BEZPIECZEŃSTWO EUROLOGISTYKI

Andrzej SZYMONIK

Streszczenie: Artykuł poświęcony jest zachowaniu ciągłości działania procesów logistycznych realizowanych w ramach eurologistyki. Składa się on z trzech rozdziałów. Pierwszy poświęcony jest analizie zagrożeń, które mogą wpływać negatywnie na działania realizowane w ramach eurokanłów logistycznych. Kolejny rozdział zawiera istotę zarządzania bezpieczeństwem eurologistyką z uwzględnieniem wszystkich jego faz tj. zapobiegania, przygotowania, reagowania i odbudowy. W ostatnim rozdziale zaprezentowane są praktyczne narzędzia wykorzystywane w zarządzaniu bezpieczeństwem eurologistyki. Zostały one podzielone na prawne i techniczno-technologiczne.

Słowa kluczowe: eurologistyka, bezpieczeństwo zagrożenia, zarządzanie bezpieczeństwem

1. Zagrożenia bezpieczeństwa

Każde działania w eurologistyce zarówno w sferze planowania, jak i realnej są obarczone niepewnością, która może być wywołana pojawiającym się niebezpieczeństwem (zagrożeniami) bądź zakłóceniami.

Jako zagrożeniami dla bezpieczeństwa w eurologistyce określamy wszelkie działania (zjawiska, zdarzenia) zakłócające realizację procesów logistycznych, do których zaliczamy przepływy dóbr rzeczowych, utrzymania zapasów, infrastrukturę strumienia logistycznego, koszty logistyczne oraz przepływ informacji. Tego typu zdarzenia mogą występować pojedynczo lub mogą się łączyć, tworząc sytuację niebezpieczną, z punktu widzenia biznesu, dla systemu gospodarczego i wszystkich uczestników eurokanałów.

Zagrożenia mogą być skierowane na zewnątrz i do wewnątrz, przy czym tak samo powinny być skierowane działania w celu ich likwidowania.

Zagrożenia ciągle się zmieniają, tak jak zmienia się wiedza o nich. Nowe zagrożenia, a także nieznane – są niebezpieczne. Istniejące i znane nie są groźne, bo możemy im zapobiec. Jedne zagrożenia oddalają się od nas, inne przybliżają – jednak stają się nieuniknione, choć inne są możliwe do uniknięcia [1, s. 20].

Zagrożenia dla bezpieczeństwa eurologistyki możemy podzielić na cztery grupy.

Do pierwszej grupy zaliczamy klęski żywiołowe i zdarzenia wywołane przyczynami cywilizacyjnymi, tj. katastrofy, awarie oraz inne zdarzenia spowodowane działaniem lub zaniedbaniem człowieka. Do tej grupy zagrożeń należą m.in.: pożary, powodzie i zatopienia, silne wiatry i huragany, kradzieże, epidemie chorób ludzi, epidemie chorób roślin i zwierząt, skażenia promieniotwórcze i chemiczne, katastrofy górnicze, budowlane i komunikacyjne, awarie sieci energetycznych, wodnych, ciepłowniczych.

Do drugiej grupy zaliczamy zdarzenia godzące w porządek konstytucyjny państwa (państw), terroryzm, blokady dróg, nielegalne demonstracje, konflikty na tle etnicznym, masowe migracje.

Do trzeciej grupy zaliczamy mechanizmy, które mają na celu niszczenie bądź zniekształcanie informacji przesyłanej, przetwarzanej, przechowywanej dla potrzeb

eurologistyki. Wszelkie zakłócenia w obiegu informacji powodują utrudnienia w sprawnym i skutecznym zarządzaniu logistyką wzdłuż całego łańcucha dostaw.

Do czwartej grupy zalicza się zagrożenia wynikające ze skutków kryzysu finansowego, który tak naprawdę dotyka wszystkich, nie omijając procesów i systemów eurologistycznych. Zabezpieczenia przed kryzysem nie daje nawet gospodarka o świetnych wskaźnikach rozwoju i tak naprawdę nie zostały wypracowane do końca instrumenty antykryzysowe.

Wymienione zagrożenia mogą destruktywnie oddziaływać na system eurologistyczny, zakłócając przepływ strumienia rzeczowego i informacji.

Zakłócenia te możemy podzielić ze względu na [2, s. 254]:

- miejsce zagrożenia – podsystem:
  - dróg wszystkich gałęzi transportu (tj. drogowego, kolejowego, powietrznego, wodnego, morskiego),
  - punktów modalnych sieci logistycznej nazywanych często punktami transportowymi (np. magazyny, samodzielne punkty kontenerowe, lotniska, porty, centra logistyczne itp.),
  - urządzeń pomocniczych ułatwiających obsługę dróg i punktów transportowych,
  - zarządzania (np. brak pełnej identyfikacji i skutków zagrożeń, przeszacowanie możliwości, niewłaściwa interpretacja wyników, brak narzędzi do optymalizacji i symulacji działań, rosnące ceny energii i transportu, niespodziewane upadłości usługodawców logistycznych),
  - zaopatrzenia (np. nieterminowość, zła jakość, cena, ilość, asortyment, przekupstwo, łapownictwo, brak możliwości pozyskania komponentów do wytwarzania, uszkodzenia systemu informacyjnego, brak buforowego zapasu),
  - produkcji (np. niedomagania systemów wytwarzania, bioterroryzm, zniszczenia, ubytki, kradzieże zasobów, dostępność fachowego personelu, przerwy produkcyjne, awarie, pożary, powodzie, katastrofy),
  - dystrybucji (np. nowe produkty, nowi producenci, kradzieże, warunki atmosferyczne, zła jakość wyrobów gotowych, kryzys gospodarczy, lekceważenie zarządzania relacjami z klientem i przepływem wyrobów w łańcuchu dostaw),
  - transportu (np. pożar, eksplozja, wypadek środka transportu, zmycie z pokładu, brak możliwości przemieszczenia ze względu na warunki atmosferyczne, niesprawny środek transportu, nieprzystosowany transport wewnętrzny, zmiany przepisów w gestii transportowej, kradzieże, katastrofy),
  - magazynowy i kształtowania zapasów (np. kradzieże, straty w wyniku ponadnormatywnych zapasów, pożary, powodzie, katastrofy budowlane, awarie sieci energetycznej i systemu informatycznego, uszkodzenie systemu automatycznej identyfikacji),
  - obsługi opakowań (np. zanieczyszczenie środowiska, zniszczenie wyrobów w transporcie na skutek złego doboru opakowań, niedostarczenie opakowań na czas na skutek złych warunków klimatycznych),
  - obsługi zamówień klienta (np. brak zapasów, błędne zamówienie i faktura, nieterminowe dostarczenie, uszkodzone wyroby dostarczone do klienta, brak reakcji na reklamacje i opóźnienia, pożary, kradzieże, zniszczenia, brak możliwości wycofania wadliwych produktów),

  - informacyjny (np. utrata poufności, integralności oraz możności dysponowania, naturalne zagrożenia, jak pożary, zakłócenia klimatyczne, elektrostatyka, ataki bierne i aktywne, przypadkowe błędy, błędne informacje na opakowaniach);
- czas trwania:
  - krótkotrwałe, sporadyczne,
  - długotrwałe, narastające,
  - powtarzające się;
- własności fizykalne:
  - materialne (np. transportowe),
  - informacyjne (np. uszkodzenia systemu informatycznego, automatycznej identyfikacji),
  - energetyczne (np. gazowe, paliwowe),
  - niematerialne (np. kryzys finansowy);
- zasięg:
  - lokalny dotyczący logistyki danego systemu gospodarczego, będącego ogniwem kanału eurologistycznego,
  - rozległy wzdłuż całego łańcucha dostaw.

2. Zarządzanie bezpieczeństwem eurologistyki

Stan bezpieczeństwa nie jest stabilny – nie jest dobrem danym systemowi gospodarczemu raz na zawsze. W świecie realnym występują ciągłe zagrożenia, zarówno od sił natury, jak i niezamierzonych oraz zamierzonych efektów działalności człowieka.

Każdy system eurologistyczny musi zatem czynić starania o zapewnienie sobie stabilnego stanu bezpieczeństwa. Każdy logistyczny system gospodarczy, będący ogniwem eurokanału, winien wykształcić w swej działalności możliwość szybkiego reagowania na wszelkie zmiany w otoczeniu wewnętrznym i zewnętrznym, w tym również możliwość współpracy w ramach systemu bezpieczeństwa z innymi podmiotami.

Stwierdzenie to nie jest niczym nowym, jako że już w połowie ubiegłego wieku ojciec współczesnego zarządzania P. Drucker proponując kryteria wyboru oraz projektowania organizacji, stwierdził, że każde przedsiębiorstwo winno posiadać trwałość końcową do przetrwania w okresie zamieszania i umiejętność dostosowania się do nowych warunków [3].

Przyjęta strategia funkcjonowania eurologistyki nie powinna być nakierowana tylko na realizację procesów logistycznych i obniżanie kosztów, ale również winna uwzględniać problematykę współczesnych zagrożeń wzdłuż całego łańcucha dostaw.

System bezpieczeństwa eurologistyki powinien być dostosowany do potencjalnych zagrożeń oraz pożądanego poziomu bezpieczeństwa, jaki musi być mu zapewniony w eurokanałach. Zatem ilość oraz jakość środków, niezbędnych do utrzymania pożądanego poziomu bezpieczeństwa w obszarze działań eurologistycznych, ich organizacja oraz sposób prowadzenia działań (a ściślej procesów), po wyzwoleniu zagrożenia (zajścia zdarzenia), zależy od jego rodzaju i skali oraz prognozy możliwości wystąpienia zagrożeń innych rodzajów.

Bezpieczeństwo działań w sieciach i kanałach eurologistycznych to stan, który daje poczucie pewności i gwarancję:

- przepływu dóbr rzeczowych i usług, w konsekwencji zaspokojenie materialnych potrzeb uczestników łańcucha dostaw zgodnie z regułą „7W" (wyjaśnienia skrótów patrz s. 13);
- przepływu informacji dla potrzeb planowania i zarządzania procesami logistycznymi;
- ochrony i przetrwania w okresie sytuacji niebezpiecznych (zagrożeń);
- dostosowania się do nowych warunków (podatność na nieplanowe sytuacje).

Poziom bezpieczeństwa procesów eurologistycznych uwarunkowany jest odpornością na zagrożenia współpracujących uczestników w kanałach i sieciach w wymiarze lokalnym i globalnym.

Bezpieczeństwo systemu eurologistycznego związane jest z:

- poziomem przygotowana i odpornością systemu do przeciwdziałania sytuacjom nadzwyczajnym (główna uwaga koncentruje się na rozpoznawaniu, monitorowaniu, analizowaniu danych i trafnym podejmowaniu decyzji w obszarze działań logistycznych wzdłuż całego eurokanału);
- jakością stworzonego i funkcjonującego systemu bezpieczeństwa – rozumianego jako zespół sił oraz środków zapewniających akceptowalny przez uczestników sieci eurologistycznych stanu bezpieczeństwa.

Określony poziom bezpieczeństwa systemu eurologistycznego możemy uzyskać na wiele sposobów – nie tylko poprzez zapewnienie określonej skuteczności bezpośredniego przeciwdziałania zaistniałym zdarzeniom.

Mamy zatem możliwość kształtowania poziomu bezpieczeństwa systemu eurologistycznego poprzez jego zarządzanie, które możemy zdefiniować jako *zestaw skoordynowanych działań podjętych w momencie pojawienia się zagrożeń (zakłóceń), skierowanych na zasoby logistyczne wszystkich uczestników eurokanału, z zamiarem osiągnięcia celu, którym może być bezpieczeństwo dostaw, zmniejszenie zagrożeń, zrealizowanie warunków ustalonych przez właściciela ładunku oraz ochronę pozycji na rynku i marki*.

Wielkościami sterowalnymi w tym przypadku są parametry charakteryzujące się czynnikami wpływającymi na poziom bezpieczeństwa systemu, czyli związane z [4]:

- zapobieganiem możliwym zagrożeniom bezpieczeństwa procesów realizowanych w ramach eurokanału.
- przygotowaniem eurosystemu logistycznego na wypadek uaktywnienia tych zagrożeń;
- zasobami przeciwdziałającymi tym zagrożeniom;
- usuwaniem następstw danego zdarzenia.

Zapobieganie możliwym zagrożeniom bezpieczeństwa systemu eurologistycznego obejmuje:

- sformułowanie polityki bezpieczeństwa przez wszystkich uczestników w sieci eurologistycznej;
- przeprowadzenie oceny ryzyka w czasie realizacji procesów w eurokanałach;
- opracowanie planu dla zarządzania i zmniejszenia zidentyfikowanych zagrożeń;
- wykrywanie, identyfikację, ewidencję i kontrolowanie możliwych zagrożeń;
- prognozowanie możliwości wystąpienia sytuacji kryzysowych (np. na podstawie hurtowni danych z wykorzystaniem systemów komputerowych);
- badanie akceptacji poziomu zagrożeń przez uczestników łańcucha dostaw w wymiarze europejskim;

- określenie rodzaju i zakresu działań zapobiegających zagrożeniom w obszarze np. dróg transportowych, magazynowania, dystrybucji, kosztów logistycznych – wzrost kosztów paliwa;
- prowadzenie szkoleń wśród osób zajmujących się logistyką w wymiarze mikro (pojedynczego systemu gospodarczego) i makro (wszystkich uczestników łańcucha dostaw w górnej i dolnej części eurokanału), ze szczególnym zwróceniem uwagi na:
  - instytucjonalizacje stosunków logistycznych,
  - ujednolicenie procesów logistycznych,
  - standaryzację procesów (np. zgodnie z GS1 czy APICS),
  - rosnące wymagania transparentności (przejrzystości) systemu gospodarczego w kontaktach biznesowo-logistycznych,
  - zaostrzenie kryteriów podejmowania ryzyka i profesjonalizacji działań w ramach eurologistyki,
  - rolę danych, informacji oraz wiedzy na możliwość monitorowania, sterowania, kontrolowania i reagowania na procesy logistyczne w eurokanałach,
  - potrzebę poszerzenia współpracy międzynarodowej nauki i przemysłu w obszarze doskonalenia procesów logistycznych,
  - odtwarzanie zniszczonego ekosystemu i szersze wykorzystanie odnawialnych źródeł energii,
  - zarządzanie zaufaniem, ryzykiem i bezpieczeństwem w działaniach eurologistycznych.

Przygotowanie systemu eurologistycznego na wypadek uaktywnienia zagrożeń obejmuje przedsięwzięcia związane z:

- wdrożeniem planu zarządzania bezpieczeństwem, np. wyznaczenie komórek kierujących i wykonawczych przez wszystkie ogniwa eurokanału;
- wykonaniem dokumentacji zarządzania bezpieczeństwem logistycznym i nadzór nad jej aktualnością;
- przygotowaniem w tym obszarze procedur postępowania akceptowanych przez wszystkich uczestników łańcucha dostaw (a więc nie tylko przez pojedynczy system gospodarczy);
- przygotowaniem zapasowej infrastruktury logistycznej (np. transport, drogi, magazyny, opakowania, dodatkowe źródła zaopatrywania – w kraju i poza jego granicami, awaryjni odbiorcy) oraz zasobów ludzkich;
- określeniem sposobu wymiany informacji wewnątrz systemu gospodarczego i pozostałymi uczestnikami łańcucha dostaw eurokanału na całej jego długości;
- określeniem systemu monitorowania w obszarze przepływu dóbr rzeczowych/usług i informacji w okresie trwania zakłócenia z uwzględnieniem dodatkowych kosztów działań;
- wdrożenie certyfikatów zapewniających ciągłość działania.

Reagowanie kryzysowe obejmuje działania i przedsięwzięcia związane z:

- uruchomieniem wcześniej opracowanych procedur i nadzorowanie ich realizacji;
- współpracą i koordynacją działań w realizacji procesów logistycznych wzdłuż całego łańcucha dostaw eurokanału;
- bieżącym reagowaniem na występujące dodatkowe, niezaplanowane sytuacje;

- zbieraniem raportów, ich analizą i podejmowaniem stosownych działań związanych z przepływem strumienia rzeczowego i informacyjnego wzdłuż łańcucha dostaw w sieci eurologistycznej.

Odbudowa obejmuje działania związane z:

- szacowaniem, ewidencją strat w obszarze kosztów logistycznych przez wszystkich uczestników kanału eurologistycznego;
- odbudową starych rynków zaopatrzenia, zbytu;
- odbudową zaufania wśród uczestników łańcucha dostaw i klientów finalnych;
- odbudową infrastruktury logistycznej.

3. Instrumenty wykorzystywane w praktycznym zarządzaniu bezpieczeństwem systemów eurologistycznych

Narzędziami pomocnymi w zarządzaniu bezpieczeństwem systemów logistycznych w ujęciu mikro i makro są rozwiązania:

- unormowane przez organizacje krajowe i międzynarodowe;
- techniczno-technologiczne.

Do pierwszej grupy między innymi zaliczamy:

- Normę ISO 28000:2007, która została stworzona specjalnie dla firm i organizacji uczestniczących w łańcuchu dostaw. Umożliwia ona identyfikację zagrożeń i ograniczenie ryzyka w łańcuchu dostaw poprzez realizację procesów zapewnienia bezpieczeństwa mających na celu zmniejszenie ryzyka kradzieży, przemytu, nielegalnego manipulowania ładunkiem i zapewnienie reakcji na zagrożenia ze strony ataków przestępców, terrorystów i innych. Wymaga, aby stosująca je organizacja sformułowała politykę bezpieczeństwa, przeprowadziła ocenę ryzyka i opracowała plan dla zarządzania oraz zmniejszania zidentyfikowanych zagrożeń, wdrażania planu zarządzania bezpieczeństwem, monitorowania i nadzorowania systemu, podejmowania działań korygujących, gdy są wymagane, a także przeprowadzania przeglądów zarządzania w celu ciągłego doskonalenia. Organizacja w celu określenia wymagań związanych z bezpieczeństwem powinna uwzględnić:
  - cele biznesowe – zawierające bezpieczeństwo dostaw, zmniejszenie zagrożeń (kradzieży, piractwa, fałszerstw, aktów terroryzmu), spełnienie wymagań właścicieli ładunków oraz ochronę reputacji i marki,
  - wymagania prawne oraz inne, takie jak np. AEO, C-TPAT, ISPS, TAPA,
  - identyfikację zagrożeń oraz szacowanie ryzyka.

  Po zidentyfikowaniu charakteru działania organizacji, jej skali i innych wymagań tworzona jest polityka bezpieczeństwa i przeprowadzana ocena ryzyka. Proces oceny ryzyka umożliwia organizacji zidentyfikowanie aktywów i procesów kluczowych dla dalszego działania, określenie realnych zagrożeń, ocenę luk w istniejących programach bezpieczeństwa, oszacowanie prawdopodobieństwa zaistnienia zagrożenia oraz rozważenie jego konsekwencji. Stosując proces oceny ryzyka, organizacje mogą określić przypuszczalną jego wielkość, a następnie priorytety (dla ustalenia celów i zadań w zakresie bezpieczeństwa), które są wykorzystywane do ustanowienia planów zarządzania bezpieczeństwem w celu ograniczenia skutków zidentyfikowanych zagrożeń.

Programy zarządzania bezpieczeństwem powinny być wdrażane i stale monitorowane pod kątem efektywności. Pozwala to na realizację działań korygujących, umożliwiając tym samym doskonalenie systemu, co z kolei wpływa na zmniejszenie poziomu ryzyka w trakcie jego następnej cyklicznej oceny. Norma ta może być stosowana przez przedsiębiorstwa w celu zapewnienia spójnego podejścia wszystkich podmiotów działających w łańcuchu dostaw oraz jako punkt referencyjny do zarządzania bezpieczeństwem w łańcuchu dostaw [5, s.28 i 29].

- Brytyjski standard BS 25999:2007 – opisujący zasady systemowego podejścia do zarządzania ciągłością działania – BCM (*Business Continuity Management*). Jego opublikowanie było odpowiedzią na oczekiwania organizacji pragnących uzyskać gwarancję funkcjonowania na rynku w razie najmniej spodziewanych sytuacji. Wdrożenie systemu zarządzania ciągłością działania (BCM) w organizacji daje następujące korzyści [6]:
  - możliwość nieprzerwanego działania w zakresie niezbędnego minimum w obliczu niezaplanowanych niekorzystnych zdarzeń,
  - minimalizuje ryzyko wystąpienia zakłóceń,
  - przygotowuje organizację na sytuacje kryzysowe oraz pozwala, dzięki odpowiednim procedurom, na ich przezwyciężenie,
  - zapewnia możliwość ponownego odtworzenia zdolności firmy do działania w określonym czasie i na ustalonym poziomie,
  - wdrożony standard podnosi wiarygodność organizacji w oczach klientów, inwestorów i udziałowców,
  - pozwala chronić pracowników organizacji,
  - wpływa na ochronę i poprawę reputacji firmy i danej marki,
  - jest częstym wymogiem regulatorów, potencjalnych klientów, a także ubezpieczycieli (certyfikat może wpłynąć na ograniczenie wysokości składki ubezpieczeniowej od przerwy w działalności),
  - stanowi o przewadze konkurencyjnej – mówi o zdolności do funkcjonowania niezależnie od zdarzeń, co w znacznym stopniu ułatwia zdobycie nowych rynków.

  BCM jest pojęciem szerszym od zarządzania ryzykiem. Poza określeniem wyrobów, usług i procesów, które wyznaczają przetrwanie organizacji oraz przeprowadzeniem szacowania ryzyka i działań z tym związanych, zgodnie z ideą BCM należy również zidentyfikować, co jest niezbędne organizacji, by mogła kontynuować wykonywanie swoich zobowiązań w przypadku materializacji ryzyka. Dzięki BCM organizacja jest w stanie rozpoznać, co należy zrobić przed wystąpieniem ewentualnego zdarzenia, by chronić swoich pracowników, teren, infrastrukturę, technologię, informacje, łańcuch dostaw, interesariuszy oraz reputację. Taka wiedza umożliwia organizacji realne spojrzenie na to, jak należy zareagować w przypadku wystąpienia ewentualnych zagrożeń oraz radzenia sobie z wszelkimi jego skutkami bez nieakceptowanej zwłoki np. w dostarczaniu produktów lub usług.
- W maju 2012 roku została opublikowana międzynarodowa norma ISO 22301, zawierająca wymagania dotyczące systemów zarządzania ciągłością działania. Zastąpiła ona wówczas obowiązujący brytyjski standard BS 25999. Jak dotąd norma ta nie została przetłumaczona na język polski. Bazując na swoim

poprzedniku, wprowadza ona nowe rozwiązania korzystnie wpływające na cały system zarządzania ciągłością działania. Wymagania ISO 22301 zostały przedstawione w 10 rozdziałach, a brytyjski poprzednik miał ich 6. Norma zawiera [7]:

- nowy formalny wymóg określenia kontekstu organizacji, celem dostarczenia wszystkich informacji do zastosowania systemu zarządzania ciągłością działania, odpowiedniego dla organizacji i będącego wsparciem jej działań oraz osiągania celów (w ramach określenia kontekstu organizacja powinna zidentyfikować i udokumentować zakres działalności, w tym produkty, usługi, miejsce w łańcuchu dostaw, relacje z dostawcami i klientami, powiązania pomiędzy polityką ciągłości a innymi obowiązującymi rodzajami polityki oraz obowiązujące ją przepisy prawa i inne regulacje),
- szczegółowe wymagania stawiane najwyższemu kierownictwu (norma wymaga, aby najwyższe kierownictwo było aktywnie zaangażowane w realizację polityki ciągłości działania i ustanawianie jej celów, ponadto powinno się wykazać dowodami zaangażowania w budowanie, wdrożenie oraz monitorowanie systemu zarządzania ciągłością działania),
- wymagania dotyczące konstruowania i wdrożenia procedur obejmujących komunikację wewnętrzną (z pracownikami organizacji), zewnętrzną (z klientami, partnerami w łańcuchu dostaw, lokalną społecznością i mediami) oraz w trakcie sytuacji kryzysowej, uwzględniającą powiadomienie, współpracę z odpowiednimi instytucjami rządowymi i samorządowymi,
- szczegółowe wymagania dotyczące wdrożenia i koordynacji systemu zarządzania ciągłością działania, m.in. dotyczącego analizy wpływu na biznes, analizy ryzyka, strategii i procedur zarządzania ciągłością działania oraz zasad ich testowania (zawiera wymagania odnośnie zarządzania incydentami, m.in. wymaga opracowania procedury, która będzie zawierała zasady wykrywania, monitorowana, dokumentowania, komunikowania, informacji dotyczących przebiegu incydentów),
- wymóg dotyczący opracowania udokumentowanych procedur w celu powrotu do normalnej działalności organizacji po opanowaniu sytuacji kryzysowej;
- wymagania dotyczące audytów wewnętrznych i przeglądów zarządzania oraz ustalenia dotyczące monitorowania, pomiaru, analizy i oceny wydajności i skuteczności systemu zarządzania ciągłością działania,
- ustalenie mierzalnych celów i ocenę ich osiągnięcia (organizacja powinna określić co powinno być monitorowane i mierzone, zdefiniować stosowane metody monitorowania, pomiaru, analizy, oceny oraz wskazać, kiedy pomiary mają być dokonywane, a także kiedy będą analizowane).

- ISO 26000:2010 – norma międzynarodowa (wypracowana wspólnie przez 99 państw) zawierająca wytyczne dotyczące społecznej odpowiedzialności organizacji za skutki (wpływ) podejmowanych decyzji i działań na społeczeństwo oraz środowisko. Norma ta zapewnia przejrzyste i etyczne postępowanie, które [8]:
  - przyczynia się do zrównoważonego rozwoju, w tym zdrowia i dobrobytu społeczeństwa,

- spełnia oczekiwania interesariuszy (osób lub grup, które są zainteresowane decyzjami lub działaniami organizacji),
- jest zgodne z obowiązującym prawem i spójne z międzynarodowymi normami postępowania,
- jest zintegrowane z działaniami organizacji i praktykowane w jej relacjach, które dotyczą działań organizacji podejmowanych w obrębie jej sfery oddziaływań;
- uporządkuje wiedzę na temat społecznej odpowiedzialności biznesu (CSR *Corporate Social Responsibility*).

Celem ISO 26000 jest wsparcie organizacji w ich udziale w zrównoważony rozwój. Norma ma zachęcić do wyjścia poza nałożone prawem zobowiązania, przy jednoczesnym zrozumieniu, że przestrzeganie prawa jest podstawowym obowiązkiem jakiejkolwiek organizacji i niezbędną częścią jej odpowiedzialności społecznej. Norma ma promować powszechne zrozumienie odpowiedzialności społecznej i uzupełniać – a nie zastępować – inne narzędzia i inicjatywy na tym polu. Wprowadzając ISO 26000, warto mieć na względzie społeczne, środowiskowe, prawne, kulturowe, organizacyjne i ekonomiczne różnice, przy jednoczesnym przestrzeganiu międzynarodowych standardów działalności.

- Wymogi organizacji transportu towarów niebezpiecznych są normowane ustawami, przepisami oraz rozporządzeniami, które uwzględniają uwarunkowania prawa międzynarodowego. W Polsce tymi dokumentami są:
  - Ustawa z dnia 19.08.2011 r. o przewozie towarów niebezpiecznych. Ustawa dokonuje w zakresie swojej regulacji wdrożenia Dyrektywy 2008/68/WE Parlamentu Europejskiego i Rady z dnia 24.09.2008 r. w sprawie transportu lądowego towarów niebezpiecznych, Dyrektywy Komisji Europejskiej 2010/61/UE z dnia 02.09.2010 r. dostosowującej po raz pierwszy do postępu naukowo-technicznego załączniki do Dyrektywy 2008/68/WE Parlamentu Europejskiego i Rady w sprawie transportu lądowego towarów niebezpiecznych, Dyrektywy 2010/35/UE Parlamentu Europejskiego i Rady z dnia 16.06.2010 roku w sprawie ciśnieniowych urządzeń,
  - ADR (fr. *L' Accord européen relatif au transport international des marchandises Dangereuses par Route*) – Umowa europejska dotycząca międzynarodowego przewozu drogowego towarów niebezpiecznych (ADR), sporządzona w Genewie dnia 30 września 1957 r. (Dz.U. z 2011 r. nr 110, poz. 641), wraz ze zmianami obowiązującymi od dnia ich wejścia w życie w stosunku do Rzeczypospolitej Polskiej, ogłoszonymi we właściwy sposób,
  - RID (fr. *Reglement concernant le transport Internationale ferroviaire des marchandises Dangereuses)* – Regulamin dla międzynarodowego przewozu kolejami towarów niebezpiecznych (RID), stanowiący załącznik C do Konwencji o międzynarodowym przewozie kolejami (COTIF), sporządzonej w Bernie dnia 9 maja 1980 r. (Dz.U. z 2007 r. nr 100, poz. 674 i 675, z 2009 r. Nr 167, poz. 1318 oraz z 2011 r. nr 137, poz. 804 i 805), wraz ze zmianami obowiązującymi od dnia ich wejścia w życie w stosunku do Rzeczypospolitej Polskiej, ogłoszonymi we właściwy sposób;
  - ADN — Umowa europejska dotycząca międzynarodowego przewozu śródlądowymi drogami wodnymi towarów niebezpiecznych, zawarta w Genewie dnia 26 maja 2000 r. (Dz.U. z 2010 r. nr 235, poz. 1537), wraz ze

zmianami obowiązującymi od dnia ich wejścia w życie w stosunku do Rzeczypospolitej Polskiej, ogłoszonymi we właściwy sposób;
  - kodeks IMDG, International Maritime Dangerous Goods Code – Międzynarodowy morski kodeks towarów niebezpiecznych;
  - kodeks IBC – dotyczy budowy i wyposażenia statków przewożących niebezpieczne chemikalia luzem;
  - kodeks IGC – dotyczy budowy i wyposażenia statków przewożących skroplone gazy luzem;
  - kodeks INF – dotyczy bezpiecznego przewozu statkami napromieniowanego paliwa jądrowego, plutonu i wysokopromieniotwórczych odpadów w pojemnikach.
- Ubezpieczenia ładunków w transporcie krajowym i międzynarodowym. W ramach ubezpieczenia cargo międzynarodowego ochrona ubezpieczeniowa obejmuje wszystkie fazy przewozu ładunku drogą lądową (samochodową lub kolejową), lotniczą, morską lub śródlądową, wraz z niezbędnymi czynnościami przeładunkowymi i przejściowym magazynowaniem ładunku na trasie transportu. Ochrona może obejmować również operacje załadunku lub wyładunku. Najczęściej ubezpieczający ma trzy zakresy ochrony do wyboru:
  - podstawowy, obejmujący szkody powstałe wskutek takich zdarzeń, jak np. pożar, eksplozja, wypadek środka transportowego;
  - rozszerzony, obejmuje najczęściej, oprócz wymienionych powyżej rodzajów ryzyka, również szkody powstałe w wyniku np.: zmycia z pokładu, przedostania się wody morskiej, jeziornej lub rzecznej do ładowni, kontenera lub miejsca składowania (oferta ta skierowana jest zatem szczególnie do importerów i eksporterów korzystających z transportów morskich);
  - pełny, obejmujący wszystkie rodzaje ryzyka.

  Transporty międzynarodowe są ubezpieczane w firmach ubezpieczeniowych w oparciu o standardowe ICC – Instytutowe Klauzule Ładunkowe (*Institute Cargo Clauses*), powszechnie stosowane zarówno przez ubezpieczycieli, jak i przez handlowców, eksporterów i importerów na całym świecie. W ramach ICC istnieją trzy podstawowe grupy, różniące się zakresem ubezpieczenia [9]:
  - ICC (A) – Instytutowe Klauzule Ładunkowe A, oznaczane dawniej literami AR, obejmujące „wszystkie rodzaje ryzyka"; zestaw klauzul stwierdzający ogólnie, że ubezpieczeniem objęte są „wszystkie rodzaje ryzyka" (tzn. wypadki losowe polegające na działaniu siły zewnętrznej) powodujące stratę lub uszkodzenie przedmiotu towaru, z wyjątkiem wyraźnie wyłączonych w klauzulach B i C; klauzula A nie obejmuje, poza wymienionymi w niej wyłączeniami (*exclusions*) i wyłączeniami klauzul B i C następującego ryzyka: wojny oraz strajków, zaburzeń społecznych i terroryzmu – tu wymagane jest ubezpieczenie na szczególnych warunkach *Institute War Clauses i Institute Strikes Clauses*; klauzula powszechnie stosowana przez polskich ubezpieczycieli przy konstruowaniu warunków ubezpieczenia mienia (ładunków) w transporcie międzynarodowym.
  - ICC (B) – instytutowe klauzule ładunkowe B, oznaczane dawniej literami WA; klauzule kazuistycznie ujmujące warunki ubezpieczenia i ryzyko objęte ochroną w przeciwieństwie do formuły *All Risks* zastosowanej w klauzulach A; wyłącza z ubezpieczenia niektóre ryzyko wymienione w klauzuli A;

klauzula powszechnie stosowana przez polskich ubezpieczycieli przy konstruowaniu warunków ubezpieczenia mienia (ładunków) w transporcie międzynarodowym.
  - ICC (C) – instytutowe klauzule ładunkowe C, oznaczane dawniej literami FPA; klauzule kazuistycznie ujmujące warunki ubezpieczenia i ryzyko objęte ochroną w przeciwieństwie do formuły *Ali Risks* zastosowanej w klauzulach A; klauzula o najwęższym zakresie ubezpieczenia z trzech podstawowych klauzul ICC; powszechnie stosowana przez polskich ubezpieczycieli przy konstruowaniu warunków ubezpieczenia mienia (ładunków) w transporcie międzynarodowym.
- Incoterms (*International Commercial Terms*) – Międzynarodowe Reguły Handlu to zbiór zasad, określających warunki sprzedaży, których stosowanie jest szeroko przyjęte na całym świecie. Reguły te dzielą koszty i odpowiedzialność pomiędzy nabywcę i sprzedawcę oraz odzwierciedlają rodzaj uzgodnionego transportu. Incoterms odnoszą się do Konwencji ONZ dotyczącej kontraktów dla Międzynarodowej Sprzedaży Dóbr. Zostały opublikowane w 1936 roku i wielokrotnie je nowelizowano. Obecnie obowiązującą wersją (od 1 stycznia 2011) jest Incoterms® 2010, który zastąpił Incoterms 2000 i *reguluje związki między sprzedającym i kupującym, nie określa jednocześnie stosunków stron umowy z przewoźnikami, spedytorami i operatorami przewozów multimodalnych. Niemniej znajomość formuły transportowej jest niezbędna spedytorowi do właściwej organizacji transportu, zabezpieczenia ewentualnych roszczeń, określenia wartości celnej towaru, jego odprawy itp.* Incoterms® 2010 *mają zastosowanie nie tylko w handlu zagranicznym, ale również w unijnym czy krajowym* [10] i zawierają wykładnię 11 formuł handlowych, podzielonych na cztery grupy (E, F, C i D), z których każda oznaczona jest trzyliterowym skrótem (pierwsze litery ich nazw angielskich). Formuły uszeregowano wg kryterium zwiększających się obowiązków i ryzyka sprzedającego (od EXW do DDP). W każdej formule obowiązki sprzedającego i kupującego ujęto odpowiednio w dziesięciu punktach, wzajemnie korespondujących. Obowiązki sprzedającego ponumerowano A1 – A10, kupującego B1 – B10.
- Status upoważnionego przedsiębiorcy AEO (*Authorised Economic Operator)* – uprawnia do korzystania z ułatwień odnoszących się do kontroli celnej w zakresie bezpieczeństwa i ochrony oraz uproszczeń podczas odpraw celnych. W zakresie kontroli celnej dotyczącej bezpieczeństwa i ochrony przedsiębiorca może korzystać z następujących ułatwień [11]:
  - podlega mniejszej niż inni przedsiębiorcy liczbie kontroli fizycznych i 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.

Do grupy rozwiązań techniczno-technologicznych zaliczamy między innymi:

- Traceability - system kompleksowego śledzenia pochodzenia (identyfikacja partii produktu, surowców użytych do jego produkcji, a następnie indywidualnie

każdego produktu składającego się na partię w czasie produkcji lub/i dystrybucji do bezpośredniego konsumenta).

- Standardy GS1: kody kreskowe (standardowe nośniki wykorzystywane w procesie automatycznej identyfikacji i gromadzenia danych), elektroniczna komunikacja (standardowe dokumenty transakcyjne do wymiany drogą elektroniczną), synchronizacja danych podstawowych (infrastruktura i standardy do wymiany danych podstawowych o produktach i usługach), Elektroniczny Kod Produktu (standardy identyfikacyjne wykorzystujące technologię RFID i Internet).
- Business Intelligence – BI (analityka biznesowa) jest pojęciem bardzo szerokim. Najbardziej ogólnie można przedstawić je jako proces przekształcania danych w informacje, a informacji w wiedzę, z pomocą szerokiego wachlarza aplikacji i technologii, która może być wykorzystana do zwiększenia sprawności oraz skuteczności określonych działań, w tym związanych z zapewnieniem bezpieczeństwa systemów logistycznych [12]. BI stanowi kompleksowe ujęcie wszystkich zjawisk związanych z wykorzystaniem narzędzi, jakie dostarcza Business Intelligence we wspomaganiu procesów decyzyjnych. BI, to nie tylko technologie informatyczne (TI), ale coś więcej, co spina działalność różnych podmiotów w sferze zarządzania bezpieczeństwem. Dane, informacja, wiedza, pochodzą nie tylko z samego systemu, ale i spoza niego. Dzięki BI można monitorować i analizować poziom bezpieczeństwa w systemach logistycznych w sytuacji, kiedy jest ona bardzo złożona, a ilość danych pochodzi z wielu baz oraz jest niepełna. Obszar wykorzystania tego narzędzia jest bardzo szeroki, może być ono zastosowane w wielu dziedzinach życia nie tylko gospodarczego. Do podstawowych komponentów systemów BI zaliczamy kluczowe technologie informatyczne (narzędzia ETL, hurtownie danych), możliwości kluczowych technologii informatycznych (techniki OLAP, data mining) oraz aplikacje wspomagające podejmowanie różnorodnych decyzji w sytuacjach występowania zagrożeń w systemie logistycznym.
- Sieci monitoringu, które są zbudowane z trzech podsystemów stanowiących jedną całość. Pierwszy podsystem to wszystko, co w sposób bezpośredni i pośredni bierze udział w wykrywaniu zagrożeń (np. sensory i radary oraz urządzenia, na których są one zamontowane, radiometry, radary, GPS). Drugi to media transmisyjne, przewodowe i bezprzewodowe używane do przesyłania sygnałów. Trzeci podsystem, stanowiący serce systemu realizujący wszystkie procesy, to informatyka.

4. Wnioski

Szybki rozwój technologiczny i ekonomiczny, zwiększający się zakres globalizacji, zanik tradycyjnych granic, to niektóre z wielu czynników powodujących wzrost zagrożeń bezpieczeństwa systemów logistycznych, w tym i w wymiarze europejskim. Ilość czynników generujących zagrożenia wraz z rozwojem cywilizacyjnym stale wzrasta. Do nich możemy zaliczyć: rosnące ceny energii i transportu, niespodziewane upadłości strategicznych usługodawców logistycznych, trudności w utrzymaniu płynności finansowej, konieczność dostosowania się do nowych wymogów (w tym ekologistki) prawa lokalnego i międzynarodowego, niedostatek wykwalifikowanych pracowników w obszarze „załadowców", usług transportowych oraz logistycznych, rosnące opłaty ubezpieczeniowe, drogowe i kredytowe [13, s. 20-23].

Optymistycznym jest to, że w miarę jak pojawiają się nowe rodzaje zagrożenia, ludzkość potrafi przeciwstawiać się im, tworząc nowe, lub doskonaląc stare, sposoby, metody i organizacje zabezpieczania się przed nimi. Systemy logistyczne, które są podatne na wszelkie zmiany i zagrożenia bliższe oraz dalsze ze względu na globalne długości i szerokości łańcucha dostaw muszą adaptować się do nowych uwarunkowań technicznych, technologicznych oraz uwarunkowań prawnych w wymiarze krajowym i międzynarodowym.

Definicje i skróty:

„7R" – *right product* (właściwy produkt), *right quantity* (właściwa ilość), *right condition* (właściwy stan), *right place* (właściwe miejsce), *right time* (właściwy czas), *right customer* (właściwy klient), *right price* (właściwa cena).
AEO – to instytucja Wspólnotowego Kodeksu Celnego, która została wprowadzona do porządku prawnego Unii Europejskiej z dniem 1 stycznia 2008 r. celem stworzenia bezpiecznego łańcucha dostaw oraz walki z terroryzmem. Upoważniony przedsiębiorca (AEO) - to biznesmen posiadający jedno ze świadectw: - świadectwo AEO C - uproszczenia celne; - świadectwo AEO S - bezpieczeństwo i ochrona; - świadectwo AEO F - uproszczenia celne/bezpieczeństwo i ochrona. Przyznanie statusu AEO to uznanie przedsiębiorcy za upoważniony podmiot gospodarczy, tj. podmiot uprzywilejowany, któremu przysługuje szereg udogodnień przy dokonywaniu obrotu towarowego. Status AEO przyznany w jednym państwie członkowskim Unii Europejskiej jest uznawany w całej Wspólnocie. Świadectwo AEO daje rękojmię przestrzegania przepisów prawa wspólnotowego przy dokonywaniu międzynarodowych transakcji, wg [10].
APICS jest stowarzyszeniem zrzeszającym praktyków zajmujących się zarządzaniem operacyjnym. Organizacja ta od ponad 50 lat tworzy standardy zarządzania przedsiębiorstwem. Akronim APICS pochodzi od oryginalnej nazwy stowarzyszenia: Am*erican Production and Inventory Control Society*, które powstało w 1958 roku. Pierwotnie APICS skupiał się na sterowaniu produkcją i zarządzaniu zapasami w przedsiębiorstwach przemysłowych. Obecnie jest liderem w dostarczaniu najwyższej jakości wiedzy w zakresie zarządzania operacyjnego, w kontekście wychodzącym szerzej poza klasyczne zagadnienia związane z produkcją. Stąd aktualna nazwa stowarzyszenia: APICS – *The Association for Operations Management.*
C-TPAT – (*Customs-Trade Partnership Against Terrorism*) amerykański certyfikat bezpieczeństwa, jest on porozumieniem pomiędzy władzami celnymi USA i biznesem, mającym na celu zapewnienie maksymalnego bezpieczeństwa łańcucha dostaw, uznanego za najbardziej zagrożony przez akcje terrorystyczne. W ramach C-TPAT wyróżnia się następujące specyficzne porozumienia dla: importerów, licencjonowanych agentów celnych, przewoźników lotniczych, przewoźników morskich, przewoźników lądowych (kolejowych i drogowych), firm konsolidujących przesyłki lotnicze, pośredników transportu morskiego, amerykańskich portów i terminali morskich, zagranicznych producentów, magazynów, wymagań dotyczących plomb i plombowania, [14].
Data mining jest jednym z etapów odkrywania wiedzy w bazach danych. Wywodzi się z takich dziedzin nauki, jak statystyka i uczenie maszynowe. Istota data miningu polega na wykorzystaniu szybkości komputerów do odkrywania ukrytych dla człowieka zależności i prawidłowości w ogromnych zbiorach danych. Przykładem może być wykrycie, które transporty morskie i z jakich kierunków najczęściej się opóźniają.

ETL (*Extract, Transform and Load*) – narzędzia wspomagające proces pozyskania danych dla hurtowni danych. Głównym zadaniem jest: pozyskanie, analiza, przechowywanie danych ze źródeł zewnętrznych.
GS1 to system globalnych standardów identyfikacyjnych i komunikacyjnych tworzących rozwiązania wspierające efektywne zarządzanie w łańcuchu dostaw. Standardy GS1 umożliwiają swobodny i bezpieczny przepływ produktów, usług i informacji, umożliwiają skuteczną wymianę towarów i danych między firmami.
ICC – Instytutowe Klauzule Ładunkowe opracowane przez Londyński Instytut Ubezpieczycieli (Institute of London Underwńters); powszechnie stosowane warunki ubezpieczenia mienia (ładunków) w transporcie międzynarodowym zarówno morskim, jak i lądowym, czasem w lotniczym, określające zakres ochrony ubezpieczeniowej (i ryzyko wyłączone z ochrony) udzielanej przez ubezpieczyciela przy ubezpieczeniu ładunku w transporcie; istnieją trzy podstawowe klauzule oznaczone literami A, B i C różniące się zakresem oferowanego ubezpieczenia; poza trzema podstawowymi istnieje również szereg klauzul specjalistycznych określających warunki ubezpieczenia określonego rodzaju transportu lub dla określonych towarów, [9].
ISPS (*International Ship and Port Facility Security Code)* – Międzynarodowy Kodeks Ochrony Statków i Obiektu Portowego określa ramy współdziałania statku i obiektu portowego, mającego na celu wykrywanie i zapobieganie działaniom, mogącym stanowić zagrożenie bezpieczeństwa. Kodeks: umożliwia wykrywanie i zapobieganie zagrożeniom w ramach międzynarodowej współpracy, ustala podział ról i obowiązków, umożliwia gromadzenie i wymianę informacji związanej z ochroną, dostarcza metod szacowania bezpieczeństwa, zapewnia odpowiednie standardy ochrony. Zobowiązuje załogę statku i pracowników zatrudnionych w porcie do: zbierania i oceny uzyskanych informacji, prowadzenia i utrzymywania standardów komunikacji; uniemożliwienia wstępu osobom nieupoważnionym, wnoszenia broni itd.; uruchamiania procedury alarmowej; opracowania planu ochrony statku i obiektu portowego i potwierdzania prowadzenia treningów i ćwiczeń, wg [15].
OLAP (*On-Line Analytical Processing*) architektura wspierająca analizy decyzyjne. Pozwala na prowadzenie zarówno wieloaspektowych, przekrojowych analiz w repozytorium silnie zagregowanych danych, jak i na przygotowanie szczegółowych raportów w oparciu o dane źródłowe. Architektura OLAP wykorzystuje hurtownie danych i szeroko rozumiane narzędzia analizy danych, takie jak generatory raportów, języki zapytań, eksplorację danych, sztuczną inteligencję.
Punkt modalny sieci logistycznej – a wszystkie miejsca zatrzymywania się produktów, tzn. magazyny, punkty i węzły transportowe oraz fabryki, sieci dystrybucji itd.
Ryzyko – warunki, w których logistyk zna przypuszczalną wielkość prawdopodobieństwa uzyskania wyniku swojej działalności, [16, s. 130], lub ryzyko to miara niepewności, ilościowa ocena prawdopodobieństwa wystąpienia zdarzeń niekorzystnych (zakłóceń), czyli tego, co postrzegamy jako zagrożenie, [17, s. 191].
TAPA (*Transported Asset Protection Association*) to międzynarodowa organizacja zajmująca się różnymi aspektami bezpieczeństwa dostaw w branży zaawansowanych technologii. Skupia producentów dóbr konsumpcyjnych wysokiej wartości, którzy dążąc do minimalizacji ryzyka utraty własnych produktów w trakcie transportu, zaczęli nakładać na swoich poddostawców obowiązek wypełniania kryteriów bezpieczeństwa. TAPA opracowała standardy dotyczące bezpiecznego transportu uchodzące na całym świecie za prestiżowe (FSR / TSR) – jest to zbiór zaleceń i wymagań, jakie muszą być spełnione podczas przewozu i magazynowania towarów określonych grup klientów [18].

Towar niebezpieczny — materiał lub przedmiot, który zgodnie z ADR, RID lub ADN nie jest dopuszczony, odpowiednio, do przewozu drogowego, przewozu koleją lub przewozu żeglugą śródlądową albo jest dopuszczony do takiego przewozu na warunkach określonych w tych przepisach, wg Ustawa z dnia 19 sierpnia 2011 r. o przewozie towarów niebezpiecznych.

Literatura

1. Tyrała P., Zarządzanie kryzysowe, Wyd. A. Marszałek, Toruń 2003.
2. Sienkiewicz P., Teoria i inżynieria bezpieczeństwa systemów, [w:] Zeszyty Naukowe AON nr 1(66)2007.
3. http://www.anonimus.com.pl/P.Drucker.html, 12.10.2013.
4. Kołodziński E., Istota inżynierii systemów zarządzania bezpieczeństwem, http://www.uwm.edu.pl, 10.04.2012.
5. Sitkowski L., Zarządzanie bezpieczeństwem dla łańcucha dostaw – ISO 28000, [w:] „Przemysł Środowisko Jakość Zarządzanie" 2(13)2009.
6. http://www.iso.org.pl/bs-25999, 12.10.2013.
7. http://csr.pl/article/214/, 20.10.2013.
8. http://www.pkn.pl/sites/default/files/discovering_iso_26000.pdf, 20.10.2013.
9. http://www.broker-serwis.pl/slownik_i.html, 16.08.2013.
10. http://www.broker-serwis.pl/slownik_i.html, 16.08.2013.
11. http://www.google.pl/#hl=pl&sclient=psy-ab&q, 08.08.2012.
12. http://www.klub-doskonalenia.pl/show.php?, 23.10.2013.
13. Wittenbrink P., Risken im Transport und Logistikbereich, [w:] "Internationales Verkehrswesen" 2//2013.
14. http://www.katowice.ic.gov.pl, 20.10.2013.
15. http://www.lr.org.pl/index.php?page=uslugi_morskie, 20.02.2013.
16. Szymonik A., Logistyka jako system racjonalnego pozyskiwania wyrobów obronnych, AON, Warszawa 2007.
17. Komorowski J., Cele przedsiębiorstwa a rozwój gospodarczy. Ujęcie behawioralne, SGH, Warszawa 2012.
18. http://sas-ma.org/analiza-tras, 02.10.2013.
19. http://www.zgapa.pl/zgapedia/Business_intelligence.html, 19.10.2013.
20. http://www.krakow.ic.gov.pl/index.php/aeo-i-uproszczenia, 20.10.2013.

Prof. PŁ dr hab. inż. Andrzej Szymonik
Katedra Zarządzania Produkcją i Logistyki
Politechnika Łódzka
90-924 Łódź ul. Wólczańska 215
tel./fax 042 6370043
e-mail: andrzej.szymonik@p.lodz.pl