykonywanej działalności) i atrakcyjnością (rodzaj i wielkość szkody). Bezpieczeństwo ma charakter podmiotowy, a rozwój firm ochrony uzależniony jest od stanu gospodarki i ekonomicznej kondycji tych podmiotów. Rozwój usług „ochroniarski" umożliwiły same przedsiębiorstwa, które zrezygnowały z ochrony „na własną rękę", a ochronę swoich przedsiębiorstw powierzyły „firmom z koncesją".

Konkurencja natomiast „wymusiła" jakość usług i zastosowanie nowoczesnych strategii zarządzania.

Rys. 7. Zasadnicze zależności budowy koncepcji ochrony (Za M. Blim, Teoria ochrony informacji cz.2, Zabezpieczenia nr 4/2007,

Summary

This paper is dedicated on problem of safety of business, which security is carried by companies, that are business venture (for-profit). Autor is showing definition of "Business Safety" and common elements of organization structures, that are responsible for safety in firm. It make a view on need to build safety policy in context of current threats on outside and inside envoirment of company. Considers that are included in this paper takes account of making audit need and appointing security menagers.

Bibliografia

1. M. Blim, *Teoria ochrony informacji*, „Zabezpieczenia" nr 3/2007.
2. P. Kubiński, *Koncesjonowanie działalności gospodarczej w zakresie ochrony osób i mienia jako forma reglamentacji publicznoprawnej*

ministra spraw wewnętrznych i administracji. Raport z badań, [w:] Przegląd Policyjny nr 4 (88)
3. P. Tyrała, *Bezpieczeństwo wymaga kompetencji. Na drodze do securitologii*, „Teraz" 2002 r., nr 31, 32, 33
4. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, Dz. U. nr 114, poz. 740 z późn. Zmianami
5. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz. U. nr 11, poz. 95 z późn. Zmianami.

Część 2

Komunikacja i bezpieczeństwo

Mirosław Czapiewski*
Stanisław Gutowski**
Andrzej Urban***

KONCEPCJA FUNKCJONOWANIA JEDNOSTKI ORGANIZACYJNEJ REALIZUJĄCEJ FUNKCJE SYSTEMÓW BEZPIECZEŃSTWA W STRUKTURZE PRZEDSIEBIORSTWA WIELOODZIAŁOWEGO – MODEL APLIKACYJNY

Streszczenie

Niniejsze opracowanie przygotowane zostało w celu przedstawienia propozycji rozwiązań strukturalnych systemu funkcjonowania organizacji przedsiębiorstwa o znaczeniu strategicznym dla gospodarki w obszarach ochrony osób i mienia, ochrony informacji niejawnych, ochrony danych osobowych, ochrony tajemnicy przedsiębiorstwa, ochrony systemów teleinformatycznych oraz spraw obronnych. Zawarty w nim projekt funkcjonowania departamentu systemów bezpieczeństwa oparto na diagnozie istniejących rozwiązań organizacyjnych w tym obszarze zarówno w centrali, jak i w terenowych oddziałach przedsiębiorstwa, rozwiązaniach benchmarkingowych oraz na podstawie uwarunkowań formalno-prawnych stawianych tego typu podsystemom zarządzania. W wyniku przeprowadzonych analiz powstał model rozwiązań strukturalnych systemu bezpieczeństwa którego rozwinięcie stanowi rozwiązanie aplikacyjne stosowane z sukcesem w praktyce gospodarczej.

*Autor jest pracownikiem Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni.
**Autor jest pracownikiem Energa Operator SA. Pełnomocnik Zarządu ds. Systemów Bezpieczeństwa.
*** Autor jest pracownikiem Energa Operator SA. Dyrektor Biura Systemów Bezpieczeństwa.

Wstęp

Systemy bezpieczeństwa w przedsiębiorstwach o strategicznym znaczeniu dla funkcjonowania gospodarki danego państwa są istotnym elementem konfiguracji jego organizacji. Proces projektowania konstrukcji strukturalnej, funkcji i zadań jednostek organizacyjnych odpowiedzialnych za obszar systemów bezpieczeństwa jest determinowany nie tylko przez uwarunkowania metodologiczne związane z wyborem metody projektowej – diagnostycznej czy też prognostycznej – lecz również przez determinanty prawne i organizacyjne. Szczególną rolę odgrywają determinanty prawne i organizacyjne. Pierwsza grupa stanowi podstawę formalizującą funkcje obligatoryjne, drugi obszar stanowi odzwierciedlenie organizacyjne sformalizowanych funkcji formalnych i obszaru funkcji fakultatywnych. Przedstawione rozwiązania funkcjonalne i strukturalne mogą stanowić podstawę do rozważań związanych z procesami benchmarkingu dla innych podmiotów wielozakładowych i są przykładem zastosowania rozwiązań funkcjonalnych podnoszących sprawność funkcjonowania systemów bezpieczeństwa w organizacji.

1. Prawne determinanty funkcjonowania Systemów bezpieczeństwa

Analizowane przedsiębiorstwo jest podmiotem gospodarczym o strategicznym znaczeniu dla gospodarki narodowej i jego funkcjonowanie determinowane jest przez istniejący system przepisów prawa zarówno w obszarze działalności gospodarczej jak i obszarze bezpieczeństwa. Szczególną istotną rolę dla funkcjonowania systemów bezpieczeństwa przedsiębiorstwa mają:
Ustawa o ochronie osób i mienia[1] – oraz 19 rozporządzeń wykonawczych z nią powiązanych. Ustawa określa obszary, obiekty i urządzenia ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa podlegające obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenia techniczne. Ustawa określa zadania i obowiązki kierownika jednostki, który zarządza tymi obszarami, obiektami i urządzeniami. Ponadto, ustawa zawiera

[1]Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia - Dz. U. z 2005r. Nr 145, poz.1221 z późniejszymi zmianami.

uregulowania prawne odnoszące się do zasad tworzenia i funkcjonowania wewnętrznych służb ochrony oraz nadzoru nad nimi.

Ustawa o ochronie informacji niejawnych[2] – która określa zasady ochrony informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem jako stanowiące tajemnice państwową lub służbową, a w szczególności:

- organizowanie ochrony, klasyfikowanie, udostępnianie informacji niejawnych;
- postępowanie sprawdzające w celu ustalenia, czy osoba nim objęta daje rękojmę zachowania tajemnicy;
- szkolenie w zakresie ochrony informacji niejawnych;
- ewidencjonowanie, przechowywanie, przetwarzanie i udostępnianie danych uzyskanych w związku z prowadzonymi postępowaniami o ustalenie rękojmi;
- zachowania tajemnicy w zakresie określonym w ankiecie bezpieczeństwa oraz kwestionariuszu bezpieczeństwa przemysłowego;
- organizację kontroli przestrzegania kontroli zasad ochrony informacji niejawnych;
- ochronę informacji niejawnych w systemach i sieciach teleinformatycznych;
- stosowanie środków fizycznej ochrony informacji niejawnych.

Uzupełnieniem są rozporządzenia wykonawcze do ustawy o ochronie informacji niejawnych (łącznie 12 rozporządzeń) oraz ustawy i rozporządzenia w obszarze obronności i klęsk żywiołowych (łącznie 27 aktów prawnych w postaci ustaw i rozporządzeń)

Ustawa o ochronie danych osobowych[3] **–** która określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Ustawa w swojej treści formułuje obowiązek administratora przetwarzającego dane do wdrożenia kompleksowej polityki bezpieczeństwa w odniesieniu do potrzeby zabezpieczenie

[2] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych – Dz. U. z 2005 r. Nr 196 poz. 1631 z późniejszymi zmianami.

[3] Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – Dz. U. z 2002 r. Nr 101, poz. 926 z późniejszymi zmianami.

gromadzonych danych zarówno w systemach informatycznych jak i wytwarzanych w sposób tradycyjny.

Ustawa o zwalczaniu nieuczciwej konkurencji[4] **–** która reguluje zapobieganie i zwalczanie nieuczciwej konkurencji w dziedzinie gospodarczej, w szczególności produkcji przemysłowej i rolnej, budownictwie, handlu i usługach – w interesie publicznym, przedsiębiorców oraz klientów. Ustawa definiuje pojęcie tajemnicy przedsiębiorstwa.

2. Zadania w obszarze bezpieczeństwa realizowane w istniejącej strukturze organizacyjnej

W dotychczasowej strukturze organizacyjnej badanego podmiotu zadania z zakresu systemów bezpieczeństwa realizowane były przez poszczególne komórki organizacyjne w ramach przyporządkowanych im zakresów uprawnień, zadań i odpowiedzialności. Nie występowała w strukturze organizacyjnej komórka organizacyjna lub zespół komórek, którym przyporządkowane byłyby kompleksowo zadania w zakresie funkcjonowania systemów bezpieczeństwa. Taki stan rzeczy powodował, że zadania te nie w pełni pokrywały swoim zakresem wszystkie obszary, które miały wpływ na sprawność funkcjonowania systemu. W rzeczywistości wykonywane były tylko niektóre działania w tym zakresie. Wymienione poniżej komórki organizacyjne badanego podmiotu realizowały następujące zadania w obszarze systemów bezpieczeństwa:

Zadania z zakresu ochrony mienia stanowiącego własność badanego podmiotu realizował Wydział Inspekcji Energetycznej wchodzący w skład Departamentu Dystrybucji. Zgodnie z Regulaminem Organizacyjnym analizowanego podmiotu wydział ten realizował następujące zadania:

- opracowywanie i koordynacja planów przedsięwzięć mających na celu ograniczanie strat wynikających z różnicy bilansowej przy współpracy z komórkami organizacyjnymi Centrali i Oddziałów;
- opracowywanie i aktualizacja jednolitych procedur i instrukcji dotyczących kontroli wykrywania nielegalnych poborów energii elektrycznej;

[4] Ustawa z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji Dz.U. z 2003 r. Nr 153 poz.1503 z późniejszymi zmianami,

- prowadzenie nadzoru oraz egzekwowanie przestrzegania regulaminów i procedur w Oddziałach w zakresie wykrywania nielegalnych poborów energii elektrycznej;
- współpraca z organami Policji i Prokuratury w zakresie wykrywania i likwidacji nielegalnych poborów energii elektrycznej oraz ścigania sprawców kradzieży elementów sieci;
- prowadzenie i koordynacja współpracy z podmiotami zewnętrznymi w zakresie wykrywania i likwidacji nielegalnych poborów energii elektrycznej w systemie zleconym;
- prowadzenie ewidencji pracowników i osób zatrudnionych z podmiotów zewnętrznych uprawnionych do przeprowadzania kontroli dotrzymywania przez odbiorców warunków zawartych umów sprzedaży energii elektrycznej;
- organizowanie i koordynacja szkoleń dla komórek organizacyjnych w Oddziałach w zakresie ograniczania strat w tym wykrywania nielegalnych poborów energii elektrycznej;
- prowadzenie nadzoru nad sposobem weryfikacji kwalifikacji pracowników uprawnionych do przeprowadzania kontroli dotrzymywania przez odbiorców warunków zawartych umów sprzedaży energii elektrycznej;
- prowadzenie zbiorczej statystyki w zakresie spraw Wydziału;

Diagnoza stanu istniejącego wykazała, że analizowana komórka organizacyjna nie realizowała zadań z zakresu ochrony osób, a ochrona mienia ogranicza się do identyfikacji oraz likwidacji nielegalnych poborów energii elektrycznej i kradzieży elementów sieci.
Badany podmiot nie posiadł w swojej strukturze innej komórki organizacyjnej zadaniem której byłaby realizacja zapisów ustawy o ochronie osób i mienia. Nie były w związku z tym realizowane zadania w zakresie nadzoru i kontroli w stosunku do Oddziałów terenowych.
Zadania zakresu ustawy o ochronie informacji niejawnych i spraw obronnych realizowane były przez Sekcję ds. Ochrony Informacji Niejawnych i Spraw Obronnych znajdującej się w strukturze Biura Zarządu. Zgodnie z Regulaminem Organizacyjnym Sekcja ta realizowała następujące zadania:

- określanie polityki i realizacja zadań wynikających z ustawy o ochronie danych osobowych i informacji niejawnych w skali Spółki;

- prowadzenie spraw związanych z obronnością oraz ustalanie zasad w tym zakresie, obowiązujących w Spółce;
- prowadzenie kancelarii tajnej;
- zamawianie, ewidencjonowanie, przyjmowanie zgłoszeń o zagubieniu lub zniszczeniu dotyczących pieczęci, stempli oraz pieczątek imiennych;

Na podstawie działań diagnozujących, dostępnych materiałów i ustaleń zidentyfikowano że zadania te w Centrali badanego podmiotu oraz oddziałach terenowych były realizowane na dobrym poziomie.

Zadania z obszaru uregulowanego ustawą o ochronie danych osobowych miały być zgodnie z zapisem znajdującym się w Regulaminie Organizacyjnym badanego podmiotu realizowane przez Sekcję ds. Ochrony Informacji Niejawnych i Spraw Obronnych. W rzeczywistości te zadania nie były realizowane przez pracowników tej sekcji. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku w badanym podmiocie nie była w odpowiedni sposób realizowana.

Przeprowadzone działania diagnozujące stan badanej organizacji w obszarze realizacji zadań w zakresie systemów bezpieczeństwa zidentyfikowały następujące dysfunkcje organizacyjne:

- brak komórek organizacyjnych odpowiedzialnych za problematykę systemów bezpieczeństwa w oddziałach terenowych;
- pełnomocnicy ds. informacji niejawnych nie są podporządkowani bezpośrednio kierownikom oddziałów terenowych;
- brak opracowanej polityki bezpieczeństwa na poziomie centrali badanego podmiotu spowodował, że w chwili niektóre oddziały terenowe opracowały własną politykę bezpieczeństwa a niektóre czekały na decyzje centrali;
- funkcję ABI pełnili przypadkowi pracownicy. Praca ABI to najczęściej dodatkowe zajęcie. Występowały przypadki braku przeszkoleń w tym zakresie;
- brak spójnego systemu szkoleń dla ABI;
- zadania w zakresie ochrony osób i mienia najczęściej sprowadzały się do zlecenia zewnętrznym firmom ochrony (po przeprowadzeniu odpowiednich procedur wynikających z przepisów prawnych) realizacji zadań w zakresie zabezpieczenia obiektów oddziałów terenowych. W strukturach centrali badanego podmiotu i w jej oddziałach terenowych nie było pracowników uprawnionych (z licencją II stopnia) do tworzenia i modyfikacji planów ochrony.

Powodowało to, że przygotowanie planów ochrony zlecane było zewnętrznym zleceniobiorcom i na ich podstawie dokonywano realizacji usługi ochrony.

3. Projekt rozwiązań strukturalnych w zakresie systemów bezpieczeństwa

Zdiagnozowany stan systemów bezpieczeństwa w badanym podmiocie wskazywał na potrzebę podjęcia działań zmierzających do stworzenia kompleksowego systemu polityki bezpieczeństwa w celu uporządkowania i ujednolicenia istniejących elementów systemów bezpieczeństwa oraz wdrożenia procedur w obszarach nie objętych tymi systemami. Efektem tak przeprowadzonych działań było zaprojektowanie kompleksowego, spójnego i kompatybilnego, zarówno w centrali jak i w poszczególnych oddziałach terenowych, systemu bezpieczeństwa organizacji.
Koncepcję zarządzania tym obszarem oparto na modelu organizacyjnych zależności liniowo – funkcjonalnych. W projekcie zastosowano model zarządzania systemami bezpieczeństwa którego głównym elementem jest podporządkowane bezpośrednio Prezesowi Zarządu Badanego podmiotu **Biuro Systemów Bezpieczeństwa,** składające się z następujących wydziałów:

- Wydział Ochrony Osób i Mienia;
- Wydział Bezpieczeństwa Informacji;
- Wydział Spraw Obronnych i Ochrony Informacji.

Poszczególne wydziały realizowały następujące zadania w zakresie funkcjonowania systemów bezpieczeństwa:

Wydział Ochrony Osób i Mienia:

- przygotowywanie założeń do kierunków strategicznych opracowywanej polityki bezpieczeństwa organizacji;
- przygotowywanie założeń do planów ochrony spółki;
- organizowanie i koordynacja szkoleń dla komórek organizacyjnych w oddziałach terenowych w zakresie sposobów zapobiegania przestępstwom i wykroczeniom na szkodę badanego podmiotu;
- prowadzenie ścisłej współpracy ze wszystkimi komórkami organizacyjnymi badanego podmiotu w zakresie ujawniania, rozpoznawania i eliminowania wszelkich nieprawidłowości prowadzących do zagrożeń dla osób i mienia,

- opracowywanie i koordynowanie planów działań zapobiegających przestępstwom i wykroczeniom na szkodę osób i mienia badanego podmiotu;
- nadzór nad sposobem realizacji ochrony fizycznej i zabezpieczenia technicznego mienia zarówno w centrali jak i oddziałach terenowych;
- prowadzenie działań zmierzających do niedopuszczenia wejść osób nieuprawnionych na obszary chronione w badanym podmiocie;
- organizowanie i prowadzenie kontroli w oddziałach terenowych;
- współpraca z organami ścigania w zakresie: zapobiegania, ujawniania, zgłaszania i wykrywania sprawców przestępstw i wykroczeń na szkodę osób i mienia w badanym podmiocie;
- informowanie Zarządu o efektach prowadzonych działań, potencjalnych zagrożeniach oraz przedstawianie stosownych wniosków i planów,
- opracowywanie procedur i planów reagowania w sytuacjach kryzysowych,

Wydział Bezpieczeństwa Informacji:

- w zakresie ochrony danych osobowych:

- przygotowywanie założeń do kierunków strategicznych polityki bezpieczeństwa organizacji;
- opracowanie i wdrożenie polityki bezpieczeństwa danych osobowych zgodnie z wymogami zawartymi w rozporządzeniu MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- wdrożenie wewnętrznych przepisów regulujących ochronę danych osobowych;
- nadzór nad przestrzeganiem zasad ochrony danych osobowych;
- prowadzenie wykazu stanowisk zajmowanie których może łączyć się z ochroną danych osobowych;
- opracowanie i wdrożenie szkoleń z zakresu ochrony danych osobowych;
- nadzór nad wydawaniem upoważnień do przetwarzanie danych osobowych;
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

- rejestrowanie zbiorów danych osobowych znajdujących się w centrali badanego podmiotu i sprawowanie nadzoru nad tą problematyką w oddziałach terenowych;
- nadzór nad wprowadzaniem danych osobowych do zbiorów oraz dalszym ich przekazywaniem;
- udzielanie informacji osobom uprawnionym o treści posiadanych na jej temat danych;
- nadzór nad realizacją zadań związanych z ochroną danych osobowych w oddziałach terenowych.

- w obszarze bezpieczeństwa informacji w sieciach informatycznych:
- opracowanie i wdrożenie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zgodnie z wymogami zawartymi w rozporządzeniu MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- opracowywanie i wdrażanie System Zarządzania Bezpieczeństwem Informacji a także nadzorowanie realizacji w oddziałach terenowych;
- określanie niezbędnych wymagań i standardów w zakresie bezpieczeństwa informacji i objecie nadzorem ich realizacji;
- przeciwdziałanie dostępowi osób niepowołanych do systemu w którym przetwarzane są dane osobowe;
- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń lub podejrzenia naruszenia;
- opracowywanie planów minimalizacji ryzyka w zakresie bezpieczeństwa teleinformatycznego;
- uczestniczenie w konsultacjach w zakresie bezpieczeństwa w projektach wewnętrznych i zewnętrznych;
- w zależności od potrzeb sporządzanie: regulaminów, procedur, instrukcji i poleceń w obszarach działalności badanego podmiotu objętych systemami bezpieczeństwa;
- organizowanie szkoleń z obszaru zarządzania bezpieczeństwem informacji;
- sprawowanie nadzoru nad fizycznym zabezpieczeniem pomieszczeń w których przetwarzane są dane osobowe;

- sprawowanie nadzoru nad naprawami konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe;
- sprawowanie nadzoru nad archiwizacją i usuwaniem danych osobowych;
- przeprowadzanie audytów nadzorowanej problematyki;
- określanie poziomu bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym.

Wydział Spraw Obronnych i Ochrony Informacji:
– w obszarze ochrony tajemnicy badanego podmiotu opracowanie następujących dokumentów:

- wykazu materiałów stanowiących tajemnicę badanego podmiotu;
- szczegółowych wymogów w zakresie ochrony informacji;
- zasad wytwarzania materiałów;
- zasad udostępniania informacji;
- rejestracji i obiegu materiałów;
- zasad kompletowania i brakowania, oraz przekazywania ich do archiwum;
- zasad ochrony fizycznej i technicznej;
- zasady przyjmowania, przewożenia, wydawania i ochrony;
- zasady postępowania w przypadku naruszenia zasad ochrony lub ujawnienia;
- wykazu stanowisk i prac zleconych z którymi łączy się dostęp do tych informacji;
- procedur zarządzania systemem informatycznym służącym do przetwarzania informacji;
- wzorów dokumentów niezbędnych do wdrożenia /i ciągłego stosowania/przepisów regulujących tą problematykę;
- instrukcji w sprawie zasad oznaczania i umieszczania na materiałach klauzuli „Tajemnica Spółki”;
- wdrażanie przygotowanych dokumentów w centrali;
- aktualizacja powyższych uregulowań zawartych w dokumentacji organizacyjnej centrali i oddziałów terenowych;
- prowadzenie działań nadzorczych i kontrolnych w obszarze objętym działaniem systemów bezpieczeństwa;
- składanie rocznego pisemnego sprawozdania Zarządowi badanego podmiotu z przestrzegania tajemnicy Spółki.

– w zakresie zadań ochrony informacji niejawnych:

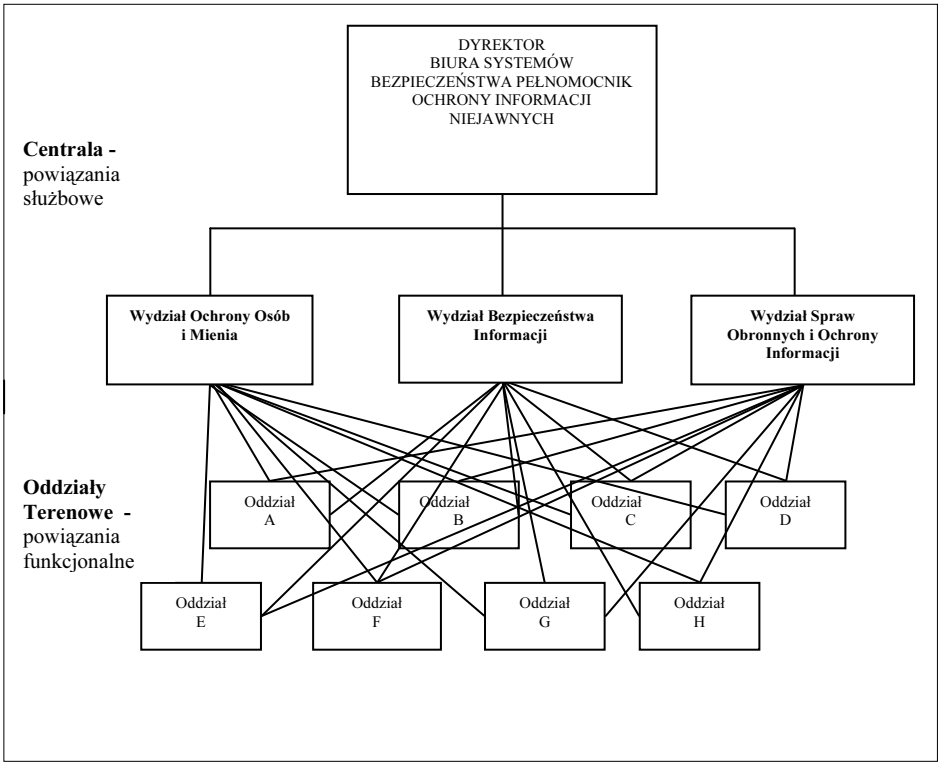
- organizowanie i realizowanie w badanym podmiocie zadań określonych w ustawie o ochronie informacji niejawnych i rozporządzeniach wykonawczych;
- prowadzenie zwykłych postępowań sprawdzających i wydawanie poświadczeń bezpieczeństwa;
- prowadzenie wykazu stanowisk pracowników posiadających upoważnienia do dostępu do informacji niejawnych;
- organizowanie i prowadzenie szkoleń dla pracowników z zakresu przepisów ustawy o ochronie informacji niejawnych;
- prowadzenie kancelarii tajnej;
- zamawianie, ewidencjonowanie, przyjmowanie zgłoszeń o zagubieniu lub zniszczeniu dotyczących pieczęci, stempli oraz pieczątek imiennych w centrali;
- nadzorowanie i kontrolowanie sposobu realizacji zadań z zakresu ochrony informacji niejawnych w oddziałach terenowych;
- podjęcie i kontynuowanie działań ukierunkowanych na uzyskanie przez badany podmiot świadectwa bezpieczeństwa przemysłowego.

– w zakresie spraw obronnych:

- realizowanie zadań obronnych w centrali badanego podmiotu;
- nadzór nad realizacją zadań obronnych w oddziałach terenowych;
- opracowywanie przepisów wewnętrznych w zakresie przygotowań obronnych;
- opracowywanie dokumentów planistycznych w zakresie przygotowań obronnych;
- opracowywanie i uaktualnianie dokumentów związanych ze stopniem osiągania gotowości obronnej badanego podmiotu;
- opracowywanie planów i programów szkoleń obronnych a także prowadzenie szkoleń dla pracowników;
- nadzór nad sposobem realizacji zadań w oddziałach terenowych;
- opracowywanie sprawozdań okresowych.

W zaprojektowanym rozwiązaniu struktury zastosowano dwa rodzaje powiązań organizacyjnych. Pierwsze – liniowe powiązania określają zależności organizacyjne pomiędzy poszczególnymi komórkami organizacyjnymi tworząc wewnętrzną strukturę biura. Drugi rodzaj powiązań – funkcjonalne hierarchiczne – określa zależności w zakresie

nadzoru oraz cedowania zakresu uprawnień, obowiązków i odpowiedzialności na odpowiednie komórki organizacyjne znajdujące się w strukturach organizacyjnych oddziałów terenowych. Schemat struktury organizacyjnej Biura Systemów Bezpieczeństwa i powiązań funkcjonalnych z oddziałami terenowymi przedstawia rys. nr 1.



Rys. 1. Struktura organizacyjna Biura Systemów Bezpieczeństwa i powiązania funkcjonalnych z oddziałami terenowymi

Podsumowanie

Działania diagnozujące związane z audytem istniejących rozwiązań strukturalnych pozwoliły na zidentyfikowanie dysfunkcji występujących w organizacji w zakresie funkcjonowania systemów bezpieczeństwa. Analizując uwarunkowania prawne oraz potrzeby organizacji w obszarach ochrony osób i mienia, bezpieczeństwa informacji niejawnych, ochrony informacji przedsiębiorstwa oraz spraw obronnych

zaprojektowano i wdrożono nowe rozwiązanie strukturalne w obszarze systemów bezpieczeństwa. Opierając nowe rozwiązanie na połączeniu powiązań liniowych i funkcjonalnych - hierarchicznych stworzono sprawnie działający system charakteryzujący się możliwościami szybkiego przepływu informacji pomiędzy poszczególnymi podsystemami bezpieczeństwa w grupie i tym samym usprawniono procesy podejmowania decyzji, koordynowania działań i szybkiego reagowania na odchylenia od stanów pożądanych dla organizacji. Przedstawione rozwiązanie strukturalne może stać się podstawą do modelowania funkcjonowania systemów bezpieczeństwa w innych organizacjach wielozakładowych – grupach kapitałowych, gdzie występuje potrzeba koordynacji i nadzoru obszarów bezpieczeństwa w organizacji.

Bibliografia

1. Ustawa z dnia 22 sierpnia 1997 roku o ochronie osób i mienia – Dz. U. z 2005r. Nr 145, poz.1221 z późniejszymi zmianami.
2. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – Dz. U. z 2002r. Nr 101, poz. 926 z późniejszymi zmianami.
3. Ustawa z dnia 22 stycznia 1999 roku o ochronie i formacji niejawnych - Dz. U. z 2005r. Nr 196 poz. 1631 z późniejszymi zmianami**.**
4. Ustawa z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji Dz. U. z 2003r. Nr 153 poz.1503 z późniejszymi zmianami.

THE CONCEPT OF ORGANISATION OF THE SECURITY UNIT IN THE MULTIDIVISIONAL COMPANY – THE APPLIED MODEL

Summary

This study bas been prepared in order to present proposals of structural solutions regarding the organisation of the security function in the strategically important enterprise in the Polish economy. The proposal covers the following areas: personnel and property protection, protection of the classified information, personnel data

protection, protection of corporate information, teleinformation systems protection, as well as defence issues.

The proposal of functioning of the security department, included in this study has been based on a diagnosis of the existing organizational solutions (in head office and divisions) in this security area.
Moreover, it has been based on benchmarking solutions as well as legal and formal requirements expected from such managerial subsystems.
As a result of the conducted analysis the model of the structural solutions in the security system has been created. This model ‘s solutions has been successfully applied in the business area.

Mirosław Matosek*

ZARZĄDZANIE KOMUNIKACJĄ W SYTUACJI KRYZYSOWEJ

Wstęp

Światowy kryzys finansowy, zamieniający się stopniowo w głęboką recesję, który jesienią ubiegłego roku uderzył w nasz rynek, obnażył słabości polskiej gospodarki i systemów zarządzania w przedsiębiorstwach. Jednym z ukrywanych do tej pory mankamentów jest fakt, że tylko nieliczne firmy i instytucje posiadają systematyczne i zintegrowane programy zarządzania w sytuacji kryzysowej. Niefrasobliwe zachowania kierownictwa można porównać tu do prowadzenia działalności gospodarczej bez polisy ubezpieczeniowej.

Myślenie w kategoriach kryzysu, a więc w warunkach niepewności, nie jest przecież zjawiskiem nowym. Podejście takie jest nieodzowne menedżerom od drugiej połowy XX wieku. Każda jednostka i organizacja funkcjonuje w burzliwym i często nieprzyjaznym otoczeniu. Po kryzysie naftowym lat siedemdziesiątych niepewność stała się przedmiotem badań naukowych i atrybutem w dziedzinie zarządzania.

Zarządzanie sytuacją kryzysową jest pojęciem określającym strategię firmy, w tym strategię komunikowania się w sytuacji, gdy kierownictwo podejmuje próbę przygotowania się na odparcie zagrożeń, które mogą, ale nie muszą wystąpić. Budowanie takiej strategii można porównać do poszukiwania recepty na ewentualną chorobę.

1. Pojęcie kryzysu

W chwili obecnej słowa takie jak kryzys, zwiastun katastrofy czy klęski, utożsamiane są z zawirowaniami na rynku kredytów hipotecznych, papierów pochodnych i banków, kurczącym się portfelem zamówień w przedsiębiorstwach, coraz słabszymi wynikami finansowymi i niekorzystnymi wskaźnikami eksportu. W kryzysowym

* Autor jest pracownikiem Wyższej Szkoły Biznesu i Administracji w Łukowie.

kalejdoskopie wyobrażeń przewijają się cięcia świadczeń socjalnych, masowe redukcje etatów i bezrobocie, strajki w zakładach i zamieszki na ulicach, interwencje sił policyjnych, niekompetencja i arogancja władz. Rodzi się pytanie, czy nie zbyt łatwo ulegamy panice.

Warto przy okazji przypomnieć, że już w latach 80-tych ubiegłego stulecia słowo kryzys i jego synonimy przestały odnosić się wyłącznie do wypadków w środowisku naturalnym. Wydarzenia, które były w przeszłości utożsamiane głównie z kataklizmami przyrody, występują obecnie w codzienności przedsiębiorstw. Ich zakres przewyższa zniszczenia wynikające z katastrof naturalnych, a negatywne skutki osłabiają, a nawet niszczą pozytywny wizerunek istniejący w świadomości otoczenia. Przykładami mogą być wydarzenia kojarzące z takimi hasłami jak: Czarnobyl, Union Corbide w Bophal, wyciek z tankowca Exxon Valdex, Kursk, okruchy szkła w odżywkach Gerbera, czy 11 września w World Trade Center.

Dramatyczne przykłady ilustrują w wymierny sposób definicję kryzysu. I tak np. według B. Wawrzyniaka[1], pioniera w badaniach tego zagadnienia w Polsce, w potocznym rozumieniu kryzys oznacza na ogół trudną sytuację, która istnieje w danym momencie, bądź też może wystąpić. W ujęciu tym kryzysem jest zarówno załamanie gospodarki światowej, jak i sytuacja stresowa wynikająca z uciążliwości codziennego życia. Może być odczuwany bardziej lub mniej dotkliwie, mieć różny czas trwania i zakres, to jednak zawsze kryzys oznacza przełom między dwiema różnymi jakościowo fazami procesu. Kończy się jeden, a zaczyna drugi etap, rozwój sytuacji i sposób działania.

2. Środowisko rozwoju sytuacji kryzysowej

Od ubiegłego roku uwaga organizacyjna mediów i pojedynczych osób koncentruje się na wskaźnikach ekonomicznej i regulacyjno-prawnej sfery makrootoczenia. Na drugi plan zeszły technologiczne i wynikające z infrastruktury przyczyny rodzącego się niebezpieczeństwa. Ocena ewentualnego ryzyka pomija tzw. miękkie aspekty zarządzania jak komunikowanie społeczne, kultura organizacyjna firmy i zwykłe ludzkie emocje. Takie podejście rodzi

[1] B. Wawrzyniak (red.), *Zarządzanie w kryzysie, koncepcje, badania, propozycje,* Wyd. PWE, Warszawa 1985.

niebezpieczeństwo załamania się jednego z kluczowych elementów strategii antykryzysowej tj. systemu komunikacji wewnętrznej i z otoczeniem przedsiębiorstwa. Krótkowzroczne kierownictwo może nie dostrzegać, że poważne kryzysy w firmie pojawiają się w wyniku równoczesnego załamania się systemów ekonomicznych, technicznych, organizacyjnych i czynników ludzkich.

I.J. Mitroff i C.M. Pearson[2] radzą, by analizować organizacje w kontekście kryzysu jak organizm podobny w budowie do cebuli. Odsłonięcie zewnętrznej powłoki pozwala dostrzec głębsze warstwy, zrozumieć współzależności podsystemów w przedsiębiorstwie.

W porównaniu z pozostałymi aspektami organizacyjnymi najłatwiej dostrzegany jest podsystem technologii. Jego przygotowanie do sytuacji kryzysowej przejawia się w niezawodności parku maszynowego, certyfikatach jakości, instrukcjach obsługi, systemów ostrzegawczych przed awariami, sprawnej aparaturze pomiarowo-kontrolnej.

Głębszym poziomem jest infrastruktura organizacji uwzględniająca schemat organizacyjny, a więc układ powiązań zależności i władzy, finanse, system wynagradzania pracowników, formalne kanały komunikacji społecznej. Zdolność tego podsystemu do reagowania na kryzys odzwierciedla się w zakresie obowiązków i odpowiedzialności każdego pracownika, skuteczności kierowania zespołami, zakresie i jakości przeszkolenia technicznego i organizacyjnego, systemie motywacyjnym uwzględniającym zachowania podnoszące bezpieczeństwo i higienę pracy.

Truizmem jest stwierdzenie, że najcenniejszym kapitałem każdej organizacji są ludzie. Diagnozowanie zasobów ludzkich pod kątem przygotowania do kryzysu polega między innymi na badaniu obciążenia obowiązkami i poziomu stresu, ocenie predyspozycji fizycznych i psychicznych. Poprzez komunikację oddolną należy zbadać rozbieżności między wymaganiami kierownictwa, a ich zrozumieniem i oczekiwaniami ze strony załogi. Uwzględnianie opinii i sugestii ze strony pracowników może przeciwdziałać pojawiającym się nieprawidłowościom. Jak stwierdził L. Clarke[3] „sama reorganizacja struktury organizacyjnej może być „zmianą ustawienia leżaków na pokładzie Titanica" tj. działaniem, które zakłada dotychczasowy porządek, ale nie przynosi efektów.

---

[2] I.J. Mitroff, C.M. Pearson, *Zarządzanie sytuacją kryzysową,* Business Book, Warszawa 1998.

[3] L. Clarke, *Zarządzanie zmianą,* Wyd. Gebethner i S-ka, Warszawa 1997, s. 42.

Głęboko ukryte w świadomości i podświadomości pracowników są podstawowe założenia kultury organizacyjnej. Kultura, która utwierdziła pracowników w bezkrytycznym przeświadczeniu o doskonałości ich firmy, jest kulturą słabą. Poziom frustracji w obliczu kryzysu może doprowadzić do paraliżu decyzyjnego uniemożliwiającego realizację operacyjnych zadań. Badacze z Centrum Zarządzania Sytuacją Kryzysową Uniwersytetu Południowej Kalifornii cytują wypowiedzi kierowników, którzy twierdzą, że:

- sytuacje kryzysowe omijają doskonale i świetnie zarządzane firmy
- sytuacje kryzysowe nie wymagają specjalnych procedur, to zbyteczny luksus
- pożądane cele gospodarcze uzasadniają sięganie po ryzykowne środki
- mają tak bardzo oddanych pracowników, że mogą mieć do nich pełne zaufanie
- nie ma żadnego problemu dopóki nie trzeba zmieniać procedur
- łamanie prawa przez pracowników należy wkalkulować w koszty prowadzonej działalności
- każda sytuacja kryzysowa jest tak specyficzna, że nie można przygotować się na każdą ewentualność, a poważne kryzysy zdarzają się wyjątkowo rzadko
- kryzys to kwestia rozwiązań technologicznych
- zarządzanie sytuacją kryzysową jest jak polisa ubezpieczeniowa – to tylko kwestia nakładów finansowych
- wiedzą jak manipulować środkami masowego przekazu.[4]

W centrum „modelu cebuli" autorzy umieścili sferę zachowań wynikających z emocji. Ocena systemu emocjonalnego przez pryzmat kryzysu oznacza przede wszystkim możliwość swobodnego i szczerego wypowiadania się, poczucia, że w sytuacjach problemowych można liczyć na zrozumienie i wsparcie ze strony przełożonych i kolegów.

W powyższym rozumieniu kryzys nie jest zjawiskiem jednoznacznie negatywnym, bo zmusza ludzi do wprowadzenia zmian. Można traktować go (i powinno wykorzystać) jako szansę dla zdobycia nowych umiejętności i rozwoju całej organizacji.

[4] I.J. Mitroff, *op.,cit*., s. 92-94.

3. Cechy sytuacji kryzysowej

Kryzysy mogą obejmować swoim zasięgiem pojedyncze firmy i instytucje, sektory, regiony i państwa. Mogą też mieć, jak dzieje się obecnie, wymiar globalny. Pojawiają się w różnych terminach, różnią się intensywnością i czasem trwania. Zawsze jednak niosą ze sobą niepewność, ryzyko oraz bilans strat i zysków.

W przedsiębiorstwie i urzędzie administracji kryzysem można nazwać sytuację, w której zagrożone jest realizowanie podstawowych funkcji w wyniku spiętrzenia różnego rodzaju trudności, a istniejące możliwości rozwiązania zaistniałego stanu są ograniczone. Symptomy sytuacji kryzysowej, które opisali Starbuck, Greve i Hedberg[5], przedstawiają się następująco:

- atmosfera organizacyjna jest burzliwa, pełna napięć; dominują emocje, więc zachowania ludzkie pozbawione są racjonalności,
- ujawniają się nowi liderzy, którzy nie zawsze potrafią sformułować pozytywny program wyjścia z kryzysu; podważane jest zaufanie do kierownictwa,
- konflikty dysfunkcjonalne powodują rozpad zespołów i dezintegrację programów; chwieją się struktury organizacyjne,
- potrzebie „zmiany wszystkiego" towarzyszy obawa przed lawiną zmian niekontrolowanych,
- brak środków i przedłużający się czas kryzysu pogłębia poczucie niemożliwości działania – typową reakcją jest oczekiwanie, aż trudności same ustąpią.

Z kolei S. Fink[6] podkreśla, że z punktu widzenia przedsiębiorstwa kryzys jest punktem zwrotnym – zwiastunem, który pociąga za sobą ryzyko wzrostu natężenia niekorzystnego zjawiska i przyciągania uwagi mediów i władz. Narażony zostaje pozytywny wizerunek firmy i ekonomiczne wyniki prowadzonej działalności, chociaż źródło kryzysu nie musi być związane z czynnikami ekonomicznymi.

[5] Podaję za B. Wawrzyniak, *op.,cit.*
[6] S. Fink, *Crisis Management*, AMACOM, New York 1986, s. 16.

4. Typologia sytuacji kryzysowych

Kryzys jest zjawiskiem trudnym do przewidzenia. Nie można zidentyfikować wszystkich potencjalnych sytuacji kryzysowych i czynników, które je wywołują. Każde zdarzenie, a tylko część z nich ma podłoże ekonomiczne, może mieć wpływ na funkcjonowanie przedsiębiorstwa. Niemożliwe jest opracowanie strategii postępowania na wypadek wszystkich zagrożeń i ich wariantów. Takie stwierdzenie nie musi zakładać bierności kierownictwa, bowiem opracowanie procedur postępowania dla grupy sytuacji kryzysowych, zabezpiecza firmę przed ryzykiem, zmniejszając jego skłonność do popadnięcia w kłopoty.[7]

S. Black z uniwersytetu w Stirling podzielił sytuacje na dwie grupy: „znane nieznane" i „nieznane nieznane". W pierwszej mieszczą się sektory przemysłowe. Niebezpieczeństwo jest znane, ale nie wiadomo kiedy wystąpi. Przypadków z drugiej grupy nie da się logicznie przewidzieć. Obejmuje klęski żywiołowe i działania kryminalne.[8]

Typologia sytuacji kryzysowych opracowana przez naukowców z Centrum Zarządzania Sytuacją Kryzysową przy Uniwersytecie Południowej Kalifornii, opiera się na dwóch wymiarach. Pierwszym jest natura kryzysu – negatywne wydarzenie może dotyczyć ekonomii lub techniki, może też być problemem ze sfery psychospołecznej. Drugim wymiarem jest „stopień powszechności" występowania kryzysu – od częstych, codziennych sytuacji po zdarzenia nietypowe i ekstremalne jak np. patologie zachowań. Skrzyżowanie wymiarów umożliwia wyodrębnienie pewnych grup, „rodzin" sytuacji kryzysowych. I tak np. do zewnętrznych zagrożeń o charakterze ekonomicznym, przebiegających w sposób nietypowy można zaliczyć szantaże, wymuszenia, przekupstwa, bojkot ekonomiczny i wrogie przejęcia firmy. W sposób nietypowy i drastyczny przebiegają działania terrorystów, zamachowców i sabotażystów. Zwykłe awarie maszyn i systemu informatycznego, brak nadzoru czy zwolnienia z pracy mogą wywołać megakryzys, np. katastrofę ekologiczną. W środku modelu umieścili autorzy choroby zawodowe i inne ubytki zdrowia. Uwzględnienie w programach antykryzysowych każdej „rodziny" sytuacji pozwala organizacji równomiernie rozłożyć ryzyko i programy przygotowawcze.

---

[7] I.J. Mitroff, C.M. Pearson, *Zarządzanie sytuacją kryzysową*, Business Book, Warszawa 1998, s. 39.

[8] S. Black, *Public relations,* Dom Wydawniczy ABC, Warszawa 2003, s.153.

5. Uczestnicy sytuacji kryzysowej

Troska o wizerunek i społeczną odpowiedzialność przedsiębiorstwa wymaga uwzględnienia w komunikacji kryzysowej szerokiego kręgu interesariuszy, a więc jednostek i grup, z którymi utrzymywane są relacje. Sytuacja w firmie wywiera na nich wpływ, a więc stają się oni uczestnikami kryzysu. Odbiorcami informacji są nie tylko pracownicy i kadra kierownicza, ale również akcjonariusze, klienci, kontrahenci, konkurenci, grupy nacisku, media, władze centralne i samorządowe. Przydatna jest identyfikacja interesariuszy z punktu widzenia ról, jakie odgrywają i w jaki sposób są postrzegani przez przedsiębiorstwo. Inaczej zachowują się sprzymierzeńcy i wrogowie, bohaterowie i ofiary, wybawcy i czarne charaktery. Inną etykietę będą przypisywać organizacji pogrążonej w walce z kryzysem. Znajdą się beneficjenci, którzy odniosą określone i wymierne korzyści.[9]

6. Anatomia kryzysu

W modelu opracowanym przez S. Finka rozwój kryzysu można porównać do postępu choroby atakującej żywy organizm. Od wielu czynników zależy czy i w jaki sposób rozwinie się infekcja. Może tu mieć wpływ zarówno wiek jak i nabyta wcześniej odporność organizmu pacjenta, rodzaj choroby, dostępność do lekarstw, wiedza lekarza, a także wyposażenie w sprzęt w przypadku konieczności zabiegu.

Sytuacja kryzysowa w firmie również zaczyna się od pierwszych symptomów i podobnie jak w przypadku choroby można je zlekceważyć. Dobrze przygotowane przedsiębiorstwa są w stanie opanować kryzys w fazie wstępnej, redukując do minimum koszty skutków. Tak przedstawia się optymistyczna wersja modelu Finka.

W wersji bardzo pesymistycznej pierwsze symptomy przechodzą w fazę kryzysu ostrego, a następnie w fazę uczenia się. Odczuły to firmy, które przeszły przez kryzys nadwyrężając wyniki ekonomiczne i własną reputację. Zlekceważenie, niezauważenie czy niedoszacowanie symptomów zwiększa niebezpieczeństwo wejścia w fazę kryzysu ostrego. Wszelkie decyzje podejmowane są pod presją czasu. Mało istotne z pozoru informacje i wydarzenia, w wyniku opieszałości w działaniu lub bezczynności mogą wywołać lawinę zdarzeń mogących

[9] B. Rozwadowska, *Public relations,* Wyd. Studio Emka, Warszawa 2002, s. 178.

zagrozić istnieniu przedsiębiorstwa. W korporacji Gerber pierwsza faza kryzysu trwała trzy dni. Wizyta niezadowolonej klientki w małym sklepie, która rzekomo w odżywce bananowej znalazła okruchy szkła, wywołała w USA ogólnokrajową paranoję. Mass media ogarnęła atmosfera sensacji.

Zagrożenie wizerunku McDonald's zaczęło się od splotu kilku nieudanych akcji marketingowych. W przypadku Procter&Gambel pierwsze tąpniecie nastąpiło, kiedy tampony uznano za przyczynę zgonów spowodowanych chorobą TSS (*toxic shock syndrome*). Nawiasem mówiąc statystyczna zbieżność między TSS, a paniami używającymi tamponów nie określała marki produktu.

W pierwszym etapie sytuacji kryzysowej cenną umiejętnością jest wczesne wykrycie i prawidłowa interpretacja symptomów. Wszystkie tego typu sytuacje, z nielicznymi wyjątkami dają znać o sobie sygnałami ostrzegawczymi. Wszystkie sygnały informujące o problemie nowego typu jest w stanie wyłapać mechanizm je wykrywający. Program kontrolny zainstalowany pod kątem wykrywania awarii technicznych nie będzie w stanie ostrzec przed groźbą utraty wizerunku.

Druga faza kryzysu trwa krótko, ale jej lawinowy przebieg wydarzeń sprawia wrażenie najdłuższej w percepcji uczestników. W korporacji Gerber w ciągu niecałych dwóch miesięcy ukazało się prawie 3 tysiące informacji na temat okruchów w odżywkach. Drastycznie zmalały obroty firmy i jej udziały w rynku (o 14,4%).W Mc Donald's średnia sprzedaż przypadająca na jedną restaurację, okazała się najniższa od pięciu lat.

Trzecią fazą w sytuacji kryzysowej jest kryzys chroniczny. W McDonald's oznaczało to m.in. zwolnienie trzech dyrektorów naczelnych korporacji. Zarząd Procter&Gambel początkowo podjął walkę o niesłusznie zniesławioną markę tamponów Rely, później zdecydowano o wstrzymaniu produkcji. Z punktu widzenia utraty wizerunku była to decyzja słuszna. Niebezpieczna sytuacja dla firm wynikała z jej publicznego wymiaru. Uczestnicy zamiast rozmawiać ze sobą bezpośrednio, komunikowali się przez media. Właściciele restauracji publicznie krytykowali zarząd McDonald's, akcje firmy spadały w dół, a media w poszukiwaniu sensacji drążyły, co jest tego przyczyną.

7. Sposoby reagowania na kryzys

Praktyka zarządzania wykazuje, że większość przedsiębiorstw koncentruje swoje środki na powstrzymywaniu i ograniczaniu rozmiaru szkód. Coraz więcej organizacji wykorzystuje czas, sprzęt i ludzi w celu przygotowania się na niespodzianki kryzysowe i planuje działania zmierzające do odzyskania równowagi. Nieliczne firmy przeznaczają duże środki na wykrywanie i interpretowanie sygnałów ostrzegawczych, wskazujących ewentualne zagrożenie. Do wyjątków należą te, które nie szczędzą wysiłków na analizowanie doświadczeń z zaistniałych sytuacji problemowych i usystematyzowanie zdobytej wiedzy.

Praktyka wykazuje również, że zarządzanie sytuacją kryzysową jest procesem cyklicznym. Podejmowane działania antykryzysowe i zdobyta wiedza zwiększają zdolność organizacji do skutecznego reagowania w przyszłych sytuacjach. W zarządzaniu komunikacją i polityce informacyjnej przedsiębiorstwa w znacznym stopniu należy uwzględniać media. Warto pamiętać, że środki masowego przekazu nie tylko przekazują informacje, ale również kształtują opinię publiczną, wpływają na poglądy, a nawet na emocje odbiorców. Mogą stać się sprzymierzeńcami lub wrogami, obrońcami lub czarnymi charakterami.

8. Znaczenie komunikowania w strategii antykryzysowej

Wspomniane wcześniej przykłady pokazały, że organizacje koncentrowały wysiłki na opanowanie sytuacji kryzysowej dopiero po jej wystąpieniu. W kulminacyjnym punkcie rozwoju wiele działań nakładało się, bo trzeba je podejmować jednocześnie. W pierwszym etapie kryzysu najważniejsze jest szybkie ustalenie i interpretacja faktów, kontrolowanie szkód i komunikacja. W procesie analizy istotne jest ustalenie sedna sytuacji i przyczyn jej powstawania. Pozwoli to na uruchomienie właściwych mechanizmów powstrzymania skutków i zastopowania nowych problemów. Dobrze przygotowana strategia komunikacyjna, w tym właściwy dobór grup docelowych, pozwala na wygaszenie czasem absurdalnych zarzutów i oskarżeń.

Zarządzanie sytuacją kryzysową i komunikowanie stały się jednym z najważniejszych elementów planowania strategicznego. Programy komunikacji kryzysowej przedsiębiorstw zawierają standardowe instrumenty *public relations*: a więc skład i zadania zespołu kryzysowego, zakresy obowiązków poszczególnych członków zespołu

i rzecznika prasowego, metody doboru grup docelowych, plany operacyjne i zalecenia w kontaktach z władzami.

Strategiczne podejście do problemu kryzysu wynika z jego natury. Cechami charakterystycznymi sytuacji kryzysowej jest zarówno element zaskoczenia jak i brak rzeczywistych informacji. Kryzysy wybuchają również w weekendy, w nocy i przy nieobecności zarządu, a pierwszą ofiarą jest prawda, ginąca pod falą pogłosek, spekulacji i pytań, na które nie ma odpowiedzi. Mają wymiar publiczny i są „mięsem dziennikarskim" dla mediów. Następuje nagłośnienie problemu i intensywne śledztwo prowadzone przez otoczenie organizacji. Kaskada wydarzeń niekontrolowanych utrudnia podejmowanie decyzji. Cechy te wzbudzają w świadomości menedżerów panikę, skupienie uwagi na zadaniach krótkookresowych. Sprawiają wrażenie osaczenia problemami, eliminując wiarę w skuteczność podejmowanych decyzji.[10]

Uwzględnienie możliwości wystąpienia kryzysu w misji i filozofii działania firmy jest przejawem potrzeby stawienia czoła problemom, może zapewnić przewagę konkurencyjną. Organizacje zbyt pewne swych sił z reguły nie są przygotowane na najgorsze, bo nie przewidują porażki. Powszechnie znane jest powiedzenie: „łatwiej zapobiegać niż leczyć". Dla przedsiębiorstw działających w burzliwym otoczeniu oznacza to budowanie i uwzględnianie scenariuszy pesymistycznych.

9. Zespól antykryzysowy i jego zadania

Jednym z pierwszych zadań, obok tworzenia listy ewentualnych zagrożeń, jest stworzenie sztabu (zespołu) do spraw zarządzania sytuacją kryzysową. Kompetentna, silna i scentralizowana struktura jest zdolna do podjęcia natychmiastowych decyzji. Członkowie zespołu powinni posiadać wyraźnie oddzielone obszary odpowiedzialności. Komunikacja wewnętrzna i na zewnątrz, powinna przebiegać według precyzyjnych procedur.

W pracach sztabu uczestniczą kierownicy z rożnych wydziałów organizacji. Rozwija to procesy uczenia się i zwiększa prawdopodobieństwo wystąpienia problemów. Przeznaczenie określonych środków budżetowych na potrzeby związane z sytuacją kryzysową tj. na przygotowanie procedur i instrukcji postępowania czy stworzenie skomputeryzowanego systemu informacyjnego, zwiększa

[10] F.P. Seitel, *Public Relations*, Wyd. Felberg SJA, Warszawa 2003, s.229-230.

skuteczność działania. Zarząd organizacji o dużej gotowości kryzysowej traktuje system zarządzania sytuacją kryzysową jak nowy instrument zarządzania.

Skuteczna reakcja w burzliwym otoczeniu jest możliwa przy odpowiednim wyszkoleniu pracowników. W odpowiedzialnych firmach symulacje wariantów sytuacji są traktowane poważnie, a warsztaty szkoleniowe przekraczają swą tematyką tradycyjne zagadnienia ochrony i bezpieczeństwa.

Sedno pakietu antykryzysowego tkwi we wszechstronności działań przygotowawczych na odparcie ewentualnego zagrożenia. Diagnostyka powinna obejmować również audyt finansowo-prawny miejsc wrażliwych w organizacji i jej otoczeniu. Eksperci firmowi śledzą rozwój sytuacji kryzysowych pojawiających się w sektorze i branżach pokrewnych. W firmach konsultingowych można nabyć specjalistyczne narzędzia analityczno-diagnostyczne.

10. System komunikacji antykryzysowej

Budowanie systemu komunikacji kryzysowej rozpoczyna się od identyfikacji i interpretacji potencjalnych zagrożeń, określonych w analizach scenariuszowych. W analizie uwzględnić należy grupy docelowe będące uczestnikami kryzysu:

- kierownicy powinni zareagować na obawy i wątpliwości zgłoszone przez podwładnych,
- pracownicy są rzecznikami przedsiębiorstwa w środowiskach, w których działają; otwartość i lojalność traktowaniu pracowników zaowocuje w każdej sytuacji,
- sprzedawcy odpowiadają na pytania klientów,
- związki zawodowe – w sytuacji zagrożenia firma potrzebuje ich wsparcia,
- pracownicy „pierwszego kontaktu”; sekretarki, pracownicy recepcji i ochrony – też mają wpływ na wizerunek firmy,
- klienci – nie można dopuścić, aby kupowali produkty u konkurentów,
- dystrybutorzy – na problemy patrzą przez pryzmat swoich zakładów,
- władze administracji państwowej i samorządowej – mogą wspierać w podjętych działaniach,
- politycy – mogą skomentować sytuację,
- grupy nacisku – mogą wykorzystać sytuację do nagłaśniania swoich problemów,

- społeczności lokalne – W obecnej sytuacji, kiedy kryzys zatacza coraz szersze kręgi i zaczyna dotykać sektorów uważanych dotychczas za bezpieczne, tym większą należy przykładać wagę do społecznej odpowiedzialności przedsiębiorstw. Współpraca ze społecznościami lokalnymi w niestabilnej rzeczywistości gospodarczej może pomóc uniknąć bojkotów konsumenckich.[11]Wiele polskich firm nie potrafi, niestety, docenić roli CRS w Internecie.
- media – złe wiadomości to okazja do głośnej publikacji,
- niezależni eksperci – ustalą fakty wiarygodne dla wszystkich odbiorców informacji.

Często stosowanym pierwszym krokiem jest embargo na informacje. W praktyce oznacza to centralizację i kontrolę przepływu informacji. Mówienie ”jednym głosem” jest lepszym rozwiązaniem niż wszelkie dwuznaczności i niekontrolowane przecieki do mediów. Można zgromadzić pełen zestaw faktów, chronić dane poufne. Z drugiej strony takie zachowanie może być interpretowane przez otoczenie, jako próba ukrycia prawdy. W rezultacie powstaną publikacje pełne oskarżeń wobec przedsiębiorstwa, podgrzewające niezdrową atmosferę, których dementowanie zwiększa straty wynikające z kryzysu. Firma ma prawo do zatrzymania informacji poufnych, ale polityka otwartości zmniejsza ryzyko utraty wizerunku. Dlatego oświadczenia prasowe powinny być konsultowane z doradcami prawnymi i zarządem.

11. Kontakty z mediami

Obecność prezesa lub dyrektora i członków zarządu na konferencji prasowej podnosi jej rangę, sprawia wrażenie poważnego podejścia do problemu. Wykorzystywać należy bogaty pakiet instrumentów public relations. Warto też wyznaczyć stałe miejsce spotkań z dziennikarzami, wyposażone w niezbędny sprzęt biurowy. Niezbędne też mogą okazać się posiłki i napoje. Odpowiednie oznakowanie dróg, budynków i pomieszczeń usprawni poruszanie się po terenie przedsiębiorstwa.

Wprawdzie kontakty z dziennikarzami nie należą do codziennych obowiązków menedżerów, to coraz większa liczba firm zwraca uwagę na szkolenia medialne: treningi mowy ciała, wypowiadanie się i zachowywanie przed kamerą. Wartość szkoleń doceniają ci, którzy je

[11] K. Garski, *CRS Lek na całe zło?*,[w] „Manager” nr 1, 2009 r, s.63.

zlekceważyli po fatalnym wystąpieniu w mediach. Podstawowe wskazówki dotyczące zachowań w kontaktach z mediami w sytuacji kryzysowej można zawrzeć w kilku regułach:

- Przede wszystkim nie należy wpadać w panikę. Być opanowanym i uprzejmym w stosunku do dziennikarzy. Zapewnić ich, że dostaną więcej informacji.
- Trzeba zacząć działać: opanować informacje, zbierać wszelkie dane o sytuacji kryzysowej i związanych z nią wydarzeniach. Zapisywać je. Pozyskane informacje należy udostępniać tylko odpowiedzialnym przedstawicielom firmy.
- Warto słuchać mediów. Zapisywać wszelkie pytania od dziennikarzy i zapewnić, że dostaną na niewyczerpujące odpowiedzi oraz skontaktuje się z nimi rzecznik prasowy.
- Należy być dostępnym i nie chować się przed prasą. Media dostarczają informacje do największej liczby odbiorców w najszybszy sposób.
- Należy mówić prawdę, nawet, jeśli nie będzie można przedstawić jej całej.
- Nie wolno przedstawiać częściowych i niepełnych faktów. Informacje połowiczne mogą być niebezpieczne dla wizerunku firmy. Warto zachować dużą ostrożność przy przekazywaniu wiadomości do mediów. Nie udzielać informacji „poza kamerą" i w stylu *prywatnie sądzę, że... w zaufaniu powiem panu, że...*
- Przez cały czas należy okazywać troskę, być cierpliwym i przyjaznym. Jeżeli firma jest prezentowana w złym świetle, trzeba wykazywać zainteresowanie sytuacją.
- Najlepsze są oświadczenia pisemne, ale przygotowanie dobrego oświadczenia pisemnego wymaga czasu. Warto przygotować foldery firmowe, dane statystyczne na temat firmy oraz inne materiały prezentujące przedsiębiorstwo, łagodzące opinię mediów na temat firmy i pozwalające dziennikarzowi rozwinąć informację o przedsiębiorstwie.
- Trzeba prezentować pozytywy. Firma prawdopodobnie nie istniałaby, gdyby nie produkowała towarów, nie zapewniała usług potrzebnych otoczeniu firmy. Warto, aby dziennikarz dowiedział się, na czym polega działalność firmy i jakie korzyści ma z tego konsument.
- Należy zapewnić dobre warunki dla reporterów i dziennikarzy.

- Trzeba zadawać pytania! Pytać, jaką redakcję reprezentują, co zamierzają napisać, z kim rozmawiali na temat sytuacji kryzysowej, jakie informacje posiadają, w jaki sposób można kontaktować się z nimi w przyszłości.
- W przypadku złych wiadomości, należy wskazać, jak firma rozwiąże problem. Nie należy spekulować. Trzeba być uważnym, mówić prostym językiem, unikać słownictwa technicznego i slangu branżowego.

Zarządzanie sytuacją i komunikacją kryzysową nie kończy się wraz z opanowaniem problemu i publicznym ogłoszeniem tego faktu. W firmie odpowiedzialnej przed otoczeniem dokonana zostanie ocena działań strategicznych i bieżących, mających miejsce przed i w czasie sytuacji kryzysowej.[12] Pamiętajmy, że czwartą fazą w modelu Finka jest uczenie się. Kryzys powinien stać się bodźcem do zmian, usprawnienia i przebudowy przedsiębiorstwa: systemu zarządzania, pełnionych funkcji kierowniczych, systemu kontroli, systemu komunikacji z otoczeniem i kultury organizacyjnej.

Podsumowanie

Organizacje przygotowane na wszelkie problemy kryzysowe, uruchamiają potężny arsenał środków zarządzania sytuacją kryzysową. Równocześnie są bardziej świadome własnych ograniczeń i słabości. Tworzą rozbudowany system własnego wykrywania sygnałów ostrzegawczych, inwestują środki we wdrażanie mechanizmów umożliwiających szybki powrót do normalności i wykorzystują doświadczenia zdobyte w przeszłości.

Będąc systemami otwartymi kształtują strategię komunikacji, pozwalającą skutecznie oddziaływać na interesariuszy, uczestników kryzysu. Świadomość, że zbudowanie dobrej reputacji zajmuje lata, a zniszczenie jej – kilka dni, inspiruje do chronienia wizerunku poprzez aktywne *public relations* z wykorzystaniem technik systemu komunikacji kryzysowej. Warto też pamiętać, że w dobie kryzysu światowego, kiedy zagrożony jest każdy sektor i każde przedsiębiorstwo, szansą na przetrwanie i kluczowym czynnikiem sukcesu może okazać się

[12] T. Smektała, *Public relations w sytuacjach kryzysowych przedsiębiorstw*, wyd. Astrum, Wrocław 2001, s. 140-141.

efektywny system komunikacji społecznej budowania relacji z interesariuszami. System umożliwiający tworzenie wizerunku firmy odpowiedzialnej za społeczność i środowisko, w którym działa, rzetelnej i zasługującej na zaufanie.

Bibliografia

1. Black S., *Public relations*, Dom Wydawniczy ABC, Warszawa 2003
2. Clarke L., *Zarządzanie zmianą*, Wyd. Gebethner i S-ka, Warszawa 1997.
3. Fink S., *Crisis Management*, AMACOM, New York 1986.
4. Garski K. *CRS Lek ana całe zło?* [w],„Manager" nr 1, 2009 r
5. Mitrof I.J., Pearson C.M., *Zarządzanie sytuacją kryzysową*, Business Book, Warszawa 1998.
6. Rozwadowska B., *Public relations*, Wyd. Studio Semka, Warszawa 2002.
7. Scitel F.P., *Public relations*, Wyd. Felberg SJA, Warszawa 2003
8. Smektała T., *Public relations w sytuacjach kryzysowych*, Wyd. Astrum, Wrocław 2001.
9. Wawrzyniak B. (red.), *Zarządzanie w kryzysie, koncepcje, badania, propozycje*, Wyd. PWE, Warszawa 1985.

MANAGING COMMUNICATION IN CRISIS SITUATION

Summary

Managing the crisis situation and media communication are important factors of strategy planning for many companies. This article deals with the features and background favourable for the development of crisis situation. The causes and ways of responding to crisis as well as constructing anti-crisis strategy have been presented. The author concentrates on the tasks given to anti-crisis group members and the rules of communicating with the media.

Zdzisław Długosz [*]

LINIOWA METODA SKALOWANIA STANU BEZPIECZEŃSTWA INFORMACJI STANOWIĄCYCH TAJEMNICE PRZEDSIĘBIORSTWA W WARUNKACH KRYZYSU

Wstęp

Realizacja bezpieczeństwa w zakresie ochrony informacji stanowiących tajemnice przedsiębiorstwa z pewnością stanowi dynamiczne nim zarządzanie.

Przedstawiona przez autora opracowania propozycja skalowania bezpieczeństwa informacji chronionych osadzona została na uświadomionych celach przedsiębiorcy i wykorzystaniu wybranego rozwiązania, którego poprawność i skuteczność sprawdzono w 8 przedsiębiorstwach gdzie przeanalizowano 156 przypadków i symptomów ujawnienia informacji stanowiących tajemnicę przedsiębiorstwa rozumianych jako incydenty. Incydentem nazwano naruszenie bezpieczeństwa informacji, to jest każde naruszenie przepisów bezpieczeństwa i zjawiska zidentyfikowane w systemie i poza tym systemem mogące zagrozić lub doprowadzić do naruszenia poufności, integralności i/lub dostępności zasobów (otoczenie incydentów).

Dobór przedsiębiorstw do przeprowadzonych badań wynikał z ich reprezentatywności w danym rodzaju działalności prowadzonej na terenie kraju i Unii Europejskiej oraz z przemyślanej ze względu na cel działania ich struktury organizacyjnej zawierającej piony ochrony informacji stanowiących tajemnice przedsiębiorstwa. Ponadto wybór przedmiotu próby zakładał zróżnicowanie poziomu: świadczonych usług, produkcji i jej charakteru; ilości zatrudnionych; wypracowanej strategii konkurencji w warunkach kryzysu oraz doświadczenia w zakresie działań w walce z nieuczciwą konkurencją.

---

[*] Autor jest Dyrektorem Instytutu Badań nad Bezpieczeństwem.

Generalnie treść opracowania oraz zaprezentowana optyka pomiaru ukierunkowana jest na podniesienie bezpieczeństwa działań przedsiębiorstwa.

1. Bezpieczeństwo informacji stanowiących tajemnicę przedsiębiorstwa

Bezpieczeństwo firmy podczas kryzysu jest sytuacją, która w szerokim rozumieniu odznacza się brakiem ryzyka utraty tego, co dla niej jest najcenniejsze potencjału materialnego i intelektualnego oraz sprawności funkcjonowania. W kryzysie następuje utrata, lub zachwianie poczucia utraty rodzajowego bezpieczeństwa to jest wartości koniecznych do normalnego funkcjonowania firmy.[1]

Zagrożenia najczęściej odnoszone są do potencjalnego stanu rzeczy, a więc takiego, który może wystąpić, ujawnić się w określonych warunkach, najczęściej, gdy czegoś istotnego zaniechamy lub też powstałego w wyniku odpowiedniego działania celowego osób trzecich. Najgroźniejszymi postaciami zagrożeń będą te, które mogą prowadzić do zawłaszczenia lub wykorzystania w sposób nieuprawniony jej wartości materialnych i intelektualnych. [2]

Uchwalenie ustawy o zwalczaniu nieuczciwej konkurencji było przejawem dostosowania polskiego prawa do „Porozumienia w sprawie handlowych aspektów praw własności intelektualnej" (tzw. TRIPS - Agreement on Trade – Related Aspects of Intellectual Property (opublikowany w Dz. U. z 1996 r., Nr 32, poz. 143), będącego załącznikiem do Porozumienia Ustanawiającego Światową Organizację Handlu. TRIPS wyznacza wspólne standardy ochrony regulowanych w nim praw dotyczących własności intelektualnej.[3] Cytowana ustawa określa, że czynem nieuczciwej konkurencji jest działanie sprzeczne z prawem lub dobrymi obyczajami, które zagraża lub narusza interes przedsiębiorcy lub klienta (art. 3 ust. 1 ustawy).[4] Z treści art. 11 ust. 4 wynika, iż: „przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość

[1] Por. W. Tarczyński, M. Mojsiewicz, *Zarządzanie ryzykiem*. PWE. Warszawa 2001.
[2] D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002. s.143.
[3] Ustawa z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji*. (Dz. U. z 2003 Nr 153, poz. 1503 z póź. zm.).
[4] Zob. Wyrok S.apel.Ca 688/00 OSA 2001/5/28 w Katowicach z 2000.11.22.

gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności". Dokonując podsumowania tej części opracowania, jego autor wskazuje na to, że realizacja bezpieczeństwa w zakresie ochrony informacji stanowiących tajemnice przedsiębiorstwa stanowi zarządzanie nim poprzez zarządzanie podmiotową i przedmiotową strukturą. Tym samym pierwotnych przyczyn słabości systemu ochrony należy szukać w sposobie i jakości zarządzania. Praktyczne podjęcie niezbędnych i skutecznych czynności zapobiegawczych możliwe jest poprzez pomiar stanu bezpieczeństwa w odniesieniu do zidentyfikowanych i przeanalizowanych incydentów w elementach systemu ochrony tajemnicy przedsiębiorstwa. Jego składowe, ustalone w wyniku badań, stanowią: pracownicy przedsiębiorstwa i ochrona danych osobowych; bezpieczeństwo informatyczne; ochrona fizyczna; proces kontroli i szkolenia oraz analiza i zarządzanie ryzykiem.[5]

Rozważając model zagrożeń, zagrożeniem dla bezpieczeństwa systemu ochrony określać będziemy każde zjawisko (proces, zdarzenie) niepożądane z punktu widzenia niezakłóconego działania systemu, pewnego ustalonego porządku.[6] W wyniku przeprowadzonych analiz okazało się, że jednym z kluczowych pojęć dla kryterium podmiotowego systemu ochrony jest informacja. Jej dualistyczne pojmowanie wynikało z tego, że po pierwsze była ona przedmiotem ochrony, a po drugie narzędziem wykorzystywanym do ochrony. Jej pierwsza postać wynikała z istoty sprawnego zarządzania bezpieczeństwem w procesie decyzyjnym oraz stanowiła element rozpoznania oraz źródło prognoz i analiz. Informacja to też w procesie zarządzania wewnętrzne normy prawne przyporządkowujące kompetencje, opisujące standardy i normy sankcjonowane. Tym samym znaczenie pojęcia tajemnica przedsiębiorstwa **(Tp)** określone zostało poprzez związanie się (jako funkcja) z takimi kategoriami pojęciowymi jak: człowiek, informacja, uświadomiona celem ochrony informacji jej reglamentacja, zagrożenia i uświadomione doświadczeniem ryzyko jej ujawnienia, ochrona prawna oraz standardy ochrony.

$$\mathbf{Tp = f\ (pc, i, c, r, z, r,op, so)}$$

gdzie:

[5] Por. P. Sienkiewicz, *Teoria bezpieczeństwa systemów*, AON, Warszawa 2005.
[6] Por. J. Jaźwiński J, K. Ważyńska – Fiok, Bezpieczeństwo systemów. PWN, Warszawa 1993 r.

pc – postawy człowieka,
i – informacja,
r – ryzyko,
op – ochrona prawna,
so – standardy ochrony.

Ponadto okazało się, że bezpieczeństwo informacji stanowiących tajemnicę przedsiębiorstwa jest wprost proporcjonalne do ilości skutecznie zaplanowanych i skoordynowanych oraz wykonanych zamierzeń przeprowadzonych w celu zachowania: poufności, integralności i dostępności, a odwrotnie proporcjonalne do ilości przypadków ujawnienia i zagrożenia ujawnieniem. Tym samym:

$$\mathbf{Bi = P \cap I \cap D / n\,U\ \check{U}\ Z}$$

gdzie:

Bi – bezpieczeństwo informacji (T.P.),
P – zachowanie poufności,
I – zachowanie integralności,
D – zachowanie dostępności,
n – ilość zdarzeń,
U – ujawnienia danych,
Z – zagrożenia ujawnieniem.

2. Skalowanie stanu bezpieczeństwa informacji stanowiących tajemnice przedsiębiorstwa

Z przeprowadzonych badań wynika, że w praktyce niemożliwym jest poddanie się prostym algorytmom działań ochronnych uruchamianych czy też pobudzanych wiedzą intuicyjną, które zabezpieczałyby interesy przedsiębiorstwa w obszarze informacyjnym. Dlatego też w zakresie rozwiązywania problemów decyzyjnych opartych o skalowanie w opisywanym jego sposobie preferuje się zastosowanie wzorca opartego na badaniach operacyjnych.

Praktyczna realizacja propozycji zawartej w publikacji, stanowi element zespołu przedsięwzięć z dziedziny zarządzania w sytuacjach kryzysowych ukierunkowanych na podniesienie bezpieczeństwa działań przedsiębiorstwa poprzez opracowanie i wdrożenie systemowych rozwiązań organizacyjnych i ich szacowania na podstawie incydentów. W tej sytuacji założono jako podstawowe, kryterium ilościowe skalowania. Wykorzystanie wyznacznika ilościowego i jego wpływ na

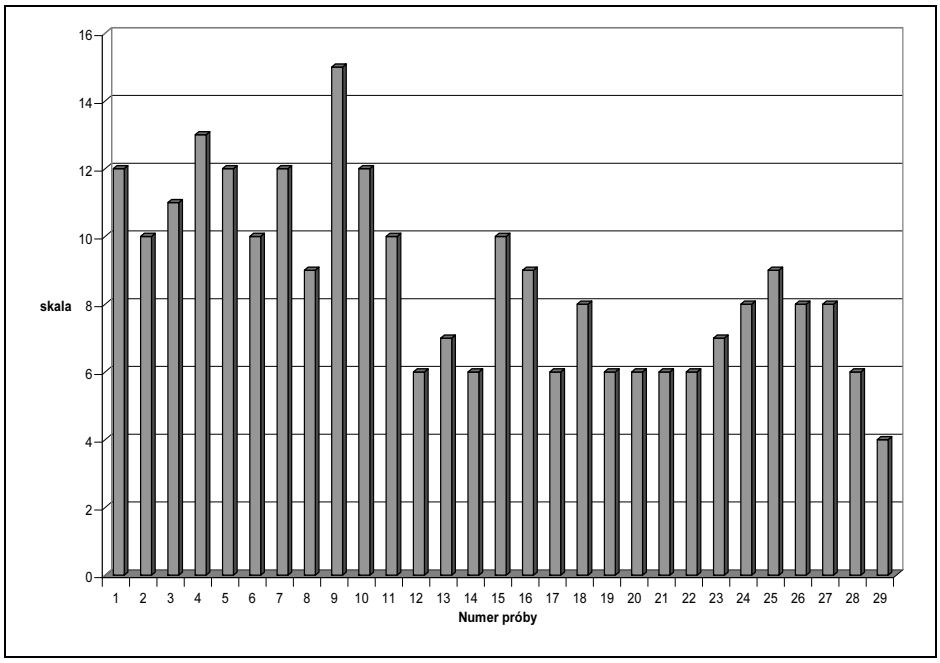
kształtowanie parametru jakościowego pozwoliło na określenie potencjalnych następstw spowodowanych naruszeniem poufności, integralności i dostępności oraz umożliwiło porównywanie wyników w tej samej skali. Miernik jakościowego skalowania to określona szkoda, niemożliwa do ostatecznego oszacowania w przypadku chociażby zagrożenia. Jakościowe skalowanie w każdym przypadku może mieć różne wartości uzależnione od potencjału związku przyczynowego ze skutkiem, którego zależności nie są możliwe do ostatecznego przewidzenia. Uzasadnienie tego wniosku wynika chociażby z tego, że badane reakcje zarządzających bezpieczeństwem na przypadki ujawnienia oraz zagrożenia w zależności od powstałej lub prawdopodobnej szkody było w każdym przypadku zróżnicowane przyjętą strategią rozwiązania problemu.

W odniesieniu do incydentów, w zakresie ich skalowania przyjęto następująca punktację U (ujawnienie) = 2 punkty oraz Z (zagrożenie) = 1 punkt. Uzasadnienie tak przyjętego sposobu skalowania wynika z tego, że najczęściej w pracach nad modelami stosuje się wszelkiego rodzaju badanie na podstawie przyporządkowania zmiennej niezależnej, zmiennej zależnej jako funkcji, w tym przypadku podstawowej, czyli liniowej o postaci ogólnej **y= ax+b.** Możliwość zbiegu incydentów powoduje, że owa suma jako wynik dodawania dwóch składników stanowi iloczyn ilości ujawnień i liczby dwa oraz iloczyn ilości zagrożeń i liczby jeden, co daje wynik skalowania. W tej sytuacji:

$$\mathbf{Ws= 2\ U + Z}$$

gdzie:
Ws – wynik skalowania (zmienna niezależna),
U – przypadek ujawnienia danych chronionych,
Z- zagrożenie ujawnienia danych chronionych.

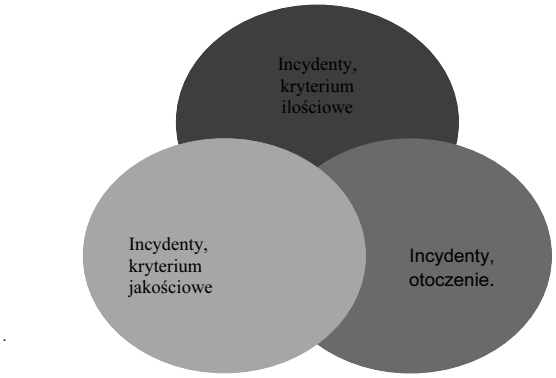
Prowadzenie procesu badawczego w oparciu o kryterium skalowania oraz ujęcie tego problemu w postaci wykresu jako funkcji wyniku skalowania i numeru próby umożliwia pogrupowanie incydentów w elementy systemu ochrony informacji niejawnych i ustalenia w ten sposób najsłabszego elementu tego systemu.



Rys. 1. Relacja wyników skalowania i numeru próby
Źródło: opracowanie własne.

Ponadto zarejestrowane podczas badań incydenty mogą wyczerpywać katalog możliwych niebezpieczeństw, których neutralizacja ma za cel uchronić przedsiębiorcę przed ujawnianiem informacji stanowiących tajemnicę jego przedsiębiorstwa. Jednakże niektóre z nich nie spełniają jednoznacznie przyjętego katalogu kryterium badań. Ich źródłowe wielorodzajowe skutkowo-przyczynowo pochodzenie powoduje, że ich identyfikację należy zakwalifikować do wspomnianego już ich otoczenia.

Tym samym wspomniane tutaj otoczenie incydentów występujące jako współczynnik incydentów (Woi), to jest chociażby kryzysy gospodarki światowej, katastrofy i kataklizmy, stanowić będą dla klasycznej postaci funkcji liniowej jej współczynnik „b" – (rzędna punktu, w którym prosta przecina oś rzędnych).



Rys. 2. Kryteria incydentów
Źródło: opracowanie własne.

W procesie badawczym, którego wynikiem była opracowana poniżej metoda skalowania, analizę ryzyka oparto na określeniu prawdopodobieństwa wystąpienia pewnych, przewidywalnych zagrożeń wykorzystujących podatność systemu i oszacowaniu ich wpływu na bezpieczną działalność przedsiębiorstwa. Na ich podstawie możliwe jest dokonanie wyboru środków ochrony, które pozwoliłyby zredukować zidentyfikowane ryzyka do poziomu możliwego do zaakceptowania. Ustalono też, że związek problemów ryzyka i zarządzania kryzysowego oznacza zarządzanie bezpieczeństwem poprzez konieczność dokonywania wyborów strategii działania w warunkach wysokiego poziomu ryzyka.

Generalnie zarządzanie ryzykiem podmiotu jest to podejmowanie decyzji i realizacja działań prowadzących do osiągnięcia przez ten podmiot akceptowalnego poziomu ryzyka.[7] W odniesieniu do zarządzania systemem bezpieczeństwa informacji stanowiących tajemnicę przedsiębiorstwa pojęcie ryzyko występuje w jego negatywnej koncepcji. Ryzyko rozumiane negatywnie (ryzyko jako zagrożenie)

[7] Por. A. Czermiński, M. Grzybowski, K. Ficoń, *Podstawy organizacji i zarządzania*, Wyższa Szkoła Administracji i Biznesu w Gdyni Gdynia 1999, s. 11-13.

oznacza możliwość nieosiągnięcia oczekiwanego celu. [8] W tej sytuacji: całkowite ryzyko w prowadzeniu działalności gospodarczej w warunkach kryzysu jest wprost proporcjonalne do ryzyka w zrozumieniu negatywnym, obojętnym lub w warunkach skłonności do ryzyka (zamierzone) i odwrotnie proporcjonalne do ryzyka w zrozumieniu neutralnym. Jak już wspomniano proces analizy ryzyka na pewnej przestrzeni czasowej oparto na określeniu prawdopodobieństwa wystąpienia pewnych, przewidywalnych zagrożeń wykorzystujących podatność systemu i oszacowaniu ich wpływu na działalność przedsiębiorstwa. To jest:

$$\mathbf{Ar= f}\,[P(Z + S)]$$

gdzie:
Ar – analiza ryzyka,
f – funkcja,
P – prawdopodobieństwo,
Z – zagrożenia i przypadki ujawnienia wynikające z podatności systemu,
S – prawdopodobna i oszacowana szkoda, straty mające wpływ na działalność przedsiębiorstwa.
Tym samym:

$$\mathbf{P(Z + S) = P(Z)+ P(S) – P\,(Z \cap S) = Pzs^{-1}}$$

W związku z powyższym wynik analizy ryzyka **Ar**, który jest prawdopodobieństwem zagrożenia i powstania szkód w systemie $\mathbf{Pzs^{-1}}$ jako ułamek właściwy stanowi w ujęciu funkcji liniowej współczynnik kierunkowy prostej, który jest równy tangensowi kąta jej nachylenia do osi zmiennej niezależnej.[9]
Przyjmując poziom bezpieczeństwa jako zmienną zależną (**Pb)** to dla postaci ogólnej funkcji liniowej (y=ax +b).

$$\mathbf{Pb= Pzs^{-1} \cdot Ws + (Woi)}$$ [10]

gdzie:

[8] K. Jajuga, *Zarządzanie ryzykiem*, PWN, Warszawa 2007, s.15.
[9] Prawdopodobieństwo rozumiane jako iloraz ilości zdarzeń sprzyjających zdarzeniu i ilości wszystkich zdarzeń. Jako ilość wszystkich zdarzeń ustalamy doświadczalnie dla kilku reprezentatywnych przedsiębiorstw. Ich liczebność w procesie przeprowadzonych badań wynosiła 30.
[10] **Woi –** współczynnik otoczenia incydentów obliczony jest analogicznie jak **Ws** – wynik skalowania.

Pb – poziom bezpieczeństwa systemu ochrony informacji T.P (zmienna zależna).
Pzs – prawdopodobieństwo zagrożenia i powstania szkód w systemie,
Ws – wynik skalowania (zmienna niezależna),
Woi – współczynnik otoczenia incydentów.

Nie ujęcie w kalkulacji wnikliwej oceny otoczenia incydentów powoduje, że poziom bezpieczeństwa systemu ochrony informacji stanowiących tajemnicę przedsiębiorstwa stanowi iloczyn prawdopodobieństwa zagrożenia i powstania szkód w systemie i wyniku skalowania.

$$\mathbf{Pb = Pzs^{-1} \cdot Ws}$$

Natomiast jego ujęcie, które wypełnia całkowicie postać funkcji liniowej sprowadza się do tego, że **Woi** określony w kategorii prawdopodobieństwa stanowi Pbs:

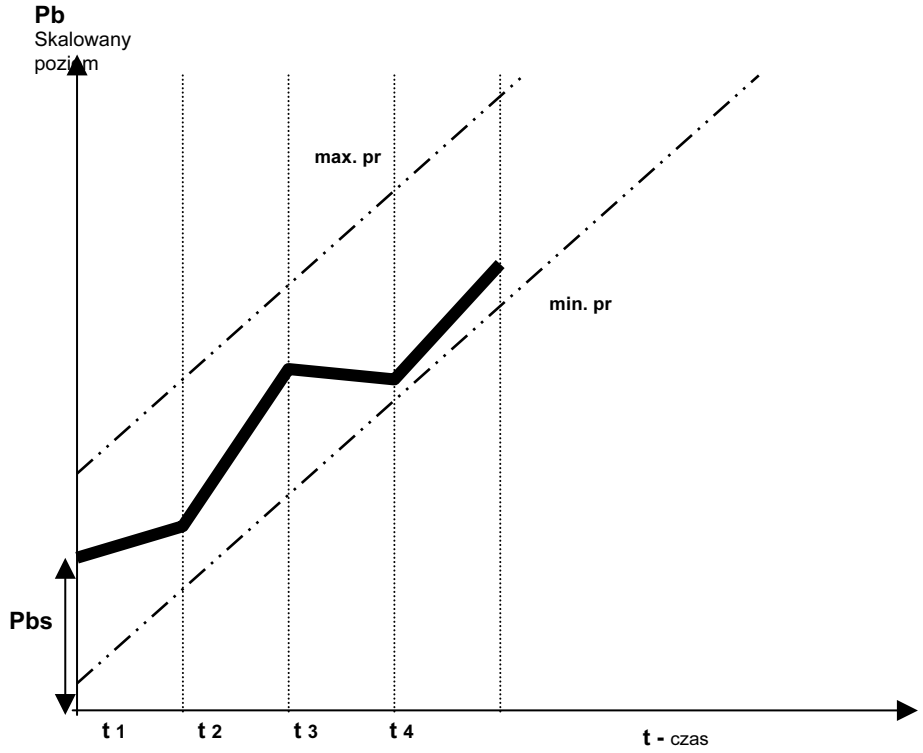
$$\mathbf{P}pb = \mathbf{P}zs \cdot \mathbf{Ws} + \mathbf{P}bs$$

gdzie:
PPb – prawdopodobieństwo poziomu bezpieczeństwa systemu ochrony informacji,
Pzs – prawdopodobieństwo zagrożenia i powstania szkód w systemie,
Ws – wynik skalowania,
Pbs – przyjęte jako stały w danym okresie prawdopodobieństwo poziomu bezpieczeństwa (otoczenie incydentów) obliczane na podstawie współczynnik otoczenia incydentów **(Woi).**.

Graficzne przedstawienie poziomu bezpieczeństwa (prosta) lub prawdopodobieństwa poziomu bezpieczeństwa, mierzone w określonych jednostkach czasowych daje możliwość badania w granicach założonego maksymalnego i minimalnego poziomu ryzyka w danym przedsiębiorstwie.

Takie ujęcie problemu umożliwia porównanie poziomu bezpieczeństwa w zarządzaniu systemem bezpieczeństwa informacji stanowiących tajemnicę przedsiębiorstwa w różnych podmiotach badań poprzez nałożenie na siebie pojedynczych wykresów. W wyniku takich zabiegów możliwe staje się wyselekcjonowanie firm o najwyższym i najniższym poziomie bezpieczeństwa, mimo że np. w firmie „A" o najwyższym poziomie bezpieczeństwa zagrożenie lub ustalone przypadki ujawnienia

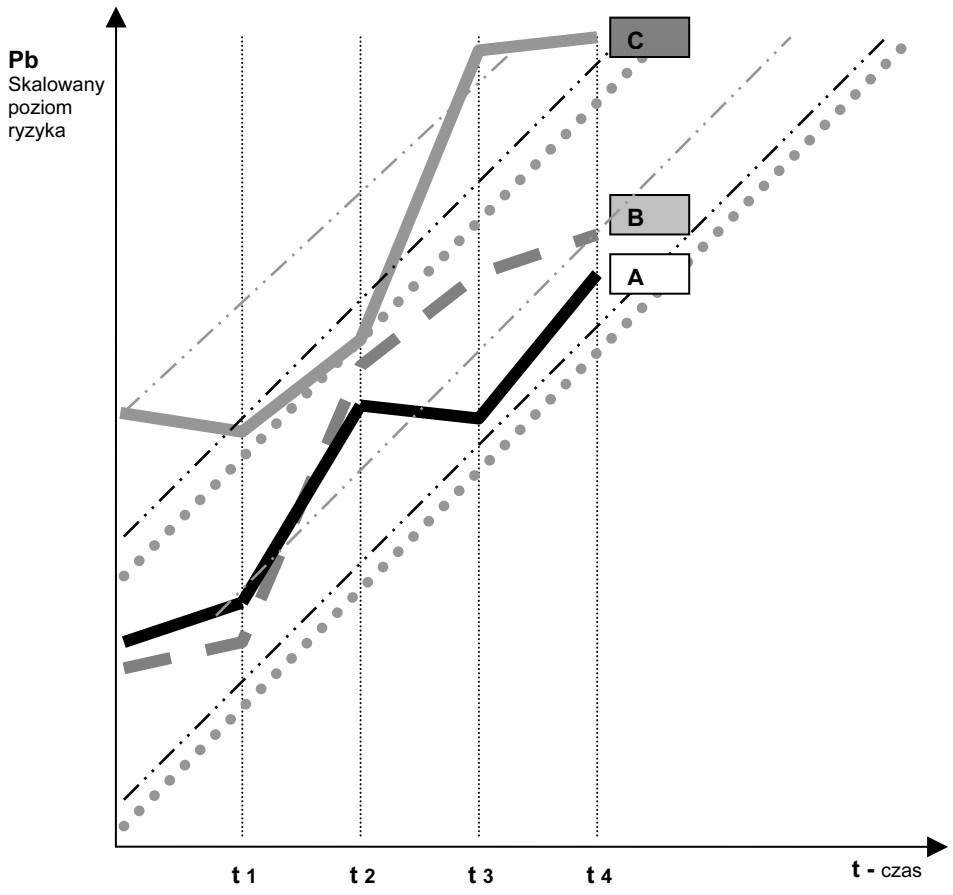
danych chronionych, zbliżają się do maksymalnego poziomu ryzyka, to w porównaniu z innym przedsiębiorstwem „B" owe usytuowanie na wykresie wskazuje na to, że przedsiębiorstwo „A" jest o wiele bezpieczniejsze niż „B". Przyjmując określony poziom granicy maksymalnego i minimalnego poziomu ryzyka w danym przedsiębiorstwie (poziomu bezpieczeństwa) należy owe przyjęcie jako świadomą i przemyślaną decyzją, na podstawie racjonalnych przesłanek wykorzystując rachunek prawdopodobieństwa, należy przyjąć jako równe 1. Tym samym proste na osi Pb będą nachylone do osi czasu (t) pod kątem 45˚ (tg ß = 1).



Rys. 3. Wykres badania poziomu bezpieczeństwa w oparciu parametr temporalny i skalowany poziom ryzyka w przedsiębiorstwie

Źródło: opracowanie własne.

gdzie:
Pb – poziom bezpieczeństwa systemu ochrony informacji T.P. skalowany poziomem ryzyka,
Pbs – przyjęty jako stały w danym okresie poziom bezpieczeństwa (otoczenie incydentów),
t – czas okres w którym prowadzono badania,
min. pr – minimalny poziom ryzyka,
max. pr – maksymalny poziom ryzyka.



Rys. 4. Wykres badania poziomu bezpieczeństwa w oparciu parametr temporalny i skalowany poziom ryzyka w przedsiębiorstwach A,B.C.

Źródło: opracowanie własne.

Wnioski

Czas przemian i transformacji, przełomów i radykalnych zwrotów sprzyja szansie na doskonalenie życia, ale również zwiększa możliwość działań destrukcyjnych. Z uwagi na zaostrzające się formy konkurencji i kryzys finansowy stanowić będzie coraz atrakcyjniejszą formę agresywnej polityki przedsiębiorstw i korporacji.

Przedstawiony w opracowaniu sposób skalowania stanu bezpieczeństwa informacji stanowiących tajemnice przedsiębiorstwa umożliwia sprawne zarządzanie systemem bezpieczeństwa w warunkach kryzysu.[11] Z przeprowadzonych badań w zakresie organizacji systemu ochrony informacji stanowiących tajemnicę przedsiębiorstwa wynika, że istotne znaczenie dla jego skuteczności należy przypisać osobie zarządzającej tym systemem.

Poprzez proces organizacji bezpieczeństwa należy rozumieć zbiór czynności obejmującym między innymi: zakres działania, czas na podjęcie i wykonanie systemu, koszty systemu i ryzyko. Natomiast kontrola realizacji przepisów i zasad obowiązujących w systemie ochrony zasobów jest podstawowym sposobem utrzymywania stanu akceptowanego ryzyka.

1. Generalnie proces analizy ryzyka służy określeniu, jakie ryzyko zagraża konkretnym zasobom oraz jaka jest ich wielkość. Proces ten polega na określeniu prawdopodobieństwa wystąpienia pewnych, przewidywalnych zagrożeń wykorzystujących podatność systemu i oszacowaniu ich wpływu na działalność przedsiębiorstwa. Prawdopodobieństwo to zależy także od atrakcyjności zasobów dla potencjalnych atakujących system ochrony. Wyniki analizy ryzyka i zaproponowanej metody skalowania pozwalają określić i dokonać

[11] T. Kotarbiński, Hasło dobrej roboty, Wiedza Powszechna, Warszawa 1975. Teoria zarządzania przejęła z prakseologii szereg zasad dobrej roboty, a w tym postulat działania sprawnego i ekonomicznego. Z tak ukształtowanym zarządzaniem bezpieczeństwem informacji stanowiących tajemnicę przedsiębiorstwa związane jest funkcjonowanie takich pojęć jak: minimalizacja interwencji (nie interweniować tam, gdzie procesy przebiegają sprawnie); potencjalizacja (osiąganie efektu przez samo ujawnienie możliwości działania); preparacja (przygotowanie zamierzonych czynności), symplifikację (uproszczenie podejmowanych działań); kooperacji pozytywna (współdziałanie) i kooperacja negatywnej (walki konkurencyjnej).

wyboru takich środków ochrony, które pozwolą zredukować zidentyfikowane ryzyka do poziomu możliwego do zaakceptowania. Powyższe uzasadnia tym samym kompetencyjny wybór struktury, dobór metod zarządzania, podział zadań i ich harmonizację. Osoba zarządzająca bezpieczeństwem powinna dysponować: określonym stanem możliwych zagrożeń i kryzysów, potencjałem odporności, kompetencyjne akty prawne, dobrane inne siły i środki ochrony, praktyczne umiejętności i doświadczenie własne oraz zespołów osobowych uczestniczących w przeciwdziałaniu zjawiskom niebezpiecznym.

2. Ponadto badania nad bezpieczeństwem systemów w sytuacjach kryzysowych należałoby rozwijać w kierunku tworzenia teoretycznych podstaw bezpieczeństwa systemów w ramach sekurologii oraz zarządzania ryzykiem w ramach inżynierii bezpieczeństwa (ze szczególnym uwzględnieniem sytuacji kryzysowych). Ponadto należy mieć na uwadze to, że proces ów nie jest i nigdy nie będzie procesem zamkniętym, albowiem postęp cywilizacyjny i związane z tym bezpieczeństwo w ujęciu systemowym wskazuje na związek bezpieczeństwa systemów z innymi cechami systemowymi takimi, jak stabilność, równowaga, niezawodność i trwałość.

Bibliografia

1. Apanowicz J., *Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania*, Wyd. WSA i B, Gdynia 2000.
2. Bertalanffy L, *Ogólna teoria systemów, Podstawy, rozwój, zastosowania*. PWN, Warszawa 1984.
3. Bizon-Górecka J., Monitoring *czynników ryzyka w przedsiębiorstwie*.; TNOiK, 1998.
4. Beck U, *Społeczeństwo Ryzyka*. Wydawnictwo Naukowe Scholar, Warszawa 2004.
5. Bogdalski P, *Tajemnica przedsiębiorstwa - zagadnienia konstrukcyjne*, „M. Prawn" 1997/6/228 - t. 2 i 5.
6. Carl L. Pritchard, *Zarządzanie ryzykiem w projektach, Teoria i praktyka*, WIG-PRESS, Warszawa 2002.
7. Czermiński A., Grzybowski M, K. Ficoń, *Podstawy organizacji i zarządzania*, Wyższa Szkoła Administracji i Biznesu w Gdyni

Gdynia 1999.
8. Denning. D., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
9. Durlik I., *Inżynieria zarządzania*, Wydawnictwo Placet, Warszawa 1996.
10. Grzybowski M., *Organizacja i zarządzanie*, AMW, Gdynia 1994.
11. Ihnatowicz I., *Człowiek, informacja, społeczeństwo*, Warszawa 1989.
12. Jajuga K., *Zarządzanie ryzykiem*, PWN, Warszawa 2007.
13. Jaźwiński J. K., Ważyńska – Fiok, *Bezpieczeństwo systemów*, PWN, Warszawa 1993.
14. Kaczmarek T., *Ryzyko i zarządzanie ryzykiem*, DIFIN, 2005.
15. Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Gliwice: Wydaw. Helion, 1999.
16. Konieczny J., *Zarządzanie w sytuacjach kryzysowych*, *wypadkach i katastrofach*, Poznań 2001.
17. Kotarbiński T., *Traktat o dobrej robocie,* Wrocław-Warszawa-Kraków, 1969.
18. Korzeniowski L., *Polityka bezpieczeństwa informacji w zrządzaniu firmą*, „Państwo i Społeczeństwo", 2003.
19. Korzeniowski L, Pepłoński A, *Wywiad gospodarczy, historia i współczesność*, *EAS*, Kraków 2005.
20. Łuczak M., *Ryzyko i kryzys w zarządzaniu przedsiębiorstwem*, WSE Warszawa, 2003.
21. Pipkin, D. L., *Bezpieczeństwo informacji*, Warszawa, Wydaw. Naukowo-Techniczne, 2002.
22. Porter M. E, *Strategia konkurencji*, PWE, Warszawa,1992.
23. Sienkiewicz P., *Zarządzanie bezpieczeństwem systemów*, Biuletyn WSAiB w Gdyni 2007.
24. Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.
25. Studenski R., *Ryzyko i ryzykowanie*, Katowice 2004.
26. Świniariki J, *O naturze bezpieczeństwa*, Warszawa 1997.
27. Tarczyński W, M. Mojsiewicz, *Zarządzanie ryzykiem*, PWE, Warszawa 2001.
28. Weber R.A., *Zasady zarządzania organizacjami*, PWE, Warszawa 1990.

ELABORATION WAY OF GRADUATION STATE OF INFORMATION SAFETY UNDERSTOOD A SECRET OF COMPANY ENABLE EFFECTIVE MANAGING OF SECURITY SYSTEM IN CIRCUMSTANCES OF CRISIS

Summary

Presented in elaboration way of graduation state of information safety understood as a secret of company enable effective managing of security system in circumstances of crisis. Results of risk study and proposed method of graduation let define and help to decide to choose way of security which let reduce identified risk to acceptable level. Main task became selection of structure an method of menaging.

Pavel Rosman*

SECURITY CONSIDERATIONS FOR VOICE-OVER IP TELEPHONY

Introduction

Voice over Internet Protocol, also called VoIP[1], IP Telephony, Internet or Broadband Telephony, Broadband Phone and Voice over Broadband, is the routing of voice conversations over the Internet or through any other IP-based network. VoIP, the transmission of voice over packet-switched IP networks, is one of the most important emerging trends in telecommunications. As with many new technologies, VOIP introduces both security risks and opportunities. VOIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but VOIP should not be installed without careful consideration of the security problems introduced.

1. Functionality

VoIP is the next generation telecommunications method. It allows to phone calls to be route over a data network thus saving money and offering increased features and productivity. However, the process is not that simple. Administrators may mistakenly assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks and remain secure. VOIP security considerations for the (PSTN[2]) are largely outside the scope of this document. All these benefits come at a price, vulnerability.

---

*Autor jest pracownikiem Tomas Bata University in Zlín.

[1] VOIP – Voice over IP.

[2] PSTN – Public Switched Telephone Network.

It is easier to attack and exploit a voice and data network. VoIP will need extra security measures beyond the standard security that is typically implement for a computer network. Many issues need to be addressed such as type of attacks, security, quality of service and VoIP protocols. VoIP can facilitate tasks that may be more difficult to achieve using traditional networks:

- Ability to transmit more than one telephone call down the same broadband-connected telephone line. This can make VoIP a simple way to add an extra telephone line to a home or office.
- Many VoIP packages include PSTN features that most Telco's (telecommunication companies) normally charge extra for, or may be unavailable from your local Telco, such as 3-way calling, call forwarding, automatic redial, and caller ID.
- VoIP can be secured with existing off-the-shelf protocols such as Secure Real-time_Transport Protocol. Most of the difficulties of creating a secure phone over traditional phone lines, like digitizing and digital transmission are already in place with VoIP. It is only necessary to encrypt and authenticate the existing data stream.

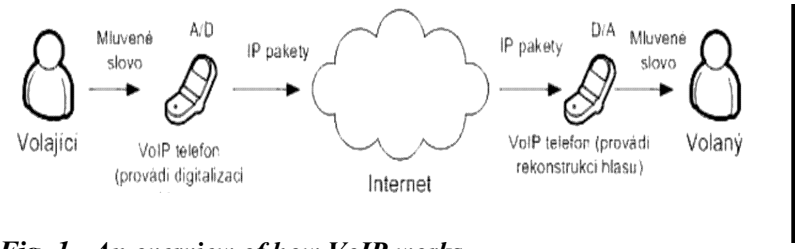


Fig. 1. An overview of how VoIP works

Companies providing VoIP service are commonly referred to as providers, and protocols which are used to carry voice signals over the IP network are commonly referred to as Voice over IP or VoIP protocols. There are two types of PSTN to VoIP services: DID[3] and *access numbers*. DID will connect the caller directly to the VoIP user while access number requires the caller to input the extension number of the VoIP user.

[3] DID – Direct Inward Dialling.

2. Reliability

Conventional phones are connected directly to telephone company phone lines, which in the event of a power failure are kept functioning by back-up generators or batteries located at the telephone exchange. However, household VoIP hardware uses broadband modems and other equipment powered by household electricity, which may be subject to outages in the absence of an uninterruptible power supply or generator. Early adopters of VoIP may also be users of other phone equipment, such as PBX and cordless phone bases, which rely on power not provided by the telephone company. Even with local power still available, the broadband carrier itself may experience outages as well. While the PSTN has been matured over decades and is typically extremely reliable, most broadband networks are less than 10 years old, and even the best are still subject to intermittent outages. Furthermore, consumer network technologies such as cable and DSL often are not subject to the same restoration service levels as the PSTN or business technologies.

3. VoIP Protocols

There are many VoIP protocols in the market. Some are proprietary while others are open standards. The *two most popular open protocols* are **H.323** and **SIP**. They both have problems with the use of random ports problems with NAT translations and firewalls. They were designed by two different organizations and operate slightly differently.

H.323 is an International Telecommunication Union standard for audio and video communication across a packet network (National Institute of Standards and Technology, 2005). H.323 is a complicated protocol and uses other protocols to perform other vital tasks. There are four types of devices under H.323: *Terminals, Gateways, Gatekeepers and Multi-Point Conference Units*. The terminals are phones and computers. Gateway provides an exit to other networks.

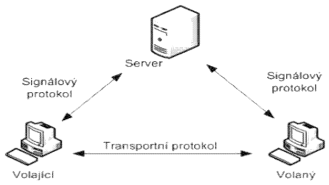


Fig. 2. Protocols of the VoIP

SIP[4] is a signaling protocol for

[4] SIP – Session Initiation Protocol.

Internet conferencing, telephony, presence, events notification, and instant messaging. SIP is an application layer protocol that uses TCP. The protocol is designed to work with servers and endpoints such as phones. The Internet Engineering Task Force developed this VoIP protocol. Another typical feature on a network is NAT[5]. NAT provides a method of changing private IP address in to public ones. It also allows for port translation. It is a method to conserve IP addresses and add another layer of security.

4. Security Vulnerabilities

A secure telephone is a telephone that provides voice security in the form of end-to-end encryption for the telephone call, and in some cases also the mutual authentication of the call parties, protecting them against a man in the middle attack. All Voice over IP traffic should be routed on separate VLAN6s than the data networks. This while make it harder to have both your data network and VoIP network compromised. Viruses will have a harder time infecting both sides of your network. It also makes it more difficult to sniff, intercept, or eavesdrop on traffic when it is divided up into separate VLANs. VoIP has many security vulnerabilities that need to be protected. Encryption, VLANs and Firewalls are a necessity on all networks that deploy VoIP. Also Network Address Translation should be avoided. These are a few important features that need to be addressed.

There are many different methods that VoIP can be attacked or exploited. Some attacks try to steal information while others attempt to shut down your network. The attacks include eavesdropping, spoofing, denial of service, call redirection, and replay attacks.

Encryption helps protect your privacy and authenticates the message. Transport Layer Security (TLS) and IPSec are the *two main encryption methods*. IP security is used to encrypt call setup and control messages. TLS is an alternative to IPSec and is based off the SSL protocol. It is used is used to provided a secure call setup. Many different algorithms can be used such as DES, 3DES, AES, RC4, and RC5. The simpler encryption results in better performance. It is an effective measure against eavesdropping and protects sensitive information.

[5] NAT – Network Address Translation.
[6] VLANs – Virtual LANs.

Eavesdropping is the unauthorized interception of voice packets and the decoding of the conversations. It is relatively easy and simple. There are many free network analyzer, snifters and packet capture tools that can convert VoIP traffic to wave files. This allows you to save the files and play them back on a computer.

Vomit (Voice over Misconfigurated Internet Telephones) is an example of such a tool. Typically eavesdropping is restricted to the subnet the phone is attached to and the path it takes to the destination. The National Security Agency (USA) is able to eavesdrop on all international calls coming into or out of the United States.

Replay attacks are used to gain more information about the source network. A packet is captured and retransmitted into the network to generate more traffic to be captured and analyzed. This allows for more information about the network. These attacks are often a prelude to other attacks such as man-in-the-middle and spoofing.

Packet spoofing uses a false source address on the IP packets. The network data such as a VoIP call will appear from a different often trust source than where it originated. This is also known as masquerading. Spoofing can change caller ID number, hide the origin of attacks, and pretend to be a trusted host. Several services available allow you to spoof your phone number.

Call redirection occurs when a call is intercepted and rerouted through a different path before reaching the destination. This could lead to eavesdropping, call fraud, and illegal use of your networks. If your network is compromised, the call could be redirected through the network to hide the source or to charge the phone calls to your company.

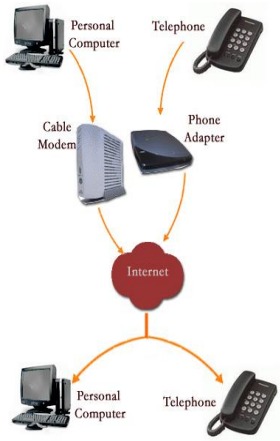


Fig. 3. *Communication - VoIP traffic*

Denial of Service is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. VoIP is more susceptible to DOS than a typical computer network. Not only does it suffer from the standard DoS attacks of flooding the network with traffic to the point it crashes but it

also has its our specific vulnerabilities. This causes the phones not being able to complete calls or hang up. With DoS there is a chance that both you data network goes down along side of your phone services provided through VoIP.

The many consumer VoIP solutions do not support encryption yet, although having a secure phone is much easier to implement with VoIP than traditional phone lines. As a result, it is relatively easy to eavesdrop on VoIP calls and even change their content. There are several open source solutions that facilitate sniffing of VoIP conversations. A modicum of security is afforded due to patented audio codec's that are not easily available for open source applications; however such security through obscurity has not proven effective in the long run in other fields. Some vendors also use compression to make eavesdropping more difficult. However, real security requires encryption and cryptographic authentication which are not widely available at a consumer level. The Voice VPN solution provides secure voice for enterprise VoIP networks by applying IPSec encryption to the digitized voice stream.

If you are considering using VoIP or digital phone service, please be aware of the following:

- VoIP *requires continuous power*. If you lose power, you will not be able to use any phone connected to VoIP.
- If you change your telephone number to take advantage of VoIP savings, it is important that you immediately advise Allied so we may update your account with accurate information.
- If the Allied alarm system has a line cut feature, it may NOT sound the alarm if the communication line on the outside of your premise is cut. The alarm panel checks the telephone line for voltage that is currently supplied by your telephone company. Certain characteristics of VoIP may lower the voltage and affect the security features of your alarm.
- Allied may lose the ability to download software changes to your alarm system (adding/deleting users, pass numbers, etc). A chargeable service call may be necessary to visit your premise to make these changes.
- Any changes or upgrades made to your VoIP service could impact the ability of the security system to transmit signals. You should always retest the system after any upgrades to your VoIP service.

- VoIP does not offer the same quality of service as direct telephony connections do. There are problems with connectivity, security, disability access, and emergency access.
- Many VoIP connections may not properly handle outgoing calls from fax machines, TiVo boxes, satellite television receivers, conventional modems or fax modems. These devices depend on conventional voice-grade telephone lines for some or all of their functionality.

5. Secure Your Wireless VoIP System

WiFi networks provide a tempting entry point for hackers and other unauthorized users. Many enterprises are discovering the cost and productivity benefits wireless VoIP provides. As a result, a growing number of enterprises are installing wireless hotspots inside office buildings, warehouses, shipping yards, corporate campuses and various other facilities, allowing employees with wireless IP handsets and other compatible devices to talk to each other, as well as the outside world, without relying on desktop phones. Yet wireless VoIP technology is not without risk.

Unsecured voice packets can be intercepted and WiFi networks provide a tempting entry point for hackers and other unauthorized users. Wireless VoIP security is always the network operator's responsibility, since mobile device users have no control over where their signals go. As with VoIP security in general, gaining control over wireless VoIP systems is challenging work. But careful planning and analysis will help ensure that your enterprise's VoIP traffic flows steadily and securely. Here are *five ways* to make that happen [1]:

1) *Look for Equipment*. That Incorporates Wireless Security Standards. The first wireless network security standard – Wired Equivalent Privacy (WEP) – was a rather weak and vulnerable technology. But newer specifications, such as WiFi Protected Access (WPA), WPA2 and IEEE 802.11i are powerful and security benchmarks. Make sure your network devices take full advantage of a least one of these technologies.
2) *Take Advantage of Encryption and Authentication*. WPA, WPA2 and IEEE 802.11i all offer built-in advanced encryption/authentication technologies that can help secure a wireless VoIP system.
3) *Use Multilevel Protection***.** Embed security within security. An IP

handset, for example, may send encrypted audio while IEEE 802.11ii authenticates and encrypts the wireless connection.

4) *Use a VoIP Firewall***.** A well-configured firewall will block hackers trying to enter an enterprise VoIP system through a wireless device. Firewalls are a standard security feature on networks. They protect the network from attacks by inspecting each packet that travels to and from the network. Firewalls have trouble filtering VoIP traffic due to dynamic port assignments through out the call.
5) *Provide Adequate Training*. Wireless VoIP users should be alerted to security threats and encouraged to report any unusual or suspicious activities they detect.

Conclusion

Security is a necessary part of any computer network. VoIP has many security vulnerabilities to attacks such as Spoofing, Eavesdropping, and Denial of Service etc. Encryption, Virtual LANs and Firewalls are a necessity on all networks that deploy VoIP. Also Network Address Translation should be avoided. These are a few important features that need to be addressed. Encryption helps protect your privacy and authenticates the message. VoIP needs to be protected beyond the standard measures. VLANs and Firewalls need to be configured to support VoIP traffic. Encryption should be used while NAT is avoided. All security measures needs to balance protect with quality of service of the network.

Bibliography and online sources

1. Edwards J. A., *Guide to Understanding the VoIP Security Threat* [online]. [cit. 2009-02-12]. Dostupné na WWW: < http://www.voip-news.com/feature/voip-security-threat-021407/>.
2. Piscitello D., Chraňte si svou síť VoIP. Whitepapers. In Computerworld – informační zdroj pro IT profesionály [online]. [cit. 2009-02-12]. Dostupné na WWW: <http://www.computerworld.cz/cw.nsf/id/technologie_chrante_si_svou_sit_voip/>.
3. Přibyl T., Technologie VoIP z hlediska bezpečnosti. In IT Systems, 2008, č. 10, s. 66-67. Brno: CCB, spol. s r.o. ISSN 1802-002X

4. RosmanP., ICT Security Incidents and Their Prevention. In *Information and Communication Technology in Education.* Rožnov p. R., 8th – 20th September 2008. Proceedings, s. 97-102. Ostrava: OSU Ostrava, Přírodovědecká fakulta. ISBN 978-80-7368-577-5.

Summary

This paper deals with problems of Internet telephony security. It also contains description of basic properties and characteristics of Voice over IP technology. The paper explains the challenges of VOIP security for agency and commercial users of VOIP, and outlines steps needed to help secure an organization's VOIP network. There are also categorized possible threats and attacks and included their short descriptions and specified basic requirements on safe and secure operation. Next part deals with tested attacks with respect to information the clients send to the Internet about their users. The last part of the papers is concluded with a list of selected implemented security mechanisms.

Roman Jašek*

HIGH FREQUENCY USED FOR IDENTIFICATION QUALIFYING OF SUBJECTS

Abstract

This contribution provides new view about to modern technology identification subjects, about use high frequency. Using KG Spectrum is possible eliminate the false alarm in another places.

Introduction

The Twenty-first Century is bringing with self a lot of possibilities, how we can secure our order. Knowing of this issue is gives a wide scale of researches, companies and individual people. It is an open task positively and secure insistence has changed over the past 5. years – people want to feel safely.

What is the main question of individual satisfaction? The reason is very simply: "less money, maximum of possession security"!

With this topic is relates a many researches for elimination of false alarm provided by Electronically Security Systems. In these papers or in lines bellow I will offer you a type of false alarm decreasing by Doppler signature performed.

It is describes change between frequency and wave length, the relationship between observed frequency f and emitted frequency f0 is given by:

$$f = \left(\frac{v + v_r}{v + v_s}\right) f_0$$

where:
v =is the velocity of waves in the medium
v_s = is the velocity of the source relative to the medium

* Autor jest pracownikiem Tomas Bata University in Zlín.

v_r = is the velocity of the receiver relative to the medium.

Both velocities vs and v rare computed so that the observed frequency is increased when either the source is moving towards the observer or the observer is moving towards the source. The frequency is decreased if either is moving away from the other. In the limit where the speed of the wave is much greater than the relative speed of the source and observer (this is often the case with electromagnetic waves, e.g. light), the relationship between observed frequency f and emitted frequency f0 is given by:

Observed frequency

$$f = \left(1 - \frac{v_{s,r}}{c}\right) f_0$$

Change in frequency

$$\Delta f = -\frac{v_{s,r}}{c} f_0 = -\frac{v_{s,r}}{\lambda_0}$$

where
$v_{s,r} = v_s - v_r$ is the velocity of the source relative to the receiver : it is negative when the source is moving towards the receiver, positive when moving away
c = is the speed of wave (e.g. 3×108 m/s for electromagnetic waves traveling in a vacuum)
λ_o = is the wavelength of the transmitted wave in the reference frame of the source.

If the source moving away from the observer is emitting waves through a medium with an actual frequency f0, then an observer stationary relative to the medium detects waves with a frequency f given by

$$f = \left(\frac{v}{v + v_s}\right) f_0$$

where v_s is positive if the source is moving away from the observer, and negative if the source is moving towards the observer.

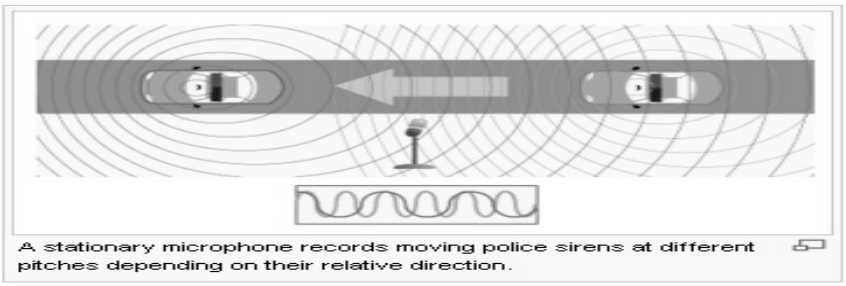


Fig. 1. Basic principle of Doppler Effect

1. KG spectrum

The KG spectrum – is a mono-static microwave radar, Millimeter Wave Surveillance Radar Sensors.

Fig. 2. Millimeter Wave Surveillance Radar Sensors.

Specifications

Spectrum Model	SR-3030	SR-4505	SR-0303
Application	General area surveillance	Invisible wall or ceiling	Pencil Beam
3dB Beam Width (Elevation x Azimuth)	30 x 30 degrees	45 x 5 degrees	3 x 3 degrees
Width of Field at maximum range	56 meters	36 meters	34 meters
Range *	100 meters (330 ft)	400 meters (1300 ft)	600 meters (2000 ft)
Range Bin	3 meters (10 ft)		
Operating Frequency	24.125 GHz (K Band)		
Modulation	Direct Sequence Spread Spectrum (DSSS)		
ERP	<250 mV/m at 3 meters (10 ft)		
MTBF	100,000 hours		
Communications	RS-485, RS-232 or Ethernet (TCP/IP)		
Alarm Output (optional)	Form-C Relay, serial port or GIS coordinates		
Power	12 to 24 VDC, 5 W		
Ambient Operating Temperature	-40 to 70 degrees Celsius		
Dimensions (W x H x D)	12.7 dia x 15.2 cm	7.6 dia x 25.4 cm	33 dia x 25.4 cm

Fig. 3. Specifications of KG Spectrum.

2. Elimination of false alarm by Doppler Effect performed

Outdoors sensors that covering of area are often identified to a wide field, with detection from 90 to 360˚. Due to this is more likely arise of false alarms, because wrong evaluation of sensors. False alarm is statement of Electronically Security System that wrong evaluates a situation about an intruder.
Like an intruder we can differentiate:

- a biped intruder;
- a quadruped intruder.

For the elimination of claimed status was provided a lot of researches of sufficient detection response. Knowing of the millimeter wave Doppler radar is possible to presents a wide range, when radars are deployed such that an intruder can be observed over a time period exceeding 10 seconds. Nevertheless KG Spectrum decided to exploit the analysis of human Doppler signature. Millimeter wave Doppler radar provides the capability to measure displacement with resolution as precise as +/- 1mm.

3. The hypothesis:

Fixed-beam radar, used to secure a perimeter – the beam is normally aimed along the secured perimeter. According to this is more likely that an intruder go to cross the radar beam at 90˚.Fact - the radar beam angle is normally oriented such that its narrow angle is on the horizontal plane and its wide angle is on the vertical plane. This type of radar is often called PIDS (PIDS=Perimeter Intrusion Detection System). Disadvantage – the intruder within the detection beam for a short time of period, that lead to difficulty applying of signal processing (alarm condition must be reported cca. ½ second).

A fixed –beam radar, used to secure a perimeter – the beam is normally aimed at the secure area. According to this is more likely that an intruder walking either toward or away from the radar.

Fact – the radar beam angle is normally oriented such that its narrow angle is on the vertical plane and it wide angle in on the horizontal plane. This type of radar is often called Ground Based Radar or Surveillance Radar.

Let me summarized that PIDS, Ground Based Radars are able to dwell on the intruder. On the basic of this is most likely moving of intruder from zone to zone which allows even longer processing time.

4. Multiple Fixed Radars for Wide 360˚ Area Coverage

This Multiple Fixed Radars opens a new type detection identified of intruder. We talk about a new technology; called Direction Finding Receiver used in electronic warfare as it is able provides 100% coverage with more probability of interception.

According to the next two Figures, the numerator can understand the main principle of function with direct oriented to the Multiple Fixed Radars. On the Figure 4 bellow, is the coverage 360˚, by using 4 fixed beam radars aimed at 90˚ from each other.

The potential intruder at position X generates a response on the West antenna of -8 dB (2x – 4dB). The same principle of intruder X is on the North antenna, provided by -18 Db (2X – 9dB). The signed differential is -8 – (-18)= +10dB. The result of this is unique and corresponds to a bearing angle pointing to -50˚. At the same time this technique can be used to calculate bearing angles with +/- 10˚.

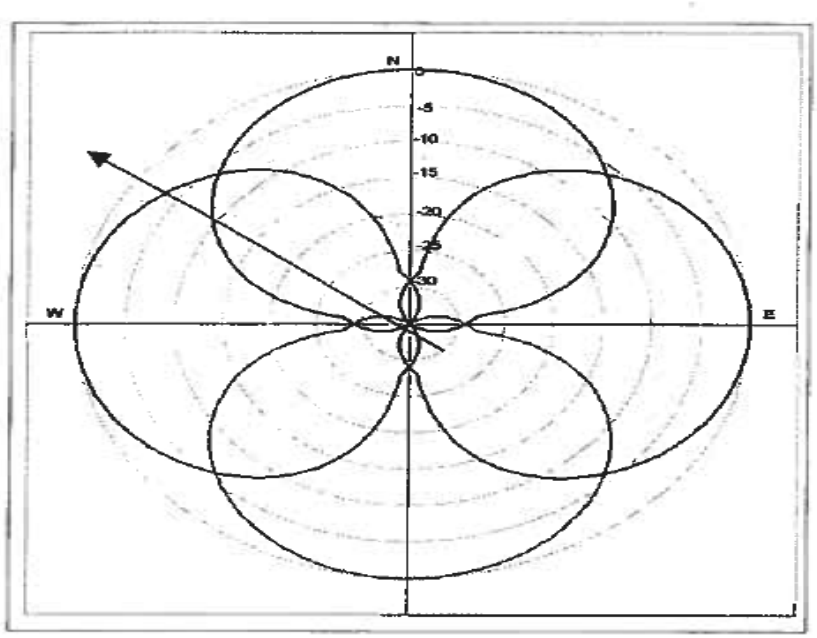


Fig. 4. The model for 4 antennas with 90˚ beam widths.

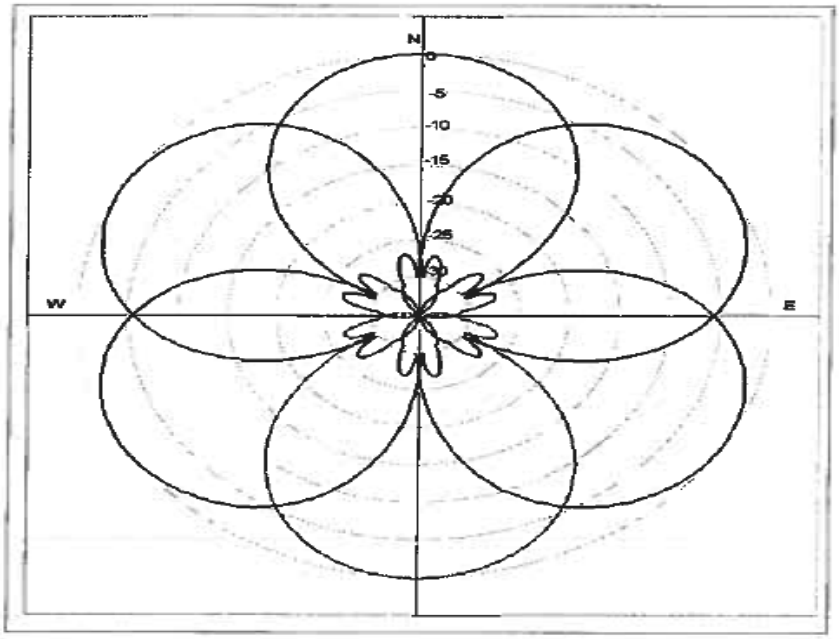


Fig. 5. The model for 6 antennas with 45˚ beam widths.

5. Biped signature or Human signature for elimination of false alarms.

According to the premise that a biped presents a significantly different Doppler signature in comparison with a quadruped Doppler signature, it may be used for detection of humans or animals attendance.

It was noted a few of human activities (in using of legs) with direction to the speed. There are:

- Walk on stret is 4.5 – 5.5 km/h;
- Exercise walk is 5 – 6.5 km/h;
- Human in a rush can walk up to 7.5 km/h;
- Easy jogging is 7.5 km/h;
- Normal running is up to 10 km/h;
- Medium running is 11 – 13 km/h;
- Ordinary human fast running is 12 – 16 km/h;
- Trained human fast running is 15 – 20.5 km/h;
- Ordinary human sprint running is 23 km/h;
- Trained human sprint running is 24 – 31 km/h.

6. The speed to Doppler frequency in version of radar equation:

$$f = \frac{2xVxF}{c}$$

F=24.125 GHz
V= velocity of activities
C= is the speed of wave (e.g. 3×108 m/s for electromagnetic waves traveling in a vacuum)
Doppler (Hz) = 44,6759 Hz/ km/h
Doppler (Hz) = 160,833 Hz/ m/sec.

Next notes are dedicated to the speed of the arms and legs as a function of the total body motion speed.

- The periodic swing of the arm at wrist-hand radius is 2 to 3 times higher than the speed of the total forward body motion.
- The periodic swing of the leg at foot radius is 2.5 to 4 times higher in speed than the total body motion forward.
- The periodic swing of the arm at wrist-hand radius is 0 to 2 times slower speed than the total body motion forward.

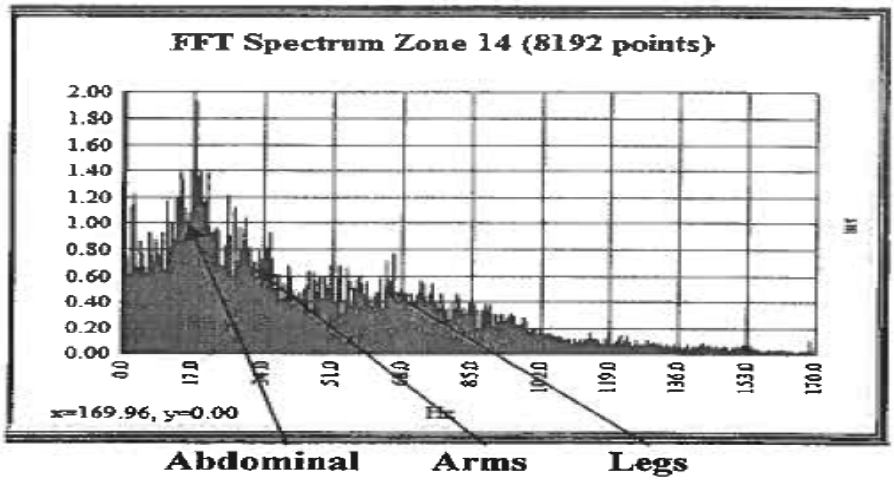


Fig. 6. View of the FFT (Fast Fourier Transform = algorithm to compute the discrete Fourier transform): Arm to Abdominal frequency ratio of 2 to 1 and the legs to Abdominal frequency ration of 4 to 1

Summary

In summary, using by KG Spectrum is possible to eliminate the false alarms. In this papers was successful demonstrate the differences between human form from a wide range of nuisance alarms.

Sources

1. Gagnon A., *Recent Developments in Ground Based MillimeterWave Radars*. Technical Note 3-2 Using Multiple Fixed Beam Radars for Wide Area Coverate. K&G Spectrum publication, 2007, revised in 2008.
2. On line sources on the net.

Andras Chernel*

COGENT ARGUMENTS FOR USING MOODLE AS AN LMS TOOL TO DELIVER SECURITY RELATED COURSES

Introduction

The European Union, in the Sixth, and Seventh Framework Agreements, have demonstrated their emminent interest and support for innovation in the education process and in increasing access to education through the exploitation of modern learning tools and their integration and implementation in the educational process at both the formal and informal levels – whether at the tertiary (e.g. Building Virtual Universities), secondary or primary levels as well as the general community level.

In Building a Virtual Learning and Teaching Community in the Czech Republic and in Europe[1], (Zimola B., Chernel A., Hán J., Poulová P.) said: "From European and non-European experience, the effectiveness and quality of higher educational institution study programmes using distance learning supported by eLearning elements is greater where this is implemented within a network of universities – i.e. a virtual university in the organisational sense."

So, let us begin with a brief overview of the challenges facing not only higher educational institutions but Distance Learning at the present time, as well as briefly looking at the roles of technology in the process and the benefits to be derived from their use in the educational process.

We can safely say that the challenges for modern education in Europe today are the whats, wheres, hows, and whys of providing Lifelong learning since – especially at a time of economic uncertainty, the European Union is faced by a range of uncertainities and issues – each of which presents risks as well as opportunities – for instance, we can mention that the advent of the Knowledge and Creative Societies and the Information Age have meant that new paradigms are needed to address the need for new jobs and skills, or demands for higher education due to population growth, or globalisation, or greater diversity and fragmentation in the labour market.

* Autor jest pracownikiem Tomas Bata University in Zlin.

[1] Zimola B., Chernel A., Hán J., Poulová P., 2006. In: Proceedings of The 4th International Conference on Education and Information Systems, Volume II, Orlando, United States, pp.77-81.

Distance learning today is faced by the following tension – there is often a lack of interaction between instructors and learners, leading to the need to increase such interaction. Teaching should be oriented on aiding learners to achieve mastery of the content and concepts of the educational process. Thus, learning should be:

- Student-focused,
- Activity-driven,
- Support all forms of feedback.

What then is the role to be played by Information Technology in this process? Some of the key roles of technology are:

- To provide creative solutions,
- To provide greater and easier accessibility to learners – 24 hours a day, 7 days a week, and 365 days a year (i.e. anytime, anywhere),
- To facilitate increased interaction between the key players (i.e. learners and teachers).

What benefits do virtual learning environments and tools provide? The core benefits are:

- Virtual classrooms have no walls, no boundaries, no frontiers
- Students learn in different locales, time zones and at different rates
- Knowledge is shared and cross-disseminated between all those involved (i.e. pedagogues-students, pedagogues-pedagogues, students-students)
- Interaction is in an authentic context in real time, on-line contexts (whether sychronomous or asynchronomous)
- On-line activities promote students' active engagement and involvement
- Learner autonomy is promoted while minimising the teacher's role
- Reduction of administrative costs (travel, telecommunications, photocopying, etc.)
- Collaboration is encouraged and supported between institutions and campuses
- There are clearly identifiable increases in students' course enrolment
- Improved time management
- Virtual collaborative relationships and friendships can be made

Virtual Learning Environments (VLEs) are sometimes referred to as LMS (Learning Management Systems) or CMS (Course Management Systems) and are web-based platforms like Moodle that support the delivery, administration and management of online educational courses.

VLEs are bundles of "communications applications" (e.g. e-mail, chat boards, etc.) that provide 24-hour access to and help to disseminate information, and course administration tools. They also facilitate

the setting and collating of assignments as well as allowing students to be automatically tested and graded using online or interactive quizzes, etc.

They are in essence empty until materials – usually provided by teachers and customised to meet the needs of a specific course, are created. These materials can be uploaded as Word or Adobe documents and PowerPoint presentations, online quizzes, or imported streamed video or audio files (e.g. using YouTube or other providers). Some institutions may also choose to buy "off-the-peg" or "tailor-made" publisher-created digital content. Nowadays, VLEs are used by universities who employ learning technologists to deal with technical issues like uploading materials. Blackboard and Moodle are two of the best-known VLEs, both commonly used in universities.[2]

For a comparison between Moodle and Blackboard see:
http://www.humboldt.edu/~jdv1/moodle/all.htm [3]

Moodle is a course management system (CMS) that aims to help educators create effective online learning communities, with a great emphasis on the concept of 'community'[4].

WikiEducator[5] is a website that provides free eLearning content that anyone can edit and use, launched by COL and piloted in August 2006 at the first course developers meeting for the Virtual University for Small States of the Commonwealth (VUSSC). It is now being used around the world extensively for the development of free educational resources. It is an evolving community focussed on collaboration in:

- Planning educational projects linked with the development of free content
- Development of free content on WikiEducator for eLearning
- Building open education resources (OERs) on how to create OERs
- Networking on funding proposals developed as free content

[2] P. Sharma, B. Barrett, *Blended Learning: using technology in and beyond the language classroom.*

[3] Blackboard vs. Moodle, A *Comparison of Satisfaction with Online Teaching and Learning Tools*, Bert Bos.
Kathy D. Munoz, Professor, Humboldt State University, Joan Van Duzer, Instructional Technologist, Humboldt State University15 February 2005.

[4] P. Sharma, B. Barrett, Blended Learning: using technology in and beyond the language classroom.

[5] www.WikiEducator.org.

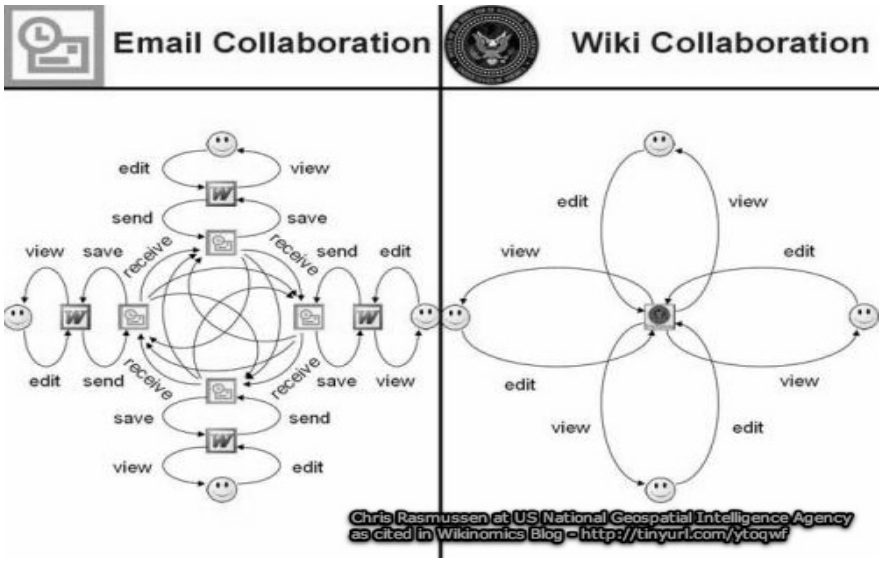


Fig. 1. Comparison of email and Wiki collaboration[6]

Web 1.0 is today taken to mean knowledge-sharing resources mainly within peer groups that were essentially passive in nature – i.e. you could create them using classic word and data-processing packages (e.g. Word, PowerPoint, email, etc.), and someone else could read them. The knowledge and information remained restricted. The first websites tended to provide information about a company and its products but were weak in allowing direct communication between users/clients and the company.

Web 2.0 is where we and technology are today – where data collection and data sharing are enhanced by other media – i.e. audio and video – and where we can use blogs, chat boards, email, wikis and streamed media to enliven content and communications. For educators and their students, it can strengthen the learning and communication processes.

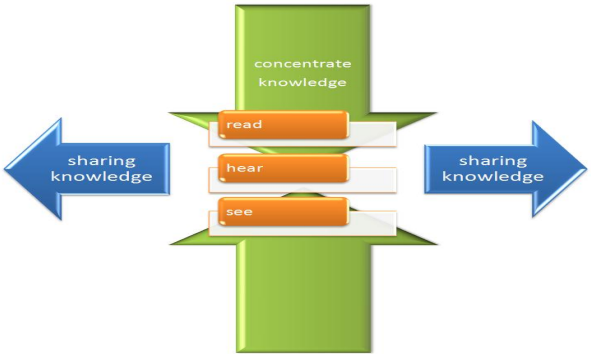


Fig. 2. The current generation Web (Web 2.0)

[6] C. Rasmussen, US National Geospatial Intelligence Agency – http://tinyurl.com/ytoqwf.

Web 3.0 is the posited web in the near future, in which data, information and knowledge-sharing and storage are much easier and more efficient. According to the schema below, provided by Radar Networks[7], 2007, (Fig. 3), 2010 should see the introduction of the 3rd generation of the Web (Web 3.0), which will be able to work with semantics and xml indexing.

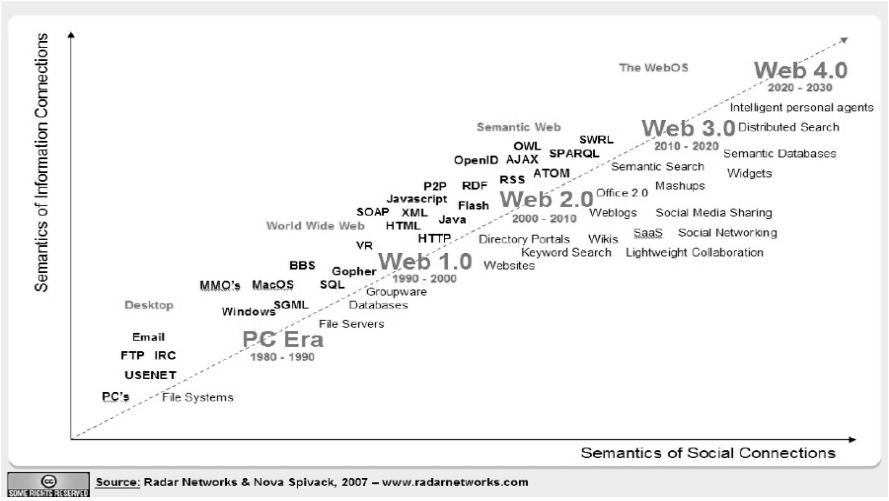


Fig. 3. The evolution of the Web

According to Tim Bernes-Lee, "the semantic web is the enlargement of the current web, whose data is allocated a specific meaning thanks to which people and software will be able to cooperate."

1. Collaborative Learning

More than one-third of the world's population is under 20. There are over 30 million people today qualified to enter a university who have no place to go. During the next decade, this 30 million will grow to 100 million. To meet this staggering demand, a major university needs to be created each week. — Sir John Daniel, 1996 [8]

The latest evolution of the Internet, the so-called Web 2.0, has blurred the line between producers and consumers of content and has shifted attention from access to information toward access to other people.

New kinds of online resources — such as social networking sites like Facebook or Second Life or MySpace or blogs, wikis, and other virtual communities — have allowed people with common interests to meet, share ideas, and collaborate in innovative ways. Indeed, the Web 2.0 is

[7] Radar Networks, http://novaspivack.typepad.com/nova_spivacks_weblog/radar_networks/

[8] J. S. Brown, R. P. Adler: Open Education, the Long Tail, and Learning 2.0, *EDUCAUSE Review,* vol. 43, no. 1 (January/February 2008): 16–32

creating a new kind of participatory medium that is ideal for supporting multiple modes of learning.[9]

2. Social Learning

The most profound impact of the Internet, an impact that has yet to be fully realized, is its ability to support and expand the various aspects of social learning … the simplest way to explain this concept is to note that social learning is based on the premise that our *understanding* of content is socially constructed through conversations about that content and through grounded interactions, especially with others, around problems or actions. The focus is not so much on *what* we are learning but on *how* we are learning. [10]

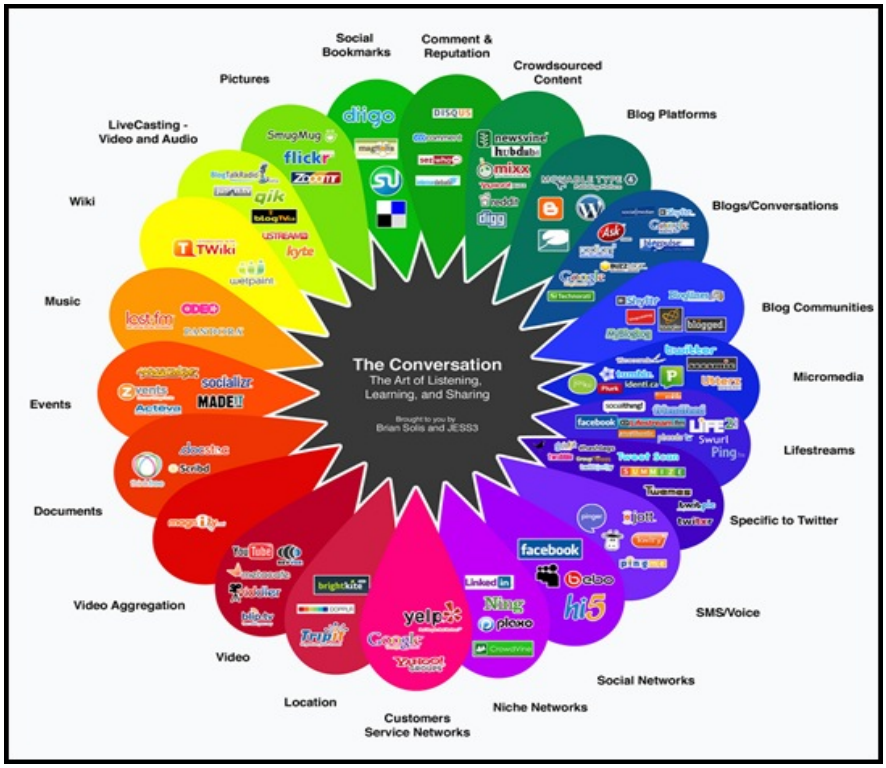


Fig. 4. The Art of Listening, Learning and Sharing – Types of Collaboration Tools

3. Learning to Be

There is a second, perhaps even more significant, aspect of social learning. Mastering a field of knowledge involves not only "learning about" the subject matter but also "learning to be" a full participant in the

[9] J. S. Brown, R. P. Adler: Open Education, the Long Tail, and Learning 2.0, *EDUCAUSE Review,* vol. 43, no. 1 (January/February 2008): 16–32.
[10] Ibidem

field. This involves acquiring the practices and the norms of established practitioners in that field or acculturating into a community of practice traditionally begin learning by taking on simple tasks, under the watchful eye of a master, through a process that has been described as "legitimate peripheral participation"; they then progress to more demanding tasks as their skills improve.[11]

4. Experience with using MOODLE

Moodle was launched in June 2003. Currently (02.04.2009) there are 52,539 sites from 207 countries who have registered. 9,735 of these have requested privacy and are not shown in the lists below. [12]

At the Department of Modern Languages (now the Department of English and American Studies), TBU in Zlin, we first heard about it from Ing. Tom Dulík – then of FT, TBU in Zlin and now of FAI, TBU in Zlin, a colleague of ours in early 2005 and immediately downloaded and implemented the LMS, registering it as the 13th site in the Czech Republic at the time. The site has just been upgraded to the latest version 1.9 and intergated into a newly created platform: http://vyuka.fhs.utb.cz/[13]. Course materials will have to be adapted over the coming summer break to work in the much faster and better environment.

To begin with, the site was used to offer paid courses to students and some information or additional information and support materials that could not be included in the official syllabii about certain courses.

In the autumn of 2006, it was used to provide study support materials to the English element of FaME`s Combined/Distance Learning programme with over 450 registered students. They had an allocation of 10 teaching hours per semester as compared to 56 hours for full-time students; and until then, there had been a lack of a way to provide readily accessible supporting study materials. Student numbers were increasing exponentially to match the increase in size of the university as a whole as well as the faculty itself.

The first decision was to ensure that over time, materials were scanned and added to the site for students to download and use in their studies – http://uni.utb.cz/moodle/ – see top right corner – Resource Links: GRAMMAR – "Grammar Resource Pack"; River of Time (PERFECTs); Tense Review ; EuroPass ; NIBE Pocket Guide; EURTIB Dictionaries . All of this was completed within the first two months of the semester.

[11] J. S. Brown, R. P. Adler: Open Education, the Long Tail, and Learning 2.0, *EDUCAUSE Review,* vol. 43, no. 1 (January/February 2008): 16–32.
[12] http://moodle.org/sites/ .
[13] http://vyuka.fhs.utb.cz/ .

The second problem was that students did not know how they had done in the end-of-semester exams for approximately 3 weeks after taking the test – since it took that long to manually mark all of the tests – and student numbers were constantly continuing to grow. It was therefore decided to try to exploit the built-in testing (Quiz) mechanism in MOODLE. The working hypotheses were inspired and adapted from the article, "Students Attitudes Towards Innovative Computer-Related Assignments: The Experiences of a Graduate Level Class", B. J. Neubauer, N. Krzychi, ©1998, The American Political Science Association.[14]

These adapted working hypotheses were as follows:

1. Electronic testing would be much faster (preferably instantaneous).
2. There would be no differentiation between genders through using electronic media for the testing process itself.
3. Potential gender and other discrimination and the subjectivity of results would be eliminated or suppressed to more acceptable levels.

Hypothesis I – Providing everything works perfectly; a test can be marked in under a minute.

Hypothesis II – So far, there is no proof that women have greater problems than men in using electronic media – indeed they have a certain advantage. Most of us nowadays have some to good computer skills. Men tend to be somewhat less careful in their typing skills.

Hypothesis III – Computers are asexual and unbiased; they mark impartialy. The creators of tests need to endeavour to balance gender, race, religion, and other issues.

Experience showed that the formulation of certain types of questions or quiz formats needs special care – for instance, complicated written assignments are totally unsuitable for language testing. Students reacted positively to the introduction of electronic testing – only 3 or 4 out of over 1095 students who have made more than 1564 attempts in two and a half years (5 semesters) have requested a written test/exam. They have also been incredibly patient and tolerant of inital problems associated with the creation and administering of such exams.

What helped enormously was the policy of checking the tests immediately afterwards before their eyes and the regrading and inclusion of students` errors into the standard data-base. As the data-base has

[14] "Students Attitudes Towards Innovative Computer-Related Assignments: The Experiences of a Graduate Level Class", B. J. Neubauer, N. Krzychi, ©1998, The American Political Science Association.

become more expansive (and "tolerant" of previously-encountered errors) it has also become more refined.

A new initiative in the 2008/09 academic year that has been greatly appreciated especially by Combined Studies students who have only 10 hours of f-2-f tuition (face-to-face) per semester as comparison to 42 hours for full-time students, and who all have to prepare for the same end-of-semester exams, is the creation of what are called (in "Moodle-speak") "Sandbox" Tests.

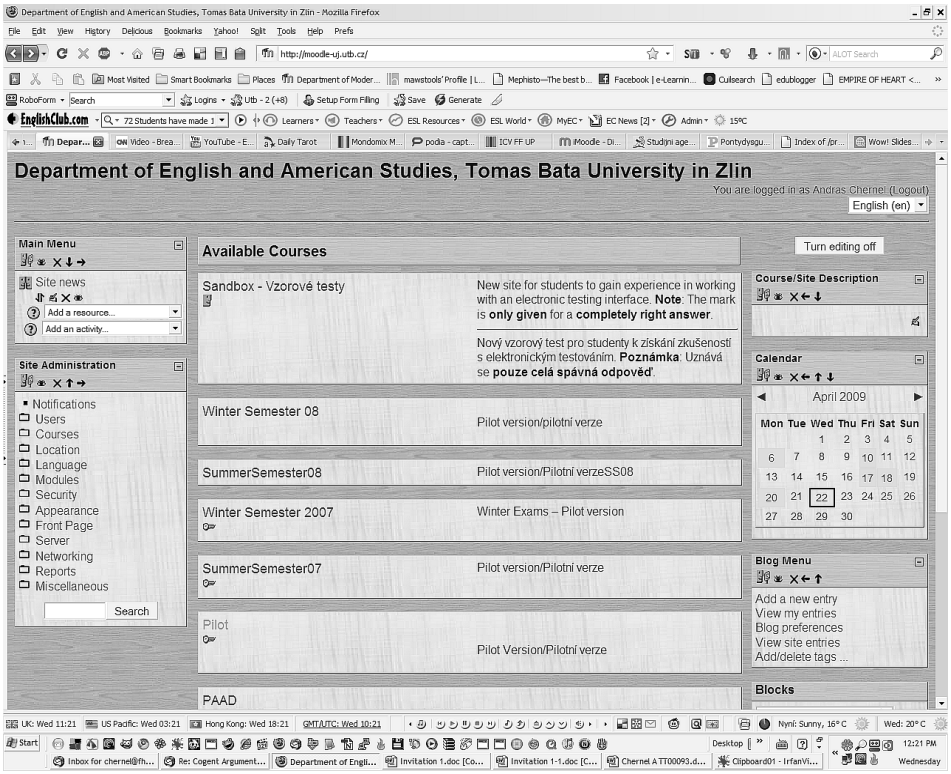


Fig. 5. View of Front-page: http://moodle-uj.utb.cz/

These sample tests are modelled on real tests with a limited selection of the questions used in the real tests that are either modified or are then not included in the real tests. They are exactly the same size (number of questions) and scope (areas tested), and are accessed and completed in exactly the same way as the real tests. Students simply register using their university generated username and password and then they have access 24-hours a day, seven days-a-week, 365 days-a-year to these tests.

The content of the sample sandbox test is not changed; whereas the real tests are expanded and renewed every semester by the inclusion of new questions used in the 4 interim "progress-check" tests given to full-time students during each semester.

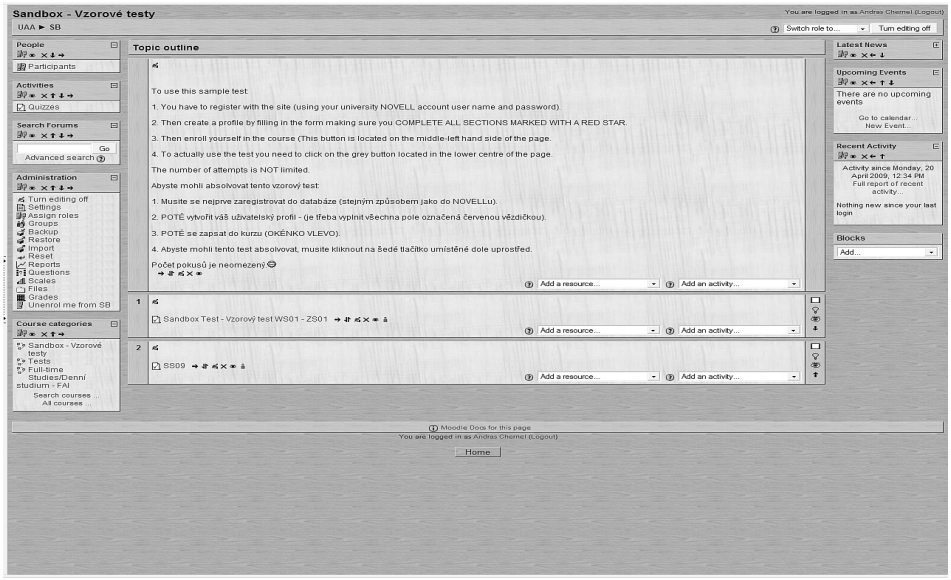


Fig. 6. View of test site, showing editing tools on the left and next to sample tests:http://moodle-uj.utb.cz/course/view.php?id=10

The following data proves the point – for the winter `08 semester exam, the sandbox test created and opened for 05.01.2009 and the beginning of the examination period took about three hours using existing data-bases. It was used by 42 students who registered and made 217 attempts – which is an average of 5.166 attempts per student. All of these students passed the examinations.

The summer semester sandbox test was created on Friday 17.04.2009 and took about two hours to create. It has already been used by 15 students who have made 18 attempts.

5. Other issues needing consideration

- **Logistics** – since Moodle is Open Source freeware, it can be readily downloaded and easily installed. The latest version handles all logistics issues relating to course delivery without problem.
- **Administration** – since all activities are recorded and backed-up regularly, all administrative, auditing and control issues are made much easier for administrative staff: e.g. assignment deadline completion; test scores, grades and logs; etc. There is also a statistrics application which allows statistics to easily be extrapolated for comparative purposes.
- **Cost benefit** – while it is recommended that a good server be used to run Moodle a standard stand-alone computer is enough to begin with. These are relatively small packages[15] (12-14 Mb) that run on Windows, Linux and Mac OS X systems. As mentioned earlier,

[15] http://download.moodle.org/ .

Moodle is an open source resource under the GPL licence. Everything they produce is available for download and use for free. It also saves costs in pedagogue wages, copying, telecommunications, etc.

- **Security** – regular upgrades and security patches are devised and provided for free as soon as a threat is encountered. However, security issues like ensuring that a student is the person who should be sitting there and their effective invigilation (oversight) when there are more of them; and the individual"eyeball" checking and correction of the results take time.

Conclusion

In conclusion, a hearty recommendation is made to all prospective users of this VLE LMS which is user-friendly, dynamic, ever-evolving and robust. The use of an LMS like Moodle allows pedagogues to create a set of materials which can be readily accessed 24 hours a day by all of their students from wherever those students happen to be with access to the Internet. It also allows the setting and collection of assignments, including setting deadlines as well as the examination of students – either in the form of "progress tests" or final examinations. It allows pedagogues to communicate directly – either collectively or individually, with their students as well as allowing students to communicate and collaborate with one another. The system allows for rapid feeback, support and advice as well as the collection and analysis of statistical data. And finally, the courses can be shared or "lent" intra-murally or inter-university – allowing potential students to "virtually" participate in courses provided by professionals and experts from other institutions and even countries without the need to travel physically – except perhaps for a recommended face-to-face session at the beginning or end of the course. For institutions` managements and administration staff, these systems also provide a source of data for course extension, expansion, improvement, monitoring and the collection of data on students progress and marks during their studies.

Sources

1. Zimola B., Chernel A., Hán J., Poulová P., *Building a Virtual Learning and Teaching Community in the Czech Republic and in Europe*. In: „Proceedings of The 4th International Conference on Education and Information Systems", Volume II, Orlando, United States 2006.
2. Sharma P., Barrett B., *Blended Learning: using technology in and beyond the language classroom*, Macmillan Publishers Limited, 2007.

3. *Blackboard vs. Moodle, A Comparison of Satisfaction with Online Teaching and Learning Tools*, Bert Bos, Kathy D. Munoz, Professor, Humboldt State University, Joan Van Duzer, Instructional Technologist, Humboldt State University, 15 February 2005.
4. Sharma P., Barrett B., Blended Learning: using technology in and beyond the language classroom, Macmillan Publishers Limited, 2007.
5. C. Rasmussen, US National Geospatial Intelligence Agency – http://tinyurl.com/ytoqwf .
6. Radar Networks, http://novaspivack.typepad.com/nova_spivacks_weblog/radar_networks.
7. Brown J. S., Adler R. P., *Open Education, the Long Tail, and Learning* **2.0**, „EDUCAUSE Review“*,* Vol. 43, No. 1 (January/February 2008): 16–32
8. Brown J. S., Adler R. P., *Open Education, the Long Tail, and Learning* 2.0, "EDUCAUSE Review"*,* Vol. 43, No. 1 (January/February 2008): 16–32
9. "Students Attitudes Towards Innovative Computer-Related Assignments: The Experiences of a Graduate Level Class", Neubauer B. J., Krzychi N., ©1998, Panel 40-4 Computers and Multimedia Section of the American Political Science Association.
10. http://moodle.org/sites/
11. www.WikiEducator.org.
12. http://vyuka.fhs.utb.cz/ http://download.moodle.org/

Summary

This contribution provides a brief overview of the history, current and future trends in integrating Internet tools like Moodle and other collaborative learning and learning tools (e.g. blogs, wikis, etc) into the education delivery process. It also sets out cogent arguments for using the Moodle LMS system for the delivery of course materials and resources, for their administration, addresses the logistical and cost aspects, and describes experiences gained through the implementation and use of the "open source" Moodle LMS (Learning Management System) to structure courses.

Mariusz Dudek,
Elżbieta Szczepankiewicz*

ROZWÓJ TECHNOLOGII INFORMATYCZNYCH A ZAGROŻENIA I ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWACH

Wprowadzenie

Na przestrzeni ostatnich kilkunastu lat systemy informatyczne stały się jednym z kluczowych narzędzi prowadzenia działalności gospodarczej. Powszechne zastosowanie techniki komputerowej w podmiotach gospodarczych wiąże się z różnymi zagrożeniami dla bezpieczeństwa informacji biznesowej. Zagrożenia te stają się coraz trudniejsze do przewidzenia i wykrycia, a ich skutki mogą być bardzo kosztowne i trudne do usunięcia.

Podmioty prowadzące działalność z wykorzystaniem techniki komputerowej powinny identyfikować te informacje i drogi ich obiegu, których utrata lub ujawnienie może być szkodliwa dla firmy. Winny rozważyć skutki naruszenia bezpieczeństwa informacji, jak np. naruszenie zaufania inwestorów, skutki prawne, utratę wizerunku, obniżenie wydajności działalności i spadek przychodów.

Według badań przeprowadzonych przez naukowców z Uniwersytetu w Chicago utrata informacji biznesowych powoduje, iż 50% firm bankrutuje natychmiast, a dalsze 20 % firm po roku od tego zdarzenia [4, s. 27]. Stąd świadomość zaostrzenia polityki bezpieczeństwa powinna wzrastać wraz z powiększaniem się zasobów informatycznych w firmie.

Celem niniejszego opracowania jest przedstawienie podstawowych źródeł zagrożeń dla informacji biznesowej. W artykule zaprezentowano wyniki badań na temat zarządzania bezpieczeństwem informacji w środowisku informatycznym przedsiębiorstw, przeprowadzonych

* Autorzy są pracownikami naukowo-dydaktycznymi Zakładu Zastosowań Informatyki w Wyższej Szkole Handlu i Rachunkowości w Poznaniu.

przez specjalistyczne firmy w latach 2004-2007 oraz wyników badań autorów przeprowadzonych w latach 2004-2008 r.

1. Źródła zagrożeń w środowisku informatycznym dla informacji biznesowych

Zagrożenia dla informacji biznesowej w podmiotach gospodarczych mogą wynikać z wielu źródeł. R .P. Fisher klasyfikuje **zagrożenia według rodzajów** [3, s. 54]. Są to zagrożenia wynikające z błędów ludzkich, błędów sprzętu i oprogramowania, celowego nadużycia zasobów informatycznych przez ludzi, bądź zdarzeń losowych (katastrof).

Podstawowymi **źródłami tych zagrożeń** są poszczególne elementy tworzące środowisko informatyczne w organizacji, jak np.:

- zasoby informatyczne, takie jak: sprzęt komputerowy, oprogramowanie operacyjne i biznesowe, wykorzystana technologia, zbiory danych i dokumentacja systemów,
- personel informatyczny,
- organizacja pracy,
- otoczenie zewnętrzne (w tym: zagrożenia wynikające z łączności podmiotu z otoczeniem biznesowym poprzez Internet).

Nie wszystkie źródła zagrożeń w jednakowy sposób mogą oddziaływać na bezpieczeństwo informacji biznesowej przetwarzanej w środowisku informatycznym.

Szczególnie istotną kategorią działania umyślnego w środowisku informatycznym jest przestępczość komputerowa. Działania przestępcze skierowane są przeciwko poufności, integralności lub dostępności informacji. Są to między innymi takie działania jak: haking, podsłuch komputerowy, szpiegostwo komputerowe, fałszerstwo komputerowe, niszczenie informacji, sabotaż komputerowy, nielegalne uzyskiwanie programu, kradzież danych lub sprzętu, rozpowszechnianie wirusów i innych szkodliwych programów.

2. Wyniki badań w zakresie bezpieczeństwa informacji w organizacjach w latach 2004-2008

Szczególnie duże znaczenie należy przywiązywać do wyników badań przeprowadzanych co rok w USA i Europie Zachodniej przez międzynarodową firmę Ernst & Young. W 2004 roku firma Ernst &

Young przeprowadziła siódme światowe badanie dotyczące bezpieczeństwa informacji w organizacjach.[1] Równolegle autorka przeprowadziła własne badania w latach 2004-2005[2].

Badania Ernst & Young i badania własne potwierdzają, że w 2004 roku ponad 70 % polskich dużych firm doświadczyło nieprzewidzianej awarii oprogramowania biznesowego. Najczęściej wskazywane powody w badaniach Ernst & Young wystąpienia nieprzewidzianych awarii krytycznych systemów biznesowych to np.:

- szkodliwe programy i wirusy (70%),
- awaria infrastruktury (67%),
- awaria oprogramowania (61%),
- awaria sieci telekomunikacyjnej (52%).

Wyniki badań własnych w tym zakresie prezentuje tabela 1.[3]

Tab. 1.
Powody wystąpienia nieprzewidzianych awarii systemów biznesowych w 2004 i 2005 roku

Powody wystąpienia nieprzewidzianych awarii systemów	2004 r.	2005 r.
Szkodliwe programy i wirusy	46%	52%
Awaria infrastruktury	29%	33%
Awaria oprogramowania	38%	35%
Awaria sieci telekomunikacyjnej	21%	22%
Błędy obsługi	8%	6%
Niedostateczna wydajność systemu	33%	35%
Ataki z zewnątrz	8%	2%

Źródło: Opracowanie własne.

Ankietowanych poproszono także o wskazanie pięciu głównych przeszkód w osiągnięciu odpowiedniego poziomu bezpieczeństwa

[1] W badaniu udział wzięło ponad 1400 przedsiębiorstw, w tym 44 duże polskie firmy. Przedsiębiorstwa reprezentowały 26 branż z 66 krajów. Ankietę skierowano do dyrektorów ds. informatyki, specjalistów ds. bezpieczeństwa informacji.

[2] Ankietę skierowano do wybranych dużych podmiotów (odpowiedzi uzyskano z 24 podmiotów w 2004 r. oraz z 41 podmiotów w 2005 r.). W badaniach wzięły udział największe polskie banki i instytucje finansowe, jednostki administracji publicznej oraz przedsiębiorstwa sektora prywatnego różnych branż, zatrudniające ponad 200 pracowników.

[3] Z uwagi na to, że do incydentów bezpieczeństwa w wielu organizacjach dochodziło kilkakrotnie w ciągu roku, ankietowani mogli wskazywać więcej niż jedną przyczynę.

informatycznego w polskich podmiotach, były to [7 oraz badania własne]:

- brak świadomości wśród użytkowników,
- ograniczenia budżetowe,
- trudność wykazania znaczenia bezpieczeństwa informacji,
- brak czasu na przygotowanie długookresowych planów/rozwiązań,
- dostępność wykwalifikowanego personelu.

Jak potwierdziły badania Ernst & Young (z 2004r.) i badania własne (w latach 2004-2008 r.)[4] mniej niż połowa polskich podmiotów podjęła działania mające na celu zwiększenie świadomości wśród użytkowników w zakresie bezpieczeństwa informatycznego, pomimo iż ankietowani wskazali brak świadomości wśród użytkowników jako główną przeszkodę w osiągnięciu odpowiedniego poziomu bezpieczeństwa informatycznego w ich firmach.

Ankietowani mieli wskazać również największe zagrożenia dla bezpieczeństwa informacji w firmach (tabela 2). Wskazywano, iż największe obawy związane są z uaktywnieniem się szkodliwych programów i wirusów, nieuprawnionymi działaniami pracowników oraz rozproszonym atakiem DoS. W pierwszej szóstce znalazły się także obawy przed atakami hakerów.

Tab. 2.
Największe zagrożenia bezpieczeństwa informacji w polskich podmiotach w latach 2004-2008

Za największe zagrożenia bezpieczeństwa informacji uznano:	Badania Ernst & Young 2004 r.	Badania własne 2004 r.	Badania własne 2005 r.	Badania własne 2008 r.
Szkodliwe programy i wirusy	2	1	1	2
Działania pracowników	1	2	3	5
Rozproszony atak DoS	4	3	2	1
Utratę poufnych danych o klientach	3	5	4	3
Ataki hakerów amatorów	6	6	6	6
Fizyczne uszkodzenie systemu	5	4	5	4

[4] Badania własne autorów w zakresie bezpieczeństwa informacji w organizacjach są nadal kontynuowane.

Źródło: Opracowanie na podstawie Światowe Badanie dotyczące Bezpieczeństwa Informacji 2004, Ernst & Young, www.ey.pl i badania własne.

Kolejne Światowe Badanie Bezpieczeństwa Informacji Ernst & Young w 2005 [6] wskazały główne czynniki, które wywrą największy wpływ w kolejnych latach na działania podejmowane przez firmy w zakresie bezpieczeństwa informacji, są to:

- zgodność z obowiązującymi regulacjami prawnymi (59%),
- ogólne priorytety organizacji w zakresie bezpieczeństwa (66%),
- osiągnięcie celów biznesowych (47%),
- wirusy i robaki (34%),
- nowe technologie (50%),
- wymagane certyfikaty z zakresu bezpieczeństwa informacji (31%),
- phishing oraz spyware (25%),
- negatywny rozgłos (3%).

Potrzebę dostosowania się do obowiązujących wymogów prawnych w kolejnych latach wskazywano jako główny czynnik skłaniający podmioty do podejmowania działań w zakresie bezpieczeństwa informacji. Wszyscy respondenci prowadzący działalność na rynku światowym deklarowali, że w ich firmach podjęto już działania mające na celu stworzenie lub dostosowanie polityk oraz procedur wewnętrznych do wymogów amerykańskiej ustawy Sarbanes-Oxley, VIII Dyrektywy UE, rekomendacji Komitetu Bazylejskiego ds. Nadzoru Bankowego. Wynikało to z wpływu na ich działalność nowych przepisów lub standardów, dotyczących tworzenia mechanizmów kontroli wewnętrznej oraz zarządzania ryzykiem operacyjnym wpływającym na bezpieczeństwo informacji. Kilkanaście procent z tych podmiotów deklaruje budowanie systemu bezpieczeństwa informacji w oparciu o uznane światowe standardy, takie jak: ISO 17799, ITIL, COBIT, a w przyszłości uzyska certyfikat zgodności z wdrażanym standardem [6, s. 10-11].

Już w 2003 r., główni analitycy firmy IDC przestrzegali, że ataki na korporacyjne systemy informatyczne, zarówno przewodowe, jak i bezprzewodowe, będą się z czasem stawały coraz bardziej wyrafinowane i będą kierowane na raz w wiele słabych punktów tych systemów. Coraz powszechniejsze będą się stawały zagrożenia wirusowe i trudniejsze do wykrycia robaki hybrydowe, czyli wykorzystujące starsze postaci wirusów. Dlatego firmy nieustannie przyglądać się muszą swoim systemom i badać nieszczelności [1, s. 22]. Z roku na rok rośnie

liczba szkodliwych programów i ataków na systemy operacyjne, rosną także potencjalne szkody.

W krótkim czasie po tych ostrzeżeniach, bo w 2005 r., pojawiły się dwa nowe zagrożenia dla bezpieczeństwa informacji, określane jako "phishing" i "pharming". Polegają one na nakłanianiu ludzi do ujawniania poufnych informacji przy użyciu fałszywej poczty elektronicznej i fałszywych stron internetowych. Te dwie formy ataków zostały ukierunkowane na pracowników firm jaki i osoby prywatne. Potwierdza się fakt, że czynnik ludzki w firmach jest nadal najsłabszym ogniwem w łańcuchu bezpieczeństwa informacji.

Istotną rolę w zmniejszeniu tego ryzyka może odegrać ścisła weryfikacja klientów, szkolenia pracowników i wiedza o potencjalnych zagrożeniach. Jednak, jak wykazało badanie przeprowadzone w 2005 roku przez Deloitte [5], szkolenia i wiedza w zakresie bezpieczeństwa nie są uznawane przez zarządy za zagadnienia kluczowe - szkolenia lub inne przedsięwzięcia poszerzające wiedzę w tym zakresie planowało na 2006 i 2007 rok mniej niż połowa (46%) respondentów[5]. Niepokojącym jest także fakt, że szkolenia i poszerzanie wiedzy o potencjalnych zagrożeniach znalazły się na końcu listy priorytetowych zagadnień związanych z bezpieczeństwem informacji. Respondenci Deloitte cenili wyżej przestrzeganie procedur (74%) oraz raportowanie i pomiary (61%). Te wyniki znalazły też odzwierciedlenie w planach inwestycyjnych podmiotów w zakresie bezpieczeństwa: najwięcej pieniędzy ma zostać przeznaczonych w kolejnych latach na narzędzia zabezpieczające (64%), podczas gdy jedynie 15% ma zostać wykorzystane na szkolenia i zwiększanie wiedzy pracowników.

Z badań własnych autorów przeprowadzonych w 2005 roku na próbie 87 dużych, średnich i małych polskich przedsiębiorstw[6] oraz w latach 2007-2008 na próbie kolejnych 72 podmiotów i wynika, że w 2005 roku 40 % firm doświadczyła niespodziewanej przerwy w działaniu systemów biznesowych w ciągu 12 ostatnich miesięcy. W badaniu przeprowadzonym w latach 2007-2008 wyniki były znacznie wyższe,

[5] Badania Ernst & Young (z 2004 r.) i badania własne (w latach 2004-2008 r.) potwierdzają także, że mniej niż połowa polskich firm podjęła szkolenia w celu zwiększenia świadomości użytkowników na temat bezpieczeństwa informatycznego.

[6] Ankietą objęto następujące typy podmiotów: przedsiębiorstwa produkcyjne, handlowe, usługowe. Podmioty zostały uszeregowane według wielkości: duże przedsiębiorstwa – powyżej 200 zatrudnionych, średnie przedsiębiorstwa – 50-200 zatrudnionych, małe firmy do 50 zatrudnionych.

ponieważ dotyczyły 72 % firm, które doświadczyły niespodziewanej przerwy w działaniu systemów biznesowych w ciągu 12 ostatnich miesięcy.

Z firm, które zanotowały niedostępność do systemów biznesowych w 2005 r. tylko 61%, a w 2007-2008 – 69%, oprócz usuwania skutków bada także przyczyny tej niedostępności. Niestety zarówno w 2005, jak i w następnych latach, w ponad jednej trzeciej podmiotów najwyższe kierownictwo nie interesuje się badaniem przyczyn niedostępności systemów.

Respondenci wskazali również główne przyczyny niedostępności oprogramowania biznesowego[7]:

- w 2005 roku 43% i w latach 2007-2008 – 69% niedostępności powodowały wirusy i inne szkodliwe programy,
- w 2005 roku 33% i w latach 2007-2008 – 38% niedostępności było wynikiem awarii oprogramowania,
- w 2005 roku 33% i w latach 2007-2008 – 32% niedostępności było wynikiem awarii sprzętu komputerowego,
- w 2005 roku 27% i w latach 2007-2008 – 48% przyczyną była niedostateczna wydajność systemów,
- w 2005 roku 10% i w latach 2007-2008 – 9% przyczynę stanowiły błędy obsługi powodowane przez użytkowników,
- w 2005 roku 10% i w latach 2007-2008 – 11% to celowe działania pracowników,
- w 2005 i latach 2007-2008 roku mniej niż 2% stanowiły ataki hakerów.

W jednej czwartej firm nie wyznaczono osoby odpowiedzialnej za bezpieczeństwo danych informatycznych. W 2005 roku aż w 45% podmiotów i w 2007-2008 roku w 37% podmiotów nie opracowano dokumentów (procedur, instrukcji, szczegółowych polityk) opisujących system bezpieczeństwa danych informatycznych. Ponad połowa podmiotów nie posiada procedur awaryjnych dla najważniejszych aplikacji biznesowych.

W 2005 roku prawie 43% podmiotów nie organizowało żadnych szkoleń dla pracowników w zakresie bezpieczeństwa danych informatycznych, a 32% podmiotów organizowało szkolenia jednorazowe. Nowo zatrudnionych użytkowników systemów w zakresie

[7] Ankietowani mogli wskazywać więcej niż jedno źródło niedostępności.

bezpieczeństwa danych informatycznych szkoliło tylko 37%. W latach 2007-2008 w każdej z wyżej wymienionych kategorii wyniki kształtowały się na poziomie o 2-5% wyżej.

Analiza największych na świecie 145 incydentów naruszenia wewnętrznego bezpieczeństwa informatycznego przeprowadzona przez firmę Kaspersky pokazuje, że „wycieki informacji" mają coraz częściej charakter globalny. Obecnie stało się bezcelowe wskazywanie obszaru działalności gospodarczej czy regionu geograficznego, w którym firmy rzadko lub nigdy nie ucierpiały w wyniku działań osób mających dostęp do poufnych informacji. W 2006 roku wycieki informacji miały miejsce zarówno w małych firmach, jak i ogromnych korporacjach, organizacjach komercyjnych oraz rządowych. Główne wnioski z raportu „Globalne badanie wycieków danych 2006" przedstawiają się następująco [9]:

- w większości przypadków (66%) wycieki poufnych informacji dotykają organizacji biznesowych. Każdy wyciek osobistych informacji może powodować milionowe straty. Oprócz strat finansowych zniszczona zostaje reputacja firmy, a setki tysięcy osób mogą stać się ofiarą kradzieży tożsamości.
- w 2006 roku ofiarą wycieku informacji padła ogromna liczba osób. W prawie 150 incydentach 80 milionów osób zostało zagrożonych kradzieżą tożsamości. Wiele z nich może stać się ofiarą oszustów i utracić wszystkie swoje oszczędności lub mieć na zawsze zrujnowaną historię kredytową.
- w grupie wysokiego ryzyka znajdują się organizacje, które pozwalają swoim pracownikom korzystać z urządzeń przenośnych. Korzystanie z takiego sprzętu doprowadziło do wycieków informacji w przypadku połowy wszystkich incydentów (50%); natomiast tylko w 12% przypadków medium wykorzystywanym do wycieków był Internet.
- główne zagrożenie w przedsiębiorstwach stanowi brak dyscypliny pracowników. W 2006 roku zaniedbanie było przyczyną przeważającej większości wycieków (77%).

Podobnie raport firmy G DATA o szkodliwym oprogramowaniu w 2007 roku [10] potwierdza również, że dominującym trendem w przestępczości internetowej stała się kradzież prywatnych danych klientów banków. W celu uzyskiwania dostępu do kont użytkowników wykorzystywano szereg rozwiązań przekierowujących do sfałszowanych witryn, bądź umożliwiających odczytanie haseł zapisanych w pamięci

komputera użytkownika. Ponadto wraz z rozwojem szkodliwego oprogramowania oraz spamu pojawiły się istotne zmiany w jego dystrybucji. W przypadku większości ataków rezygnowano z umieszczenia załączników w e-mailach, zastępując je linkami do witryn internetowych zawierających złośliwe programy, bądź umożliwiających zainfekowanie komputera. Stałym zagrożeniem pozostają nadal wirusy, bowiem ich ilość od 2007 roku zwiększyła się aż pięciokrotnie, w dużej mierze dzięki popularności mobilnych nośników danych. Obok nowych wirusów, pojawiają się starsze, które po zmianie kodu źródłowego nie są rozpoznawane przez skanery internetowe i mogą ponownie skutecznie atakować.

Warto także zwrócić uwagę na wyniki opublikowane przez Computer Security Institute [2]. Z badań przeprowadzonych w 2007 roku wskazują, że po raz pierwszy od pięciu lat zaobserwowano znaczny wzrost średniej straty spowodowanej przestępczością komputerową. Przyczyny upatrywać należy w coraz popularniejszych przestępstwach na tle finansowym (m.in. phishing, vishing czy spam), z których straty finansowe w 2007 roku znacznie przewyższyły straty z ataków wirusów. Prawie jedna piąta ankietowanych (18%) potwierdziła, że w ciągu minionego roku stała się celem skrzętnie zaplanowanego i spersonalizowanego ataku. Respondenci wskazywali również na inne czynniki powodujące straty spowodowanej przestępczością komputerową jak np.: kradzież firmowych laptopów i urządzeń przenośnych – 50%, ataki rozproszone blokujące usługi (DDoS) – 25%, podmianę firmowej strony WWW – 10%, ataki sieci bezprzewodowej – 17%.[8]

Z badań przeprowadzonych w 2007 roku przez firmę Symantec wynika, że [9]:

- 69% ankietowanych spodziewa się wystąpienia drobnego incydentu bezpieczeństwa raz w miesiącu,
- 63% szacuje prawdopodobieństwo wystąpienia poważnej systemu informatycznego co najmniej raz w roku,
- 25% uważa, że wyciek danych wystąpi co najmniej raz w roku.

Istotną kwestią jest ocena postawy zarządów i właścicieli w kwestii nadzoru nad bezpieczeństwem informacji. Badania własne potwierdziły, zarówno w 2005, jak i w latach 2007-2008, że w mniej niż połowie polskich dużych firm sektora prywatnego najwyższe kierownictwo

[8] CSI co roku buduje raport w oparciu o ankiety wysyłane do kilku tysięcy amerykańskich firm. Wiele z tych firm ma także oddziały w Polsce.

otrzymuje okresowo informacje o poziomie bezpieczeństwa zasobów informatycznych. Jeszcze słabsze zainteresowanie tym zagadnieniem wykazują kierownicy mniejszych przedsiębiorstw.

Wnioski

Na podstawie prezentowanych badań wśród polskich i zagranicznych podmiotów należy stwierdzić, że skala incydentów bezpieczeństwa informacji i braki w zakresie zarządzania bezpieczeństwem informacji biznesowych są podobne.

Z zaprezentowanych wyników badań wynika, iż zarządy firm zbyt wolno reagują na nowe zagrożenia w środowisku informatycznym. Przykładem jest tu rozwój technologii mobilnych. Wymogi biznesowe oraz malejące koszty połączeń bezprzewodowych są siłą napędową rozwoju tych technologii. Jednak ich użycie powoduje, że zasoby informacyjne, wydostają się poza kontrolowane środowisko organizacji. Wymaga to znacznie większej odpowiedzialności pracowników, którzy korzystają z przenośnych urządzeń informatycznych, wymiennych nośników danych i sieci bezprzewodowych.

Kolejny wniosek z badań to, że działania z zakresu bezpieczeństwa informacji rzadko są zintegrowane ze strategią biznesową firmy. Podmioty wymagające wysokiego poziomu bezpieczeństwa informacji biznesowej powinny prowadzić ciągłą analizę ryzyka elementów środowiska informatycznego i systemu zabezpieczeń. Powinny identyfikować te informacje i drogi ich obiegu, których utrata lub ujawnienie może być szkodliwa dla firmy. Winny również rozważyć skutki naruszenia bezpieczeństwa informacji, jak np. naruszenie zaufania inwestorów, skutki prawne, utratę wizerunku, wydajności działalności i obniżenie przychodów. Natomiast podmioty, które nie wymagają wysokiego poziomu bezpieczeństwa informacji, rezygnują zwykle z kosztownej i pracochłonnej analizy ryzyka i decydują się na pewien standardowy, wypracowany na podstawie innych instytucji, zestaw zabezpieczeń. Obecnie także i zarządzanie bezpieczeństwem danych finansowych na poziomie podstawowym w wielu firmach jest niewystarczające. Badania własne potwierdziły, że w większości średnich i mniejszych podmiotów kierownictwo słabo dba o przestrzeganie przepisów w zakresie podstawowej ochrony informacji (np. ustawy o rachunkowości – rozdział VII – Ochrona danych).

Prawdopodobnie jest to konsekwencją braku obowiązkowego audytu w tych podmiotach.

Należy podkreślić, że nieuświadamianie sobie ryzyk, przez kierownictwo i nieprzeciwdziałanie im drogą projektowania i stosowania odpowiednich mechanizmów ochrony, kontroli i podnoszenia świadomości zagrożeń wśród pracowników, może prowadzić do ryzyka utraty zasobów informatycznych i incydentów bezpieczeństwa informacji. W każdym przypadku wdrożenie i funkcjonowanie skutecznego systemu zabezpieczeń powinno uwzględniać zarówno aspekty prawne, programowe, techniczne, jak i organizacyjno-administracyjne. System zabezpieczeń powinien skutecznie chronić dostęp do oprogramowania biznesowego i zbiorów danych. Zwiększenie bezpieczeństwa zasobów informatycznych i informacji biznesowej powinno być jedną z głównych dziedzin zainteresowania kierownictwa jednostki gospodarczej.

Bibliografia

1. Cosgrove Ware L., *Nie ma końca inwestycjom w bezpieczeństwo, Bezpieczeństwo – podejście strategiczne i najlepsze praktyki*, „Raport CXO", Listopad 2003.
2. „Dwunasty doroczny Raport FBI I CSI" – bezpieczeństwo informatyczne 2007. www.e.gospodarka.pl.
3. Fisher R.P., *Information Systems Security*, Prentice-Hall Inc., Englewood Cliffs 1984.
4. Korytowski J*., Budowa efektywnego systemu kontroli wewnętrznej – wybrane aspekt*y, Materiały konferencyjne ISACA, Warszawa 1.2.2001.
5. Raport Security Survey 2005, www.deloitte.com.pl.
6. Raport Światowe Badanie Bezpieczeństwa Informacji 2005, www.ey.com.pl
7. Światowe Badanie Bezpieczeństwa Informacji 2004 – Wyniki dotyczące Polski, Ernst&Young, www.ey.com.pl.
8. www.media.netpr.pl/PresOffice/getFilePressRelease.92320.po?oid=43929.
9. Wycieki danych w firmach w 2006r. www.kaspersky.pl
10. Zarządzanie ryzykiem IT – obalenie mitów, www.symantec.pl.

DEVELOPMENT OF IT AND INFORMATION SECURITY IN ORGANIZATIONS

Summary

Organizations are continually seeking more productive and competitive ways of working, which are driving the proliferation of rapidly developing technologies. Business demands and the low cost of wireless connectivity are driving the rapid adoption of mobile technology. These technologies hold the potential of increasing organizations competitive advantage. These technologies bring also the growing risk.

This article indicates that information security in organizations 2004-2008. Many organizations is not doing enough to keep up with these changes in technology. It now becomes imperative for them to take action. Both larger and smaller organizations face similar challenges with acquiring qualified information security specialists and certified in information security standards.

INTRODUCTION

At the turn of 20th and 21st century significant changes took place in the world economy. The diversification of production has been associated by changes in the distribution of labour markets and the development of consumer and industrial markets until the present. Markets of such countries as China, India, Brazil or Turkey belong to the most dynamically growing ones as regards business and consumption. Within the European Union the quickly developing regions include the group of Central and East European countries. Such distribution of markets determines the changes in the trade exchange between Europe and other markets and this, in turn, enforces the development of logistic networks.

The changes on the international labour and consumption market are reflected in the sea transport. In 2005-2008 alone the sea transport increased from 6.7 billion tonnes to 7.4 billion tonnes. The global demand for sea transport reached 32 billion tonne-miles (in 2008). It was estimated that by 2008 this demand had grown by 5% annually. It has been assumed that after the period of recession the demand will come back to its initial status and that means that in 2030 the sea transport figures may even be doubled. Between 1970 and 2008 the international sea trade grew by almost 190% together with the increase of consumption and the changes in the international market of manufacture. Liquid cargo transport increased in the period almost by 100%. Dry cargo transport increased between 1970 and 2008 almost by 260%. Such dynamics of the goods exchange contributed to the fast development of logistic networks and information systems particularly in the recent years. The global trade connections are associated by the network of communication networks and logistic chains.

The crisis on the global financial market in the middle of 2008 and the following crash in demand on the market of goods and services curbed the increase of cargos in containers and the ro-ro transport on the navigation and harbour market and to a lesser degree on the mass cargo market. The prosperity period provoked optimism on the transport market as regards planning of the acquisition of new means for land, air and sea transport. Large expenditures were incurred in the building of

the logistic infrastructure including the indispensable infrastructure for cargo handling of dynamically growing demand for goods in containers. The collapse of economy in the leading economies resulted first in perturbations on the sea transport market and later in ports (decreased trans-shipment), followed by the shipbuilding industry that was shown by the ship-owners withdrawing the orders for new ships. That, in turn, resulted in the decrease of the demand for steel products and for specialist appliances. This is an example of a crisis situation on a few markets connected with the logistic system.

The authors of the research included in the publication titled *Logistics, communication and security* tried not only to prepare a diagnosis of threats in the field of logistics, communication and power generation but also to find the answer to the present day problems and to propose solutions enabling safe operation of logistic and information networks.

In the first part of the monograph titled **Logistic and security** the authors paid attention to the whole spectrum of security of logistic processes including the energetic and physical security of logistic areas and even technical aspects of rail transport units.

In part 2 titled **Communication and security** the authors shared the results of their research concerning the efficiency of the flow of information within an organisation in stable and crisis situations as well as the aspects of information protection of an enterprise. This part also includes the presentation of the results of the research on communication in the most modern ICT solutions in the technical and organisational aspect.

The monograph has been created for the needs of those readers who are interested in the look at the security issues from the perspective of logistic networks manager, trade exchange organiser or person managing information within a company in stable and crisis conditions.

Marek Grzybowski, Janusz Tomaszewski