

Andrzej Szymonik

**ZARZĄDZANIE BEZPIECZEŃSTWEM
GOSPODARCZYM W SYSTEMIE
BEZPIECZEŃSTWA NARODOWEGO
Aspekty logistyczne**



**Monografie Politechniki Łódzkiej
Łódź 2016**

Andrzej Szymonik

Zarządzanie bezpieczeństwem gospodarczym w systemie

bezpieczeństwa narodowego. Aspekty logistyczne *Nr 2165

Andrzej Szymonik

ZARZĄDZANIE BEZPIECZEŃSTWEM
GOSPODARCZYM W SYSTEMIE
BEZPIECZEŃSTWA NARODOWEGO
Aspekty logistyczne

Monografie Politechniki Łódzkiej
Łódź 2016

Recenzenci:
prof. dr. hab. Zenon Stachowiak
prof. dr. hab. inż. Piotr Zaskórski

Redaktor Naukowy
Wydziału Organizacji i Zarządzania
prof. dr hab. inż. Jerzy Lewandowski

© Copyright by Politechnika Łódzka 2016

WYDAWNICTWO POLITECHNIKI ŁÓDZKIEJ
90-924 Łódź, ul. Wólczańska 223
tel. 42-631-29-52, 42-631-20-87, fax 42-631-25-38
e-mail: zamowienia@info.p.lodz.pl
www.wydawnictwa.p.lodz.pl

ISBN 978-83-7283-729-5

Nakład 100 egz. Ark. druk. 25. Papier offset. 80g, 70 x 100
Druk ukończono w maju 2016 r.
Wykonano w Drukarni „Quick-Druk” s.c. 90-562 Łódź, ul. Łąkowa 11
Nr 2165

Spis treści

| | |
|---|-----|
| WSTĘP | 5 |
| 1. ZARZĄDZANIE BEZPIECZEŃSTWEM GOSPODARCZYM W POLSCE | 17 |
| 1.1. Rola i miejsce bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego | 17 |
| 1.2. Idea i główne cele zarządzania bezpieczeństwem gospodarczym | 30 |
| 1.3. Determinanty i funkcje zarządzania bezpieczeństwem gospodarczym.... | 33 |
| 1.4. Zarządzanie bezpieczeństwem gospodarczym – realia polskiej polityki..... | 43 |
| 2. BEZPIECZEŃSTWO SYSTEMÓW LOGISTYCZNYCH | 47 |
| 2.1. Logistyczne uwarunkowania funkcjonowania podmiotu bezpieczeństwa | 47 |
| 2.2. Klasyfikacja zagrożeń w kontekście bezpieczeństwa systemów logistycznych | 53 |
| 2.3. Współdziałanie systemów logistycznych w czasie działań kryzysowych ... | 60 |
| 3. BEZPIECZEŃSTWO TRANSPORTU, GOSPODARKI MAGAZYNOWEJ, ŻYWNOŚCIOWE | 66 |
| 3.1. Nowe i przyszłe uwarunkowania wpływające na bezpieczeństwo transportu | 66 |
| 3.2. Determinanty bezpieczeństwa w transporcie | 76 |
| 3.3. Telematyka w bezpieczeństwie procesów transportowych | 91 |
| 3.4. Bezpieczeństwo gospodarki magazynowej | 106 |
| 3.5. Zapewnienie bezpieczeństwa żywnościowego | 118 |
| 4. EKOLOGISTYKA W SYSTEMIE BEZPIECZEŃSTWA ŚRODOWISKA NATURALNEGO | 126 |
| 4.1. System bezpieczeństwa środowiska naturalnego..... | 126 |
| 4.2. Zagrożenia ekologiczne | 132 |
| 4.3. Ekologistyka w ochronie środowiska | 146 |
| 5. TECHNOLOGIE WSPOMAGANIA ZARZĄDZANIA BEZPIECZEŃSTWEM SYSTEMÓW LOGISTYCZNYCH | 151 |
| 5.1. Informatyczne wspomaganie | 151 |
| 5.2. Elektroniczna platforma logistyczna | 163 |
| 5.3. Automatyczna identyfikacja..... | 169 |
| 5.4. Elektroniczna wymiana danych | 182 |
| 5.5. <i>Traceability</i> w logistyce | 185 |
| 5.6. Bezpieczeństwo procesów informacyjnych | 189 |

| | |
|---|------------|
| 6. MODEL ZARZĄDZANIA BEZPIECZEŃSTWEM GOSPODARCZYM I LOGISTYCZNYM NA POTRZEBY SYSTEMU BEZPIECZEŃSTWA NARODOWEGO | 208 |
| 6.1. Modelowanie systemowe w zarządzaniu i logistyce | 208 |
| 6.2. Analiza wyników badań | 231 |
| 6.3. Model zarządzania bezpieczeństwem systemów logistycznych na potrzeby logistyki bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego | 305 |
| ZAKOŃCZENIE | 314 |
| BIBLIOGRAFIA | 319 |
| ZAŁĄCZNIKI | 340 |
| WYKAZ RYSUNKÓW..... | 382 |
| WYKAZ WYKRESÓW..... | 384 |
| WYKAZ TABEL | 389 |
| WYKAZ ZAŁĄCZNIKÓW | 392 |

WSTĘP

Obecna Europa należy do kontynentu pokoju i stabilizacji życiowej, mimo różnych zagrożeń, takich jak np.: podważanie wiarygodności porozumień rozbrojeniowych, kryzys w strefie euro, różny poziom dochodu na jednego mieszkańca, nielegalna migracja, międzynarodowy terroryzm, zorganizowana przestępczość, kryzys demograficzny, cyberprzestępczość czy wzrost zapotrzebowania na energię, żywność i wodę pitną.

Polska, będąca członkiem UE, nie funkcjonuje w próżni i z każdym z tych problemów w sposób większy lub mniejszy musi się zmierzyć, a nade wszystko zapewnić bezpieczeństwo krajowi i jej obywatelom. A jest to możliwe poprzez utrzymywanie na optymalnym poziomie wymagań wynikających między innymi z *Konstytucji Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 roku, *Białej Księgi Bezpieczeństwa Narodowego* z 2013 roku, *Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022* przyjętej uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r., *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 5 listopada 2014 roku.

Bezpieczeństwo jest pojęciem szerokim i różnie definiowanym, jednak trudno się nie zgodzić, że służy ono zapobieganiu zagrożeniom, zapewnieniu warunków przetrwania, realizacji interesów przez określony podmiot, poprzez wykorzystanie skutecznego potencjału, w celu minimalizowania ryzyka oraz przeciwdziałaniu zagrożeniom dla niego i zadań, które on realizuje.

Zgodzić się należy, że bezpieczeństwo jest zjawiskiem dynamicznym, zmieniającym się w czasie, przestrzeni i wymiarze. Architektura bezpieczeństwa to wiedza, działalność praktyczna i obejmuje szerokie spektrum form i sposobów organizowania warunków dla *zapewnienia niepodległości, nienaruszalności terytorialnej, wolności, bezpieczeństwa, poszanowania praw człowieka i obywatela, a także zachowanie dziedzictwa narodowego oraz ochrona środowiska naturalnego w warunkach zrównoważonego rozwoju*¹.

W świetle wskazanych zapisów konstytucyjnych oraz analizując treści innych dokumentów można wskazać, że nadrzędnym celem Rzeczypospolitej Polskiej jest stworzyć *zintegrowany system bezpieczeństwa narodowego obejmującego zarówno jego elementy bezpieczeństwa zewnętrznego, jak i wewnętrznego. Środki polityki bezpieczeństwa, rozumiane jako zasoby i instrumenty, są generowane i używane przez państwo, a więc rozwój społeczno-gospodarczy zapewnia dostępność tych środków, a wzmocnienie bezpieczeństwa państwa (narodowego) pozytywnie wpływa, w niektórych sytuacjach wręcz warunkuje dalszy rozwój kraju. To w sposób ostateczny*

¹ Zob. *Konstytucja Rzeczypospolitej Polskiej*, Dz. U. 1997, nr 78, poz. 483 z późn. zmianami, art. 5.

przesądza o potrzebie jednoczesnego umacniania bezpieczeństwa kraju w powiązaniu z jego rozwojem społeczno-gospodarczym².

Zintegrowany to znaczy dokładnie zdefiniowany, wyszczególniający dziedziny, sektory, transsektory, podmioty realizujące zadania, a także precyzujący obszary odpowiedzialności i współdziałania w ramach bezpieczeństwa narodowego³.

Struktura bezpieczeństwa narodowego w literaturze przedmiotu wynika z przyjętego kryterium i tak np. w *Białej Księdze Bezpieczeństwa Narodowego* wyszczególniono w bezpieczeństwie narodowym: dziedziny (obrona, ochrona, społeczna, gospodarcza), sektory (w tym transektorowe), działy i podmioty⁴. A zatem możemy konstatować, że bezpieczeństwo gospodarcze, jako jedna z czterech podstawowych dziedzin bezpieczeństwa narodowego, ma za zadanie ochronę podmiotów bezpieczeństwa przed destabilizacją, dezintegracją wywołaną negatywnymi czynnikami (zagroženiami), zarówno wewnętrznymi, jak i zewnętrznymi.

Działania gospodarcze w sferze bezpieczeństwa są możliwe dzięki czynnościom instytucji i podmiotów zmierzających do wzmocnienia bezpieczeństwa finansowego, zwiększenia bezpieczeństwa energetycznego, utrzymania rezerw strategicznych, wzmocnienia bezpieczeństwa żywnościowego oraz ochrony środowiska naturalnego⁵.

Poziom bezpieczeństwa gospodarczego zależy od wielu składowych, do których możemy między innymi zaliczyć:

- współdziałanie i współpracę z pozostałymi trzema dziedzinami bezpieczeństwa narodowego;
- odporność na zakłócenia sektorów (finansowego, energetycznego, transportowego, infrastruktury, w tym infrastruktury krytycznej, środowiska naturalnego, żywnościowego, podmiotów produkcyjnych i usługowych) bezpieczeństwa gospodarczego, które należy rozpatrywać systemowo, w sposób zintegrowany, gdyż tylko wtedy możemy mówić o efekcie synergicznym, o oczekiwanym potencjale niezawodności;
- wielkość PKB, stabilność finansową, niezależność energetyczną i surowcową, zdolność magazynową, właściwą infrastrukturę, potencjał geogra-

² R. Zięba, J. Zając, *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski*, Ekspertyza, Warszawa 2010, s. 38.

³ Zob. M. Malec, *Strategiczny Przegląd Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego, Strategiczny Przegląd Obronny – ich zakres i cele*, [w:] *Bezpieczeństwo Narodowe* 2011, nr 17, ss. 118-119.

⁴ Zob. *Biała Księga Bezpieczeństwa Narodowego*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, s. 247.

⁵ Zob. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 5 listopada 2014 roku*, pkt. 100-105.

ficzny, środowisko naturalne, rolnictwo, rezerwy strategiczne, instytucje kierujące i wykonawcze w obszarze bezpieczeństwa gospodarczego;

- sprawność i skuteczność logistyki bezpieczeństwa i bezpieczeństwa systemów logistycznych.

Trudno się nie zgodzić, że efektywność funkcjonowania bezpieczeństwa gospodarczego w dużej mierze zależy od logistyki (tak często pomijanej w ważnych dokumentach dotyczących strategii bezpieczeństwa⁶), która powinna być nowoczesna, a nade wszystko odporna na wszelkie zakłócenia i zagrożenia. Ta logistyka, która ściśle jest sprzężona z podmiotami i instytucjami zaangażowanymi w system bezpieczeństwa narodowego, w literaturze przedmiotu jest nazywana jako: *logistyka bezpieczeństwa*⁷. Określenie tej logistyki ściśle jest związane ze strukturami ministerstwa: obrony narodowej, spraw wewnętrznych, zdrowia, finansów, gospodarki, rolnictwa i rozwoju wsi, transportu, budownictwa i gospodarki morskiej.

Niekwestionowany udział logistyki w bezpieczeństwie gospodarczym dotyczy przede wszystkim podmiotów z sektora transportowego, infrastruktury (magazynowej, krytycznej) i ochrony środowiska naturalnego, żywnościowego. Należy podkreślić, że logistyka jest również związana z innymi dziedzinami i sektorami bezpieczeństwa narodowego, między innymi z sektorem militarnym, z ratowniczym, z socjalnym, z prawnym i porządku publicznego.

Wyniki ekonomiczne dowolnego podmiotu bezpieczeństwa (w tym zaangażowanego w bezpieczeństwo) zależą od wielu czynników. Jednym z nich jest efektywnie zorganizowana logistyka, w której przepływ strumienia rzeczowego i towarzyszących informacji jest niezawodny oraz wyraża się użytecznością, funkcjonalnością, jakością, kompletnością, a także spójnością działania. Mówimy wtedy o dobrze zorganizowanym, w szerokim ujęciu, *bezpieczeństwie logistycznym* lub *bezpieczeństwie systemu logistycznego* w wymiarze mikro (pojedynczego podmiotu bezpieczeństwa) oraz makro (wzdłuż całego łańcucha dostaw o zasięgu krajowym czy międzynarodowym). Dzięki tak zorganizowanej logistyce czynności transportowe i składowanie, realizowanie zamówień, zaopatrywanie w części, obsługa klienta (potrzebujących, uszkodzonych), prognozowanie popytu, przepływ informacji, kontrola zapasów, czynności manipulacyjne, lokalizacja zakładów produkcyjnych, usługowych i składów, procesy zaopatrzeniowe, pakowanie, obsługa zwrotów, gospodarowanie odpadami (recyklingiem) przebiegają i funkcjonują niezawodnie (są zdolne do pełnienia przewidzianych dla nich funkcji).

Należy podkreślić, że nawet najlepiej zaplanowane działania nie dają gwarancji ich pełnej realizacji z powodu turbulencji środowiska, które to może

⁶ Zob. Załącznik 2.1.

⁷ Zob. T. Jałowicz, *Logistyczne wymiary systemu bezpieczeństwa państwa*, [w:] *Logistyka* 5/2014, s. 617 i A. Szymonik, *Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce*, [w:] *Logistyka* 2/2011, s. 7.

ulegać zmianie w wyniku zagrożeń wewnętrznych i zewnętrznych. Często nie ma możliwości przewidzenia wszystkich czynników, od których zależy bezpieczeństwo systemu logistycznego, a tym samym i bezpieczeństwo sektora (sektorów) gospodarczego. Dodatkowym utrudnieniem są problemy we wczesnym wykrywaniu zagrożeń, ich monitorowanie, określenie rodzaju, skali, możliwych konsekwencji, jakie mogą spowodować itp. Sprawia to, że opracowanie skutecznego modelu przeciwdziałania skutkom zagrożeń stanowi główne wyzwanie.

Identyfikacja zagrożeń, określenie częstotliwości ich wystąpienia, prawdopodobieństwo pojawienia się oraz przewidywane straty pozwalają na odpowiednie przygotowanie sił i środków na neutralizację negatywnych skutków i realizację zadań w ramach systemu logistycznego, zabezpieczającego określony podmiot, w granicach akceptowalnych przez interesariuszy. Należy jednak zgodzić się, że jest to problem wieloaspektowy i wielokryterialny.

Dalece problematyczne jest podjęcie decyzji dotyczących wyboru sił i środków oraz procedur, by procesy realizowane w ramach systemów logistycznych zapewniały bezpieczeństwo gospodarcze. Wynika to między innymi z faktu udzielenia odpowiedzi na szereg pytań, które pozwalają na logiczne i racjonalne rozwiązanie problemu. Do pytań tych możemy zaliczyć:

- w jakim środowisku są realizowane procesy logistyczne na rzecz bezpieczeństwa gospodarczego?
- dla kogo i w jakim celu są realizowane procesy logistyczne?
- jaki jest stopień ważności realizowanych procesów logistycznych dla podmiotu bezpieczeństwa?
- jakie są koszty zapobiegania możliwym zagrożeniom dla podmiotu bezpieczeństwa?
- jakie są koszty przygotowania systemu logistycznego na wypadek uaktywnienia się tych zagrożeń?
- jakie są koszty reagowania?
- jakie są koszty odbudowy w celu przywrócenia poprzedniego stanu?
- jakie są koszty utrzymania dodatkowych sił i środków w ramach logistyki bezpieczeństwa do zapewnienia bezkolizyjnego funkcjonowania bezpieczeństwa gospodarczego?
- w jakim stopniu są przygotowane siły i środki do reagowania na pojawiające się zagrożenia?
- jakie są koszty szkolenia?

Znajomość odpowiedzi na zaprezentowane pytania pomaga zapewnić akceptowalny poziom bezpieczeństwa systemowi logistycznemu, ale go nie gwarantuje, bowiem np. kto potrafi w czasie powodzi jednoznacznie określić, o ile zostanie przekroczony i w jakim czasie stan alarmowy oraz jakie będą ewentualne straty oraz poniesione koszty. Zasada racjonalnego gospodarowania nakazuje bilansowanie efektów z nakładami (określenie granicznego punktu rentowności), by nie okazało się, że więcej wydajemy pieniędzy na zabezpieczenie się przed wszelkimi zagrożeniami niż możemy stracić.

Należy przy tym pamiętać, że strat związanych z życiem, zdrowiem człowieka nie da się ocenić, jest to dobro nadrzędne i koszty są trudne do zobiektywizowania. Podobna jest sytuacja z bezpieczeństwem w innych dziedzinach, sektorach, podmiotach bezpieczeństwa.

Cele, główny problem badawczy, hipoteza, przedmiot i zakres badań

Cel główny monografii dotyczy identyfikacji (poznania) *stopnia wdrożenia systemów zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych oraz poznania zasad i form tych systemów, w kontekście zarządzania ciągłością działania, tak istotną z punktu widzenia zapewniania bezpieczeństwa gospodarczego.*

Natomiast do celów szczegółowych zaliczono:

C1: Identyfikacja domen bezpieczeństwa systemów logistycznych, realizujących zadania na korzyść bezpieczeństwa gospodarczego.

C2: Identyfikacja zagrożeń wpływających na funkcjonowanie bezpieczeństwa systemów logistycznych.

C3: Identyfikacja warunków funkcjonowania bezpieczeństwa systemów logistycznych w kwestiach znajomości i poziomu wdrożenia procedur prawnych, organizacyjnych, technicznych zarządzania kryzysowego, a także możliwości szkolenia w tym zakresie.

Zakłada się zrealizowanie następujących celów aplikacyjnych:

C4: Zaproponowanie narzędzi ułatwiających zapobieganie, przygotowanie, reagowanie na zagrożenia procesów logistycznych realizowanych na rzecz podmiotów (instytucji) bezpieczeństwa występujących w systemie bezpieczeństwa gospodarczego.

C5: Opracowanie modelu zarządzania bezpieczeństwem systemów logistycznych na potrzeby logistyki bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego.

Główny problem badawczy sformułowano w postaci następującego pytania: *w jakim stopniu funkcjonujący system zarządzania bezpieczeństwem systemów logistycznych zapewnia bezpieczną i niezawodną realizację zadań z zakresu bezpieczeństwa gospodarczego oraz jakie zmiany w systemie będą sprzyjać zapewnieniu bezpieczeństwa w warunkach możliwych i prawdopodobnych zagrożeń?*

Realizacja celów i problemu badawczego przyczyni się do uzupełnienia luki w literaturze przedmiotu, związanej z zarządzaniem bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego w kontekście aspektów logistycznych.

Na podstawie przedstawionego celu głównego, celów szczegółowych oraz aplikacyjnych, a także głównego problemu badawczego sformułowano hipotezę monografii (H): *z uwagi na fakt rosnącej liczby stwierdzonych naruszeń bezpieczeństwa, istnieje potrzeba zmian w systemie zarządzania bezpieczeństwem logistycznym, z wiodącą rolą instytucjonalnych rozwiązań opartych o przepisy prawa, standardów i ich korelacji z wewnętrznymi uregulowaniami.*

Przedmiotem badań były systemy logistyczne oraz uwarunkowania ich funkcjonowania z uwzględnieniem ewentualnych zagrożeń, mogących naruszyć poziom bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego. Funkcjonowanie systemów w kontekście zapewnienia akceptowanego poziomu bezpieczeństwa gospodarczego było badane w:

- nowoczesnych firmach, między innymi z Żnina k/Bydgoszczy, Strykowa k/Łodzi, Mysłowic, Zabierzowa k/Krakowa, Ozorkowa k/Łodzi, Wrocławia, Grójca k/Warszawy, a także z uzyskanych danych z przedsiębiorstw w Niemczech i krajach Skandynawskich, współpracujących z nimi;
- jednostkach podległych Ministerstwu Spraw Wewnętrznych (Policji, Państwowej Straży Pożarnej);
- administracji rządowej i samorządowej.

Charakterystyka wybranych firm znajduje się w załączniku 1.

Zakres przestrzenny monografii wyznacza obszar funkcjonowania wybranych systemów logistycznych realizujących zadania w podmiotach, na terenie kraju w relacjach z innymi, krajowymi, jak i poza granicami.

Natomiast zakres czasowy rozważań monografii został ograniczony do dwóch pierwszych dekad XXI wieku, to jest okresu, w którym dokonują się istotne zmiany w gospodarce i instytucjach rządowych oraz samorządowych.

Metoda badawcza i użyte narzędzia

Do zrealizowania celów (głównego, szczegółowych, aplikacyjnych), weryfikacji przyjętych hipotez (monografii i szczegółowych) zastosowano metody teoretyczne i empiryczne w ujęciu systemowym. Spowodowało to możliwość skoncentrowania się na zarządzaniu bezpieczeństwem systemu logistycznego, pomijając jego poszczególne podsystemy.

Teoretyczne metody badawcze obejmowały analizę literatury przedmiotu, analizę porównawczą, uogólnienia, syntezy i wnioskowania itp.

Analiza literatury pozwoliła uzyskać teoretyczne podstawy badań empirycznych, warunkowała także syntezę. Umożliwiła określenie aktualnego stanu wiedzy i czynników wpływających na jakość funkcjonowania zarządzania bezpieczeństwem systemu logistycznego.

Metoda porównania pomogła wskazać cechy wspólne i różnice pomiędzy systemami logistycznymi różnych podmiotów funkcjonujących w systemach militarnych, niemilitarnych i gospodarczych. Dało to podstawę do przewidywania dalszego kierunku rozwoju badanego zjawiska oraz przyszłych możliwych przemian i stanów.

Synteza umożliwiła określenie związków i zależności przeprowadzonych badań i była pomocna we właściwej interpretacji uzyskanych wyników badań. Ponadto przyczyniła się do ujęcia całościowego problemu badawczego poprzez powiązanie faktów szczegółowych z jednoczesnym częściowym odrzuceniem niektórych z nich i z uogólnieniem innych, a także do precyzyjnego sformułowania wniosków.

Zastosowanie metod empirycznych polegało przede wszystkim na badaniu sądów i opinii metodą pośrednią oraz bezpośrednią za pomocą kwestionariusza ankietowego, który zawierał 18 pytań, w tym 16 zamkniętych i 2 otwarte (załącznik 2). Kwestionariusze zostały wysłane do 168 różnych firm, z czego zwrotnie otrzymano 92: 4 z mikro, 24 z małych, 29 ze średnich i 35 z dużych.

Dodatkowo, w celu zweryfikowania wyników badań, przeprowadzono pięć rozmów z ekspertami, logistykami dużych firm prywatnych i państwowych w oparciu o materiały zgromadzone w kwestionariuszu. Miały one również na celu zebranie uzupełniających opinii o aktualnym stanie zarządzania bezpieczeństwem systemów logistycznych w celu zapewnienia akceptowanego poziomu realizowanych przez nie zadań na rzecz podmiotu bezpieczeństwa.

W monografii wykorzystano szeroki i różnorodny zbiór materiałów źródłowych zarówno krajowych, jak i zagranicznych (głównie anglojęzycznych). Bibliografia obejmuje książki (monografie), artykuły umieszczone w czasopismach i zeszytach naukowych, akty normatywne i dokumenty oraz źródła internetowe.

Struktura monografii została podzielona na logicznie następujące po sobie bloki merytorycznych wywodów.

Pierwszym elementem jest wstęp, który składa się z wprowadzenia i opisu wybranych kategorii i zarysowuje ogólne tło badanych problemów oraz wskazuje przesłanki wyboru tematu badań. Zaprezentowany jest zarys metodologiczny podejmowanych w monografii problemów oraz wskazany jest sposób prezentacji wyników z przeprowadzonych dociekań. Opisane wybrane kategorie pojęciowe ułatwiają jednoznaczną interpretację rozważanych problemów naukowych.

Blok drugi (rozdział pierwszy i drugi) skupia się na zarządzaniu bezpieczeństwem gospodarczym w Polsce i bezpieczeństwem systemów logistycznych. Pokazane są determinanty i funkcje zarządzania bezpieczeństwem w kontekście zagrożeń i logistycznych uwarunkowań.

Trzeci blok (rozdział trzeci i czwarty) zawiera merytoryczne analizy problemów bezpieczeństwa w takich sektorach jak transport (samochodowy i kolejowy), infrastruktura (magazynowa), ochrona środowiska i żywność. Pokazane są nowe i przyszłe uwarunkowania wpływające na bezpieczeństwo wybranych sektorów bezpieczeństwa gospodarczego.

Czwarty blok (rozdział piąty i szósty) to pragmatyczne podejście do zarządzania bezpieczeństwem systemów logistycznych na potrzeby bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego. Zostały zaprezentowane nowoczesne narzędzia informatyczne, które można i trzeba wykorzystywać w celu poprawy bezpieczeństwa w logistyce. Zaprezentowany model zarządzania bezpieczeństwem systemów logistycznych na potrzeby podmiotów jest nowatorskim ujęciem tego problemu.

Monografię finalizuje zakończenie, w którym dokonano syntetycznego podsumowania badań związanych z zarządzaniem bezpieczeństwem gospo-

darczym w systemie bezpieczeństwa narodowego w kontekście nowoczesnej logistyki.

Monografia *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne* stanowi innowacyjne ujęcie podstawowych problemów bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego w kontekście współczesnych systemów logistyki. Jest wyrazem holistyczno-systemowego ujęcia problemowych obszarów wiedzy bezpieczeństwa gospodarczego (ekonomicznego) i logistyki w systemie bezpieczeństwa narodowego. Zaprezentowana monografia stanowi zatem kompleksowe połączenie bezpieczeństwa gospodarczego i działań logistycznych w systemie bezpieczeństwa narodowego.

Monografia może być bardzo dobrym źródłem informacji i wiedzy dla studentów kierunku kształcenia bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, inżynieria bezpieczeństwa i logistyka, słuchaczy studiów podyplomowych, a także dla instytucji zajmujących się bezpieczeństwem oraz organizacji (instytucji) uczestniczących w logistycznym zabezpieczeniu podmiotów bezpieczeństwa.

Wybrane kategorie pojęciowe

Obszar bezpieczeństwa⁸

Podmiot bezpieczeństwa – każdy świadomie istniejący i celowo działający podmiot (indywidualny lub zbiorowy), analizowany z punktu jego bezpieczeństwa. Tym podmiotem może być przedsiębiorstwo produkcyjne, usługowe, transportowe, infrastruktura (w tym krytyczna), środowisko, instytucja publiczna, prywatna itd.

Bezpieczeństwo – teoria i praktyka, która zapewnia możliwości przetrwania (egzystencji) i realizacji własnych interesów przez dany podmiot, w szczególności poprzez wykorzystanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawienie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów.

Interesy podmiotu bezpieczeństwa – to zsyntetyzowane oczekiwania podmiotu wobec otoczenia wynikające i kształtowane przez jego tożsamość, wyznawane wartości, historyczny dorobek, tradycje, bieżące potrzeby oraz dążenia i aspiracje przyszłościowe. Można wyróżnić interesy żywotne (dotyczące istnienia podmiotu) i pożądane (związane z jakością owego istnienia, trwania).

Środowisko bezpieczeństwa – zewnętrzne i wewnętrzne, militarne i niemilitarne (cywilne) warunki bezpieczeństwa (warunki realizacji interesów danego podmiotu w dziedzinie bezpieczeństwa i osiągnięcia ustalonych przezeń

⁸ Kategorie pojęciowe zostały przedstawione w oparciu o *Białą Księgę Bezpieczeństwa Narodowego*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, ss. 247 i 248.

celów w tym zakresie), charakteryzowane za pomocą podstawowych kategorii, jakimi są szanse, wyzwania, ryzyka i zagrożenia.

Szanse bezpieczeństwa – niezależnie od woli podmiotu, okoliczności (zjawiska i procesy w środowisku bezpieczeństwa) sprzyjające realizacji interesów, osiągnięciu celów podmiotu w dziedzinie bezpieczeństwa.

Wyzwania bezpieczeństwa – sytuacje problemowe generujące dylematy decyzyjne, przed jakimi staje podmiot w rozstrzyganiu spraw bezpieczeństwa. Niewłaściwie zaadresowane lub niepodjęte wyzwania bezpieczeństwa mogą w efekcie przekształcić się w realne zagrożenia bezpieczeństwa.

Zagrożenie bezpieczeństwa – pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot. Najbardziej klasyczny czynnik środowiska bezpieczeństwa; różni się zagrożenia potencjalne i realne; subiektywne i obiektywne; zewnętrzne i wewnętrzne; militarne i niemilitarne; intencjonalne, przypadkowe i losowe.

Ryzyka bezpieczeństwa – możliwości negatywnych dla danego podmiotu skutków własnego działania w sferze bezpieczeństwa.

Bezpieczeństwo informacyjne – obrona informacyjna, która polega na uniemożliwieniu oraz utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania oraz utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych.

Logistyka

System logistyczny jest pojęciem wieloaspektowym, jako że funkcjonuje on w warunkach złożonych, które powodują potrzebę⁹:

- wyodrębnienia systemu z otoczenia – system logistyczny jest postrzegany jako pewna całość, która znajduje się w określonych wzajemnych relacjach z otoczeniem (np. rynkiem dostawców i odbiorców), przy czym nakładając ograniczenia na system oraz precyzując relacje z otoczeniem, system zachowuje pewną autonomię;
- budowy systemu logistycznego z elementów (podsystemów) – wyróżnione elementy systemu logistycznego (np. podsystem zaopatrywania, produkcji, dystrybucji, transportu, utylizacji) oddziałują na siebie wzajemnie, w środowisku turbulentnym, przy czym oddziaływania te mają istotny wpływ na własności systemu jako całości;
- określenia funkcji spełnianej przez system logistyczny – zadanie, które jest realizowane przez system stanowi podstawę do traktowania go jako całości, przy czym system logistyczny jako całość jest zdolny do realizowania założonej funkcji oraz spełniania celu jego działania;

⁹ Por. D. Pyza, *Modelowanie systemów przewozowych w zastosowaniu do projektowania obsługi transportowej podmiotów gospodarczych*, PW, Warszawa 2012, s. 9.

- uwzględnienia ograniczonej zmienności systemu w czasie i przestrzeni – system podlega większym lub mniejszym zmianom w czasie i przestrzeni, planowym i nieplanowym, jednak zachowuje on pewne właściwości podstawowe, mianowicie swoją istotę wynikającą z definicji logistyki, czyli zapewnienie użyteczności miejsca i czasu na wyroby i usługi.

System logistyczny dowolnego systemu gospodarczego¹⁰ (podmiotu bezpieczeństwa) można zdefiniować jako celowo wyodrębnioną całość składającą się z podsystemów (takich jak np. zaopatrzenia, produkcji, dystrybucji, magazynowania, transportu, utylizacji), powiązanych relacjami fizycznymi (np. transport) oraz niematerialnymi (np. wzajemnym zaufaniem, wielostronnymi ustaleniami) między sobą i otoczeniem w sposób umożliwiający swobodny przepływ strumienia rzeczowego i informacji lub uporządkowany zbiór, złożony z organów kierowania oraz komórek i urzędzeń wykonawczych dysponujących środkami zaopatrzenia i sprzętem technicznym, powiązanych relacjami służbowymi i funkcjonalnymi, przeznaczony do zabezpieczenia realizacji dostaw i świadczenia usług.

W systemie logistycznym można wyróżnić dwa podsystemy, od których zależy jakość realizowanych procesów, a mianowicie: *system* i *otoczenie*, które oddziałują wzajemnie na siebie poprzez wielkości wejściowe do systemu, zwane bodźcami oraz wielkości wyjściowe z systemu, zwane reakcjami. Ponadto wpływ otoczenia na system często odbywa się przez różnego rodzaju zakłócenia oraz wielkości sterujące. Zakłócenia systemu są niezależne od wielkości sterujących i charakteryzuje je jedynie to, co nazywane jest niepewnością, która może być związana z zagrożeniami, wywołanymi celowymi (niecelowymi) działaniami człowieka i przyrody.

Niepewność funkcjonowania systemu logistycznego dowolnego systemu gospodarczego (podmiotu bezpieczeństwa) jest związana ze złożonością realizowanych procesów logistycznych; zmiennością środowiska wykonywanych zadań; możliwymi, zewnętrznymi (otoczenia) i wewnętrznymi (systemu) zagrożeniami realizacji procesów logistycznych; przygotowaniem podmiotu na reagowanie na ewentualne pojawiające się trudności czy zakłócenia; przewidywaniem, wykrywaniem, monitorowaniem, oceną zagrożeń i ich wpływem na funkcjonowanie systemu logistycznego; opracowaniem skutecznych przedsięwzięć, które należy zrealizować by zapewnić pożądany poziom bezpieczeństwa funkcjonowania systemu logistycznego; losowym charakterem

¹⁰ System gospodarczy jest to każdy, otwarty, dynamiczny system społeczno-techniczny, realizujący określone cele gospodarcze w sferze wytwórczej (koncerny, przedsiębiorstwa jedno i wielozakładowe, spółki, spółdzielnie, gospodarstwa domowe) i usługowej (banki, poczta, szkoły i uczelnie, wojsko i policja), urzędy administracji państwowej i samorządowej, jednostki świadczące usługi konserwacyjno-naprawcze, osoby fizyczne.

zjawisk „systemu” i „otoczenia” wpływających na procesy realizowane w ramach systemów logistycznych; oszacowaniem kosztów itp.

Logistyczny system transportowy to zorganizowany i zsynchronizowany sposób fizycznego przemieszczania osób, dóbr materiałowych (usług) z punktu odprawy (nadania) do punktu przeznaczenia, wykorzystujący układ komunikacyjny (podsystem bierny) wypełniany inwestycjami transportowymi (podsystem czynny).

Logistyczny systemem magazynowania to skoordynowana działalność w czasie i przestrzeni, polegająca na gromadzeniu zapasów, ich składowaniu wraz z czynnościami manipulacyjnymi, pielęgnacyjnymi oraz kontrolą. Działalność ta jest prowadzona z wykorzystaniem całej infrastruktury magazynowej.

Logistyczny system obsługi klienta (potrzebującego) – to pełna realizacja zamówienia, kontakty z nabywcą, wysyłka, transport, pełna obsługa posprzedażna (powysyłkowa).

Łańcuch dostaw – to sieć powiązanych i współzależnych podmiotów bezpieczeństwa (systemów gospodarczych), które działając na zasadzie wzajemnej współpracy, wspólnie kontrolują, kierują i usprawniają przepływy rzeczowe i informacji od dostawców do ostatecznych użytkowników.

Zagrożenie bezpieczeństwa systemu logistycznego – to każda sytuacja (działanie, zdarzenia, zjawisko, proces) niepożądane i mające negatywny wpływ na przebieg strumienia rzeczowego i informacji w łańcuchu dostaw.

Logistyka bezpieczeństwa (logistyka w bezpieczeństwie) – to wiedza i umiejętności potrzebne do kształtowania (planowania, przygotowania) racjonalnych strumieni rzeczowych i związanych z nimi strumieni informacji oraz projektowania (konfigurowania i wymiarowania) procesów przepływu materiałów i informacji w celu zaspokojenia potrzeb na rzecz wszystkich podmiotów (instytucji) bezpieczeństwa występujących w systemie bezpieczeństwa narodowego (w tym gospodarczego) przy racjonalnych nakładach i kosztach.

Bezpieczeństwo logistyki, teoria i praktyka, która zapewnia przepływ strumienia rzeczowego i towarzyszących informacji, na rzecz podmiotu bezpieczeństwa, w szczególności poprzez wykorzystanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukcja ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawienie się) wszelkiego rodzaju zagrożeniom dla działań logistycznych.

Zarządzanie logistyką bezpieczeństwa – zestaw skoordynowanych działań, skierowanych na zbiór zasobów i łączących ich relacji, których celem jest przepływ zaplanowanego oraz zorganizowanego strumienia rzeczowego, a także usług logistycznych na korzyść podmiotów bezpieczeństwa.

Bezpieczeństwo systemu logistycznego – zapewnienie, na określonym poziomie, możliwości realizacji funkcjonujących procesów logistycznych

w dowolnym podmiocie (instytucji) bezpieczeństwa, w konkretnych warunkach, poprzez wykorzystywanie okoliczności sprzyjających (nowych technologii IT, nisz rynkowych, dogodnych systemów podatkowych itd.), podejmowanie wyzwań biznesowych, redukcja ryzyka, niepewności oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla działań logistycznych.

1. ZARZĄDZANIE BEZPIECZEŃSTWEM GOSPODARCZYM W POLSCE

Bezpieczeństwo gospodarcze, różnie definiowane, jest traktowane jako jedna z czterech podstawowych dziedzin bezpieczeństwa narodowego, obok obronnej, ochronnej i społecznej. Zadaniem nadrzędnym bezpieczeństwa gospodarczego jest ochrona podmiotów bezpieczeństwa przed destabilizacją wywołaną zagrożeniami, zarówno wewnętrznymi, jak i zewnętrznymi. Poziom bezpieczeństwa gospodarczego jest funkcją wielu składników. Do nich możemy zaliczyć: skuteczność i efektywność zarządzania, odporność na zakłócenia sektorów bezpieczeństwa gospodarczego, wielkość zgromadzonych zasobów materialnych i ludzkich. I w tym miejscu należy się również zgodzić, że niekwestionowany udział w bezpieczeństwie gospodarczym przypada logistyce.

1.1. Rola i miejsce bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego

W występujących obecnie uwarunkowaniach i perspektywach rozwojowych koniecznością staje się patrzeć na bezpieczeństwo i stabilność poszczególnych krajów przez pryzmat czynników gospodarczych, tworzących w swej istocie strukturalnie środowisko bezpieczeństwa gospodarczego/ekonomicznego. Wszeghogniający determinizm czynnika ekonomicznego sprawia, że metody i sposoby zapewnienia krajowi bezpieczeństwa gospodarczego stały się fundamentem polityki bezpieczeństwa narodowego wszystkich rozwiniętych państw świata, a co za tym idzie wiodącą stała się problematyka sprawnego i efektywnego zarządzania tym obszarem (dziedziną) bezpieczeństwa ogólnego.

Przystępując do identyfikacji istoty, miejsca i roli bezpieczeństwa gospodarczego w ogólnym systemie bezpieczeństwa narodowego, czy też bardziej instytucjonalnie ujmując bezpieczeństwie państwa, logicznym krokiem metodologiczno-merytorycznym staje się konieczność stosunkowo precyzyjnego uchwycenia sedna kategorii bezpieczeństwo i bezpieczeństwo narodowe/państwowe.

Najogólniej ujmując, „bezpieczeństwo” we współczesnych poglądach, zarówno teoretyków, jak i praktyków życia codziennego w jego różnych wymiarach kształtowania coraz częściej jest ujmowane w kategoriach: zagrożeń wartości chronionych (czyli sposób określania celu) oraz przeciwdziałań zmierzających do redukcji zagrożeń lub ograniczenia skutków destrukcyjnych oddziaływań (czyli odpowiednich działań i nakładów zapewniających pożądany stan). Stąd też można powiedzieć, że zagrożenia są nieodłącznym elementem zarówno negatywnej, jak i pozytywnej interpretacji bezpieczeństwa, a stan bezpieczeństwa jest zawsze albo wypadkową, albo kompromisem pomiędzy

potrzebami związanymi z kształtowaniem pożądanego stanu a możliwościami ich zaspokojenia.

Definicje słownikowe „bezpieczeństwo” określają jako ...*stan niezagrażenia, spokoju, pewności*¹¹ oraz zagrożeń, czyli bycia niebezpiecznym dla kogoś lub czegoś¹². Takie podejście do *bezpieczeństwa* uwypukla dwa główne jego aspekty postrzegania, tzn.¹³: brak zagrożenia oraz poczucie pewności albo ochronę przed nim.

Dla pełnego zrozumienia i dogłębnej analizy istoty bezpieczeństwa celowe jest dodanie przymiotników obu tym kategoriom, co sprawia, że stają się one bardziej skonkretyzowane i zawężone przez wskazanie kogo lub czego dotyczą (wskazanie podmiotu lub przedmiotu).

Na przykład wskazując podmiot, można wyróżnić np. bezpieczeństwo osobiste, bezpieczeństwo państwa, bezpieczeństwo narodowe.

Odnosząc zaś bezpieczeństwo do ujęcia przedmiotowego, wypada wspomnieć o np. bezpieczeństwie politycznym, technicznym, militarnym, społecznym, ekonomicznym itd. Oczywiście jest, że bezpieczeństwo może być także konkretyzowane poprzez zagrożenia (przedmiot oddziaływań i cechy źródeł zagrożeń)¹⁴. Powstaje dzięki temu szereg nowych (szczegółowych) grup (kategorii, topologii) bezpieczeństwa¹⁵.

Rozumienie bezpieczeństwa zmienia się również w zależności od charakteru nauki wyznaczającej perspektywy badawcze. Najbardziej przydatnymi, z punktu widzenia rozważanych w pracy problemów, są spojrzenia na bezpieczeństwo przez pryzmat obszaru wiedzy nauk społecznych, ścisłych, przyrodniczych i technicznych – rys. 1.1.

Nauki społeczne, dające całościowe spojrzenie na rzeczywistość, pokazują bezpieczeństwo w jego złożoności i wielopłaszczyznowej zależności. Bezpieczeństwo traktowane jest jako dobro o podstawowym znaczeniu dla ludzi i ich zbiorowości.

Nauki ścisłe pozwalają precyzyjnie definiować, opisywać, przeprowadzać naukowe eksperymenty, symulacje, modelować zjawiska związane z bezpieczeństwem. W tym celu wykorzystuje się przede wszystkim statystykę, probabilistykę, informatykę.

Nauki przyrodnicze zajmują się badaniem różnych aspektów świata materialnego, ożywionego i nieożywionego. W postrzeganiu bezpieczeństwa eksponują kwestie przystosowywania się organizmów do zmieniających się

¹¹ *Słownik języka polskiego*, red. M. Szymczak, PWN, Warszawa 1978, t. 1, s. 147.

¹² Tamże, t. 3, s. 907.

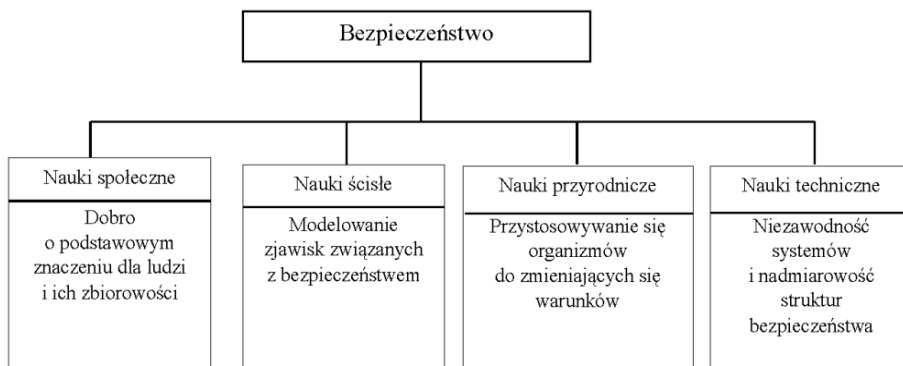
¹³ W najbardziej dosłownym znaczeniu bezpieczeństwo jest rzeczywiście identyczne z pewnością (*Safety*) i oznacza brak zagrożenia (*Danger*) fizycznego albo ochronę przed nim (*A Dictionary of the Social Sciences*, London 1964, s. 629).

¹⁴ Zob. P. Sienkiewicz, *Teoria i inżynieria bezpieczeństwa systemów*, [w:] *Inżynieria systemów bezpieczeństwa*, red. nauk. P. Sienkiewicz, PWE, Warszawa 2015, ss. 10, 11.

¹⁵ Szerzej zostało opisane w podrozdziale 2.2.

warunków i zmianę formy istnienia, czyli skoków jakościowych pozwalających uzyskać inną, lepszą, formę istnienia (bezpieczeństwa) lub dających przewagę nad innymi w środowisku¹⁶.

Nauki techniczne badają zjawiska i ustalają prawidłowości, jakie zachodzą w świecie wytworów i procesów powstałych w wyniku technicznej działalności człowieka. Przy postrzeganiu bezpieczeństwa kładzie się nacisk na kwestie niezawodności systemów i nadmiarowość struktur bezpieczeństwa¹⁷.



Rys. 1.1. Bezpieczeństwo w kontekście obszaru wiedzy nauk społecznych, ścisłych, przyrodniczych, technicznych

Źródło: opracowanie własne.

Podstawowe znaczenie w analizie systemowej charakteru i istoty bezpieczeństwa gospodarczego/ekonomicznego ma obszar wiedzy nauk społecznych. Pozostałe nauki i ich dorobek są instrumentami i narzędziami, które pozwalają zrozumieć zachodzące procesy w bezpieczeństwie (akceptować lub je zmieniać), dokładnie je definiować. Nauki ścisłe, przyrodnicze i techniczne pozwalają na określenie jego pożądanych cech i kształtu (np. formy czy warunków skuteczności zastosowanych środków).

Obszar nauk społecznych (w tym dziedziny: nauki społeczne, ekonomiczne i prawne) nakazują, by bezpieczeństwo, w tym bezpieczeństwo narodowe/ państwa w jego różnych wymiarach, postrzegać jako kategorię o dwoistym charakterze, która jest z jednej strony potrzebą, a z drugiej strony dobrem (zasadniczo o charakterze publicznym).

¹⁶ Por. J. Świniarski, *O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych*, Wyd. ULMAK, Warszawa-Pruszków 1997, ss. 122-128.

¹⁷ Por. I. Jaźwiński, K. Ważyńska-Fiok, *Bezpieczeństwo systemów*, PWN, Warszawa 1993.

Bezpieczeństwo jako potrzeba wyraża wartości i cele, które na poziomie państwa/narodu określają jego rację stanu. Prawdłowo rozumiane i wyartykułowane przyjmują formę doktryny (czy też strategii) bezpieczeństwa.

Z kolei bezpieczeństwo jako dobro publiczne oznacza dostarczenie środków o takich właściwościach, których użycie powoduje zaspokojenie odczuwanej potrzeby na określonym poziomie¹⁸. Przykładowo, bezpieczeństwo militarne jest zapewniane dzięki pewnej wielkości uzbrojenia i sprzętu oraz utrzymaniu i wyszkoleniu armii. Bezpieczeństwo państwa jest swoistym dobrem, z którego korzystają wszyscy obywatele kraju i przynosi korzyści zewnętrzne w postaci niepodzielnej konsumpcji.

W naukach społecznych wyróżniamy dwa nurty rozważań nad bezpieczeństwem i jego istotą, nurt tzw. personalny oraz nurt strukturalny. Jeżeli pierwszy cechuje się bezpośrednim, indywidualnym, jednostkowym charakterem bezpieczeństwa, to w przypadku drugiego bezpieczeństwo jest realizowane w strukturach społecznych i państwowych, czyli posiada wymiar pośredni – społeczny i globalny¹⁹.

Przenosząc analizy na płaszczyznę narodu/państwa stwierdzić można, że bezpieczeństwo narodowe jest rozumiane jako *stan świadomości społecznej, w którym istniejący poziom zagrożeń, dzięki posiadanym zdolnościom obronnym, nie budzi obaw, lęku o zachowanie (osiągnięcie) uznanych wartości²⁰, poczucie pewności państwa w środowisku międzynarodowym, brak jego zagrożenia oraz ochronę przed zagrożeniem²¹, stan uzyskany w wyniku odpowiednio zorganizowanej obrony i ochrony przed zagrożeniami zewnętrznymi i wewnętrznymi określany stosunkiem potencjału obronnego do skali zagrożeń²², czy też stan równowagi między zagrożeniem wywołanym możliwością zaistnienia konfliktu a potencjałem obronnym²³.*

Zaprezentowana analiza i treści zawarte w literaturze przedmiotu pozwalają stwierdzić, że bezpieczeństwo narodowe to z jednej strony najwyższa wartość, z drugiej zaś potrzeba i priorytetowy cel działalności państwa, grup społecznych i jednostek. To również „proces obejmujący różnorodne środki, gwarantujący trwałą, wolny od zakłóceń byt i rozwój państwa, w tym ochronę i obronę państwa jako instytucji społecznej oraz ochronę jednostek i całego społec-

¹⁸ Por. P.A. Samuelson, W.D. Nordhaus, *Ekonomia 2*, PWN, Warszawa 1998, s. 237.

¹⁹ Por. S. Kurek, S.T. Kurek, Z. Stachowiak, *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej*, AON, Warszawa 2004, s. 9.

²⁰ Por. C. Rutkowski, *Bezpieczeństwo i obronność: strategie – koncepcje – doktryny*, AON, Warszawa 1995, s. 30.

²¹ *Leksykon pokoju*, Krajowa Agencja Wydawnicza, Warszawa 1987, s. 29.

²² Por. *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002, s. 10.

²³ Por. W. Stankiewicz, *Bezpieczeństwo narodowe a walki niezbrojne*, Studium, Warszawa 1991, s. 73.

czeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie i godzą w dobra podlegające szczególnej ochronie²⁴.

Przedstawione rozumienie bezpieczeństwa narodowego jest niezwykle przydatne do opisu istoty bezpieczeństwa gospodarczego państwa i jego umiejscowienia w całym systemie bezpieczeństwa państwowego i bytu społeczno-politycznego.

Przechodząc zatem do identyfikacji kategorii bezpieczeństwa gospodarczego (ekonomicznego) państwa, zauważamy studiując literaturę przedmiotu, że ewolucja pojęcia bezpieczeństwa ekonomicznego państwa podążała za zmianami zakresu przedmiotowego pojęcia bezpieczeństwa ogólnego i bezpieczeństwa państwa²⁵. Początkowo jego zakres był wyznaczany przez pojmowanie bezpieczeństwa państwa głównie w kategoriach militarnych i politycznych. Następnie, szczególnie pod wpływem wyraźnego zdefiniowania bezpieczeństwa państwa jako problemu ekonomicznego²⁶ (głównie w kontekście efektywnej alokacji zasobów wynikającej między innymi z rozwoju logistyki), wzrosła świadomość wagi gospodarki jako względnie samodzielnego segmentu bezpieczeństwa, zmieniając tym samym sposób postrzegania bezpieczeństwa ekonomicznego.

Pojęcie bezpieczeństwa gospodarczego (ekonomicznego) odzwierciedla w sobie nie tylko pewien stan zgodności określonych wielkości ekonomicznych (tak makro, jak i mikro), ale również liczne pola zagrożeń, których ograniczenie czy też pokonanie wymaga wysiłku całego społeczeństwa. Pola zagrożeń dają się rozpoznać zarówno jako efekt działań ze strony państw, których one dotyczą, jak również jako te, które wynikają z rozwoju i funkcjonowania gospodarki światowej²⁷.

Wzrost znaczenia segmentu ekonomicznego w strukturze ogólnego bezpieczeństwa państwa jest, jak się okazuje, efektem zmian w jego postrzeganiu. Spośród wielu determinantów wpływających na jego percepcję do najistotniejszych zaliczyć wypada:

²⁴ Tamże, s. 29.

²⁵ Por. J. Świniarski, *O naturze ...*, op. cit.; M. Cieślarczyk, *Teoretyczne, metodologiczne i praktyczne aspekty zarządzania bezpieczeństwem w pierwszej dekadzie XXI wieku*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, red. M. Lisiecki, WSzZiP, Warszawa 2008; *Bezpieczeństwo państwa*, red. nauk. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza Aspra-Jr, Warszawa 2009.

²⁶ Por. Z. Stachowiak, *Teoria i praktyka mechanizmu bezpieczeństwa ekonomicznego państwa Ujęcie instytucjonalne*, AON, Warszawa 2012, s. 45.

²⁷ E. Frejtag-Mika, Z. Kołodziejak, W. Putkiewicz, *Bezpieczeństwo ekonomiczne we współczesnym świecie*, Wyd. Politechniki Radomskiej im. K. Pułaskiego, Radom 1996, s. 8.

- zmianę struktury zagrożeń bezpieczeństwa międzynarodowego wynikającego z zakończenia epoki zimnej wojny i wynikającego stąd zakresu pojmowania bezpieczeństwa państwa, wskutek czego narastała świadomość wagi gospodarki jako względnie samodzielnego segmentu bezpieczeństwa (np. skutki sankcji gospodarczych, kryzysu finansowego²⁸, migracji);
- zmianę teleologii (celów) bezpieczeństwa – od woli przetrwania do ochrony dobrobytu kraju i obywateli oraz zapewnienia warunków rozwoju;
- wzrost zależności pomiędzy bezpieczeństwem pojedynczego państwa a bezpieczeństwem realizowanym w ramach ugrupowań integracyjnych typu społeczno-ekonomicznego i sojuszy o charakterze polityczno-militarnym.

Pomimo znaczącego dorobku na polu definiowania bezpieczeństwa gospodarczego, nie ma jeszcze ostatecznych, jednolitych rozstrzygnięć co do istoty treści i zakresu przedmiotowego tego bezpieczeństwa na różnych szczeblach gospodarowania – od poziomu podmiotów gospodarczych i sektorów gospodarki, do poziomu państwa i ugrupowania integracyjnego²⁹. Stąd problemy związane z rozumieniem bezpieczeństwa ekonomicznego zaczynają się już na etapie definiowania i ustalenia zakresu pojęciowego tej kategorii. Pomijając inne kwestie, trzeba zwrócić uwagę na różnice w zakresie przedmiotowym, a w konsekwencji także określenia płaszczyzn bezpieczeństwa w sferze gospodarczej, bezpieczeństwa ekonomicznego państwa. W tym obszarze da się wyróżnić dwa stanowiska: zawężone i szerokie.

Stosunkowo wąskie rozumienie bezpieczeństwa ekonomicznego prowadzi do ograniczenia przedmiotu badań. Jego treść przedstawia myśl, że *...istota kategorii bezpieczeństwa ekonomicznego będzie polegać, z jednej strony na zapewnieniu niezakłóconego funkcjonowania gospodarki, z drugiej na utrzymaniu komparatywnej równowagi z gospodarkami innych państw*³⁰.

Powyższe ujęcie jest przydatne, kiedy bezpieczeństwo ekonomiczne rozpatruje się tylko przez pryzmat bezpieczeństwa gospodarki, bez uwzględniania świadczeń, które musi ona ponosić na rzecz innych segmentów bezpieczeństwa państwa.

Szersze zrozumienie istoty bezpieczeństwa ekonomicznego/gospodarczego umożliwi analiza przytoczonych definicji:

²⁸ F.S. Mishkin, *Global financial instability: framework, events, issues, journal of economic perspective*, [w:] *Journal of Economic Perspectives*, 1999, vol. 13, no. 4, ss. 3-20.

²⁹ Por. B. Stevens, *The Emerging Security Economy: An Introduction*, [w:] *The Security Economy*, OECD, OECD Publications, Paris 2004, ss. 7-16.

³⁰ Por. K.M. Księżpolski, *Ekonomiczne zagrożenia bezpieczeństwa państw. Metody i środki przeciwdziałania*, Wyd. Kolor Plus, Warszawa 2004, s. 20.

- *bezpieczeństwo ekonomiczne kraju wyraża się w zdolności gospodarki do suwerennego przewycięzania skutków wynikających z ekspansji napięć w międzynarodowych stosunkach ekonomicznych*³¹;
- *przez bezpieczeństwo ekonomiczne w kontekście ekonomiki obrony rozumiemy równowagę między siłą zagrożenia gospodarki obronnej a reakcją na to zagrożenie*³²;
- *pojęcie bezpieczeństwa ekonomicznego służy do określenia przedsięwzięć podejmowanych w płaszczyźnie gospodarczej, mających zapewnić względną swobodę kształtowania procesów gospodarczych zgodnie z interesami narodu (państwa)*³³;
- *międzynarodowe bezpieczeństwo ekonomiczne stanowi wyobrażenie stopnia efektywności zewnętrznej ingerencji w trzy zasadnicze sfery, decydujące o łącznym bezpieczeństwie kraju: rozwój gospodarczy, stabilność przyjętego systemu społeczno-politycznego oraz potencjał obronny*³⁴;
- *bezpieczeństwo ekonomiczne wyraża stopień podatności danego kraju na przeniesienie przez płaszczyznę gospodarczą, głównie przez transmisję kanałami i mechanizmami zależności ekonomicznych, działań gospodarczych o charakterze politycznym, skierowanych na osłabienie bezpieczeństwa kraju*”;
- *bezpieczeństwo ekonomiczne to zdolność systemu gospodarczego państwa do niezagrażonego rozwoju – oznacza ono brak zewnętrznych i wewnętrznych zagrożeń gospodarczych*³⁵;
- *bezpieczeństwo ekonomiczne jest równoznaczne z utrzymaniem na odpowiednim poziomie bogactwa i potęgi państwa przez dostęp do zasobów, finansów i rynku*³⁶;
- *bezpieczeństwo ekonomiczne państwa jest to względnie zrównoważony endo- i egzogeniczny stan funkcjonowania gospodarki narodowej, w którym występujące ryzyko zaburzeń równowagi utrzymywane jest w wyznaczonych*

³¹ Por. R. Zieliński, *Kierowanie gospodarką socjalistyczną w świetle teorii bezpieczeństwa ekonomicznego*, [w:] *Bezpieczeństwo ekonomiczne. Teoria i praktyka*, red. Z. Kołodziejak, Wyd. Uniwersytetu Łódzkiego, Łódź 1986, s. 74.

³² Por. W. Stankiewicz, *Zagadnienia bezpieczeństwa ekonomicznego a gospodarka obronna*, [w:] *Bezpieczeństwo...*, op. cit., s. 39.

³³ Por. F. Majchrzak, *Bezpieczeństwo ekonomiczne a teoria wojny gospodarczej*, [w:] *Bezpieczeństwo...*, op. cit., s. 46.

³⁴ Por. S. Michałowski, *Bezpieczeństwo ekonomiczne w stosunkach wschód-zachód*, PISM, Warszawa 1990, s. 8.

³⁵ Por. A. Jurkowska-Zeidler, *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*, Oficyna Wydawnicza Wolters Kluwer, Warszawa 2008, s. 166.

³⁶ Por. K.M. Książkowski, *Bezpieczeństwo ekonomiczne*, Dom Wyd. ELIPSA, Warszawa 2011, s. 29.

*i akceptowalnych normach organizacyjno-prawnych oraz zasadach współżycia społecznego*³⁷;

- *bezpieczeństwo ekonomiczne państwa to taki stan rozwoju krajowego systemu gospodarczego, który zapewnia wysoką sprawność jego funkcjonowania – poprzez należyte wykorzystanie wewnętrznych czynników rozwoju – oraz zdolność do skutecznego przeciwstawienia się zewnętrznym naciskom, mogącym doprowadzić do zaburzeń rozwojowych*³⁸.

A oto kilka wniosków:

Pierwszy. Bezpieczeństwo ekonomiczne jest ściśle związane z płaszczyzną społeczno-gospodarczą (ogólnoekonomiczną) w wymiarze państwowym, wyrażając jako cel rozwój gospodarki i powiązań międzynarodowych, gwarantujący stabilność funkcjonowania i odporność na zagrożenia i destabilizację systemu społeczno-politycznego oraz osłabienia zdolności obronnej.

Drugi. Bezpieczeństwo gospodarcze na płaszczyźnie ekonomiczno-obronnej (lub dokładniej obronno-ekonomicznej) w wymiarze pojedynczego państwa oznacza w tym przypadku zdolność jego systemu gospodarczego do efektywnego przeciwstawiania się zewnętrznej ingerencji ekonomicznej oraz w miarę niezagrażonego rozwoju potencjału obronno-ekonomicznego i funkcjonowania różnych modeli gospodarki obronnej.

Trzeci. Bezpieczeństwo ekonomiczne odnosi się do zagrożeń dla dobrobytu, swobodnego dostępu do rynków, środków finansowych i zasobów naturalnych (ropa naftowa, gaz), które gwarantują stały rozwój państwa i utrzymanie jego pozycji.

Bezpieczeństwo ekonomiczne państwa można kategoryzować poprzez wykorzystanie wyróżników, do których zaliczamy: zakres pojęciowy, płaszczyzny występowania, formę klasyfikacji, podmiot (przestrzeń) opisu, czas, intensywność ograniczeń, zakres realizowanych wartości, wymiar lub inaczej relacje z otoczeniem zewnętrznym, cechy wyróżniające oraz sposób realizacji. Przykładowa systematyzacja istoty i treści bezpieczeństwa ekonomicznego państwa została przywołana w tabeli 1.1.

Należy podkreślić, że bezpieczeństwo ekonomiczne ściśle wiąże się z takimi aspektami, jak: sprawność funkcjonalna, wytrzymałość oraz odporność gospodarki na oddziaływanie wszelkich negatywnych czynników (zarówno zewnętrznych, jak i wewnętrznych) mogących rodzić zagrożenia dla procesów reprodukcji gospodarczej, a także z zagadnieniem szeroko pojmowanej konkurencyjności. Stąd też można powiedzieć, iż nieodłączną treścią opisu

³⁷ Por. K. Raczkowski, *Percepcja bezpieczeństwa ekonomicznego i wyzwania dla zarządzania nim w XXI wieku*, [w:] *Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem*, red. K. Raczkowski, Oficyna Wydawnicza Wolters Kluwer, Warszawa 2012, s. 82.

³⁸ Zob. Z. Stachowiak, *Teoria i praktyka mechanizmu ekonomicznego państwa Ujęcie systemowe*, AON, Warszawa 2012, s. 33.

bezpieczeństwa ekonomicznego są jego zagrożenia. Bez zagrożeń, ich skali, formy, intensywności nie sposób orzekać o poziomie bezpieczeństwa i sposobach jego zapewnienia.

Tabela 1.1

Systematyzacja istoty i treści bezpieczeństwa ekonomicznego państwa

| BEZPIECZEŃSTWO EKONOMICZNE/GOSPODARCZE PAŃSTWA wartość, jedna z 4. dziedzin bezpieczeństwa państwa | |
|--|--|
| <p>Bezpieczeństwo ekonomiczne państwa – stan rozwoju gospodarki, który zapewnia jego wysoką sprawność oraz zdolność do skutecznego przeciwstawienia się zewnętrznym naciskom.</p> <p>Ekonomiczne bezpieczeństwo obronne – zdolność systemu gospodarczego państwa do efektywnego przeciwstawienia się zewnętrznej ingerencji ekonomicznej oraz rozwoju gospodarki obronnej.</p> | |
| Kryterium wyróżnienia | Zakres (wymiar) treści pojęcia „bezpieczeństwo ekonomiczne” |
| Zakres pojęciowy | <ol style="list-style-type: none"> 1. Tradycyjne – BE pochodne problemów politycznych i militarnych, określane w tym ujęciu jako „ekonomiczne aspekty bezpieczeństwa”. <ul style="list-style-type: none"> • Podatność kraju na przeniesienie przez płaszczyznę gospodarczą działań gospodarczych o charakterze politycznym, skierowanych na osłabienie bezpieczeństwa kraju. 2. Współczesne – rozszerzanie BE poza kwestie obronno-ekonomiczne i nadawanie podstawowej i względnie samodzielnej rangi kwestiom bezpieczeństwa gospodarki. <ul style="list-style-type: none"> • Takie wykorzystanie wewnętrznych czynników rozwoju i międzynarodowej współzależności ekonomicznej, które będą gwarantowały niezagrożony rozwój. |
| Płaszczyzny | <ol style="list-style-type: none"> 1. Ogólnoekonomiczna (społeczno-ekonomiczna). 2. Obronno-ekonomiczna (wojenno-ekonomiczna). |
| Forma | <ol style="list-style-type: none"> 1. Przedmiotowe – surowcowe, finansowe, technologiczne, rolne, żywnościowe itp. 2. Podmiotowe – współzależności, zależności, siły i trwałość powiązań. |
| Podmiot (przestrzeń) | <ol style="list-style-type: none"> 1. Państwa. 2. Grupy państw (ugrupowania, regionu). 3. Globalne. |
| Czas | <ol style="list-style-type: none"> 1. Stan. 2. Proces. |
| Intensywność ograniczeń i sprzeczności | <ol style="list-style-type: none"> 1. Stan gospodarki, w którym zapewniono zaspokojenie podstawowych potrzeb. 2. Proces, zapewniający przetrwanie i rozwój systemu gospodarczego w sytuacji zagrożenia. 3. Sytuacja, w której sprzeczności (wewnątrz i międzysystemowe) nie prowadzą do wystąpienia zagrożeń, konfliktów i kryzysów. |

| | |
|-------------------------------|---|
| Zakres realizowanych wartości | <ol style="list-style-type: none"> 1. Pozytywne – zespół właściwości gospodarki narodowej, o której możemy orzekać, że trwa i rozwija się (rozwój, dobrobyt). 2. Negatywne – przetrwanie, ochrona osiągniętego poziomu rozwoju i pozycji w układzie międzynarodowym. |
| Wymiar (relacje z otoczeniem) | <ol style="list-style-type: none"> 1. Wewnętrzne – efektywne wykorzystanie wewnętrznych czynników rozwoju zgodnie z preferencjami społeczeństwa (hierarchią wartości). 2. Zewnętrzne – brak zagrożeń zewnętrznych, wykorzystania współzależności gospodarczych i zasobów zewnętrznych do przyspieszenia rozwoju i realizacji racji stanu państwa. |
| Cechy wyróżniające | <ol style="list-style-type: none"> 1. Nie można sformułować w stosunku do pozytywnego bezpieczeństwa ekonomicznego warunku wystarczalności. 2. Znaczenie podstawowe mają wewnętrzne czynniki rozwoju. 3. Bezpieczeństwo ekonomiczne budują adaptacyjność i podatność na zmiany, a nie stabilizacja. 4. Sprzeczności pomiędzy potrzebną współzależnością warunkującą efektywność i poszerzanie rynków a uzależnieniem zewnętrznym gospodarki. 5. Ograniczona rola państwa w kształtowaniu bezpieczeństwa ekonomicznego. |
| Sposób realizacji | <ol style="list-style-type: none"> 1. Indywidualne. 2. Integracja. 3. Współpraca. |

Źródło: S. Kurek, S.T. Kurek, Z. Stachowiak, *Bezpieczeństwo ...*, op. cit., ss. 34-35.

Warto także zauważyć, iż zazwyczaj sposób postrzegania szczegółowego obszaru kategorii „bezpieczeństwo ekonomiczne” jest determinowany przedmiotem rozpatrywanego podmiotu oraz zjawisk, działań i procesów charakterystycznych dla poszczególnych poziomów analizy bezpieczeństwa: systemu i podsystemów międzynarodowych, poziomu korporacji międzynarodowych, państwa i gospodarki narodowej oraz krajowych podmiotów gospodarczych, w tym jednostek ludzkich, gospodarstw domowych i przedsiębiorstw³⁹.

Bezpieczeństwo ekonomiczne państwa jest często charakteryzowane jako⁴⁰:

- zdolność systemu gospodarczego (państwa, grupy państw, regionu, świata) do takiego wykorzystania wewnętrznych czynników rozwoju i międzynarodowych współzależności ekonomicznych, aby zagwarantować możliwości rozwoju;

³⁹ L. Chojnowski, *Poziomy analizy bezpieczeństwa*, [w:] *Współczesne Bezpieczeństwo. Perspektywa teoretyczno-metodologiczna*, red. S. Jaczyński, M. Kubiak, M. Minkina, Wyd. Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Warszawa-Siedlce 2011, ss. 35-50.

⁴⁰ S.T. Kurek, Z. Stachowiak, *Podstawy bezpieczeństwa ekonomicznego państwa*, [w:] *Podstawy bezpieczeństwa współczesnego państwa (podmiotu). Implikacje*, red. J. Pawłowski, AON, Warszawa 2015, s. 397.

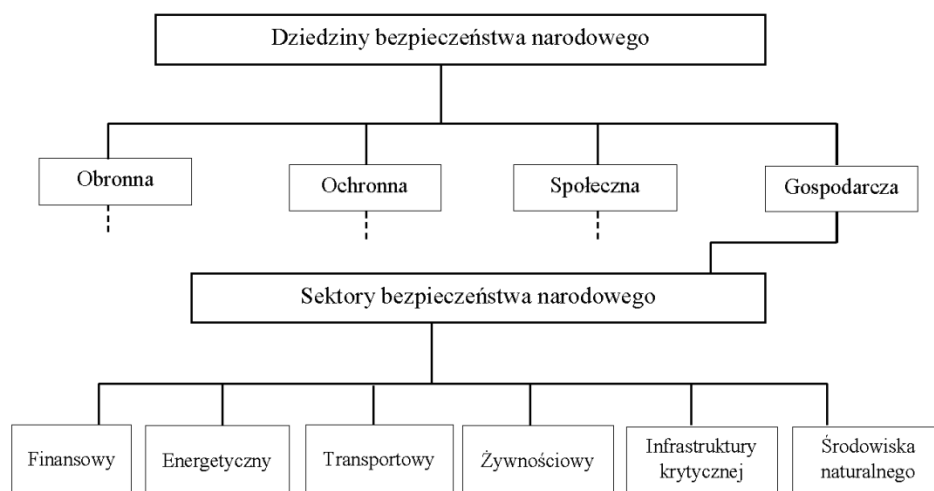
- wypadkowa czynników rozwoju gospodarczego i ograniczających go barier, tkwiących we wszystkich czynnikach jego kształtowania;
- bilans potrzeb rozwojowych i możliwości ich zaspokojenia;
- stan gospodarki i jej struktur oraz stosunków gospodarczych i powiązań umożliwiających skuteczne przeciwstawianie się negatywnym oddziaływaniom zewnętrznym, które mogą osłabiać rozwój gospodarczy, stabilność systemu społeczno-politycznego i zdolność obronną;
- ogólny stan zależności ekonomicznych, określający stopień efektywności zewnętrznej ingerencji ekonomicznej w wewnętrzny rozwój gospodarczy, zdolność obronną i stabilność systemu społeczno-politycznego danego kraju;
- wyobrażenie co do rzeczywistych, względnie potencjalnych, zagrożeń gospodarczych kraju, które określają stopień efektywności rozwoju gospodarczego, zdolności obronnej i stabilności systemu społeczno-politycznego danego kraju;
- wyraz stopnia podatności danego państwa na przeniesienie przez płaszczyznę gospodarczą, głównie przez transmisję kanałami i mechanizmami, zależności ekonomicznych działań o charakterze politycznym skierowanych na osłabienie bezpieczeństwa państwa.

Próbując z kolei wskazać miejsce bezpieczeństwa gospodarczego w całościowym systemie bezpieczeństwa narodowego/państw, zauważamy już na wstępie badań literaturowych, iż nie jest to ze swej natury przedsięwzięcie łatwe. Choć znamienne jest, że znaczenie składnika ekonomicznego w strukturze bezpieczeństwa dostrzega i podkreśla wielu autorów. Jedno z bardziej czytelnych stanowisk w tej sprawie przedstawił J. Świniarski, który twierdzi, że: „W tradycji myślenia o bezpieczeństwie bardzo często dostatek, dobrobyt i bogactwo sytuowane są wśród jego warunków. Od dawna szczęście, pomyślność i pewność podejmowanych przez ludzi starań w celu realizacji swego życia (jego prolongowania i doskonalenia) uzależniano od warunków ekonomicznych. Były one i są elementem, filarem i czynnikiem oraz warunkiem bezpieczeństwa. Wyrażane są przez *komponent nazywany dziś bezpieczeństwem ekonomicznym*. Ono zaś osnute jest na jakimś bogactwie, dobrobycie i dostatku tudzież dochodzie (narodowym) lub produkcji (globalnym) zarówno wytwarzanym jak i podzielonym. Dość powszechne jest bowiem przekonanie, iż bogactwo i dobrobyt dopełniają istotnie szczęście i bezpieczeństwo. Stąd i sytuowanie tego komponentu wśród kardynalnych filarów, na których wsparte jest bezpieczeństwo, pojmowane, już to jako taka forma istnienia i życia, która zapewnia trwanie, przetrwanie i zwiększa szanse na jego rozwój, już to jako pewność trwania i przeżycia oraz swobody rozwoju”⁴¹.

⁴¹ Zob. J. Świniarski, *Ekonomia wojenna i ekonomia pokojowa w systemie ogólnej teorii bezpieczeństwa*, [w:] *Ekonomika wojskowa i logistyka wojskowa – podobieństwa i różnice*, Materiały z sympozjum, AON, Warszawa 1998, ss. 29-30.

Kontynuując badania analityczne, dochodzimy do ogólnego wniosku, że pozycja i relacje bezpieczeństwa ekonomicznego z innymi segmentami (subelementami) ogólnego bezpieczeństwa państwa zależą przede wszystkim od przyjętego kryterium jego wyodrębnienia oraz postawy preferowanej przez dane środowisko/badacza. Stąd też na chwilę obecną nie można przywołać jednego, ogólnie aprobowanego, modelu bezpieczeństwa narodowego wraz z jego podrodzajami, gdyż podejść do tej kwestii jest co najmniej kilka.

Na przykład w *Białej Księdze Bezpieczeństwa Narodowego* wyszczególniono w systemie bezpieczeństwa narodowego cztery główne jego dziedziny (rys. 1.2), tzn.⁴²: obronną, ochronną, społeczną, gospodarczą.



Rys. 1.2. Struktura bezpieczeństwa narodowego ze szczególnym uwzględnieniem bezpieczeństwa gospodarczego

Źródło: opracowanie własne na podstawie *Białej...*, op. cit., s. 19 i *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 5 listopada 2014 r., s. 12.

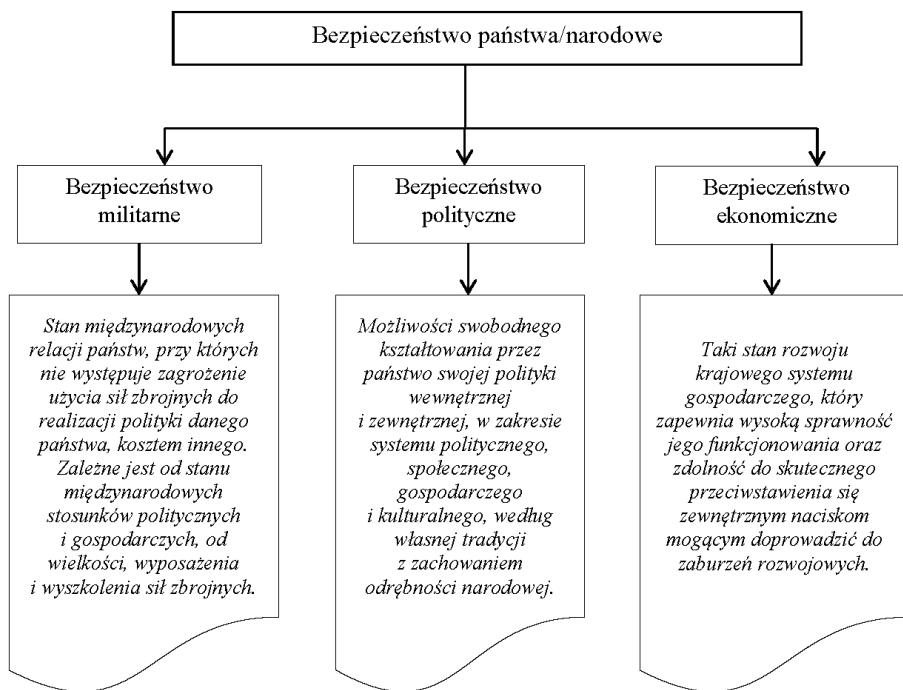
Każdej dziedzinie zostały przyporządkowane sektory bezpieczeństwa narodowego, zagregowane ze względu na podobieństwo przedmiotowe (bliskość zakresu działalności podmiotów odpowiedzialnych za poszczególne działy) oraz transsektorowe⁴³ obszary bezpieczeństwa.

⁴² Zob. *Biała Księga Bezpieczeństwa Narodowego*, Wyd. BBN, Warszawa 2013, s. 19.

⁴³ Transsektorowe (transpodmiotowe) obszary bezpieczeństwa narodowego (państwa) to część zintegrowanego bezpieczeństwa narodowego obejmujące swą treścią problematykę właściwą jednocześnie różnym podmiotom, dziedzinom i sektorom tego bezpieczeństwa. Są one często wyodrębnione z uwagi na nowe i pilne w danym okresie

Takie umiejscowienie bezpieczeństwa gospodarczego sprawia, że jest ono traktowane jako jedna z czterech dziedzin bezpieczeństwa narodowego, której głównym zadaniem jest ochrona podmiotów przed destabilizacją, dezintegracją wywołaną negatywnymi czynnikami (zagrożeniami), zarówno wewnętrznymi, jak i zewnętrznymi.

Dziedzina bezpieczeństwa gospodarczego obejmuje takie sektory, jak: finansowy, energetyczny, transportowy, infrastruktury, w tym infrastruktury krytycznej, środowiska naturalnego, żywnościowego⁴⁴, podmiotów produkcyjnych i usługowych.



Rys. 1.3. Płaszczyzny kształtowania bezpieczeństwa państwa (narodowego)

Źródło: opracowanie własne na podstawie S. Kurek, S.T. Kurek, Z. Stachowiak, *Bezpieczeństwo ...*, op. cit., s. 24.

potrzeby praktyczne, niemające wyraźnego adresata w istniejącej strukturze wykonawczej podmiotu, tamże, s. 248.

⁴⁴ Por. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 5 listopada 2014 r., s. 12.

Samą zaś istotą działań gospodarczych w sferze bezpieczeństwa jest ochrona podmiotów i materialnych zasobów gospodarczego potencjału bezpieczeństwa narodowego przed zagrożeniami w czasie pokoju, kryzysu i wojny oraz wsparcie działania podsystemów operacyjnych systemu bezpieczeństwa narodowego, co powinno być możliwe dzięki działaniom instytucji i podmiotom zmierzającym do wzmocnienia bezpieczeństwa finansowego, zwiększenia bezpieczeństwa energetycznego, utrzymania rezerw strategicznych, wzmocnienia bezpieczeństwa żywnościowego oraz ochrony środowiska naturalnego⁴⁵.

W nieco innym ujęciu problemowym bezpieczeństwo narodowe jest traktowane jako zbiór nakładających się na siebie płaszczyzn⁴⁶: politycznej, militarnej i ekonomicznej (rys. 1.3). W literaturze przedmiotu noszą one miano płaszczyzn kształtowania (filarów) bezpieczeństwa państwa.

W powyżej przedstawionym ujęciu o wyjściowym poziomie bezpieczeństwa narodowego/państwa stanowi zbiór trzech specyficznych płaszczyzn jego kształtowania.

Niezależnie od tego, jak bezpieczeństwo gospodarcze państwa będzie ujmowane, i w jakim kontekście charakteryzowane, jego istotę można sprowadzić zasadniczo to tego, że oznacza ono zdolność systemu gospodarczego z jednej strony do tworzenia, z drugiej zaś do wykorzystywania współzależności gospodarczych o charakterze wewnętrznym i międzynarodowym w celu zwiększenia dynamiki rozwoju gospodarczego i efektywności gospodarki, przekładających się na jakość życia obywateli⁴⁷.

Faktem bezsprzecznym jest w dniu dzisiejszym również to, że bezpieczeństwo gospodarcze stanowi nieodłączny element bezpieczeństwa narodowego i jako takie stanowi jego niezaprzeczalny fundament i narzędzie formujące stan bezpieczeństwa każdego współczesnego państwa⁴⁸.

1.2. Idea i główne cele zarządzania bezpieczeństwem gospodarczym

Mając na względzie zarówno istotę samego bezpieczeństwa gospodarczego (ekonomicznego) państwa oraz jego główne czynniki kształtowania, zaznaczyć

⁴⁵ Tamże, pkt. 100-105.

⁴⁶ Por. S. Michałowski, *Bezpieczeństwo ...*, op. cit., s. 19.

⁴⁷ Por. A. Kalata, Z. Nowakowski, I. Protasowicki, *Determinanty bezpieczeństwa ekonomicznego Polski*, [w:] *Współczesne wyzwania polityki bezpieczeństwa – wybrane zagadnienia*, red. M. Ilnicki i Z. Nowakowski, Wyd. Towarzystwo Naukowe Powszechne, Warszawa 2014, rozdz. 3.

⁴⁸ Por. *Economics and National Security*, [w:] *Issues and Implications for U.S. Policy*, cor. D.K. Nanto, CRS Report for Congress, 4 January 2011, s. 78.

trzeba już na wstępie, że w ujęciu procesowym zarządzanie tym specyficznym obszarem bezpieczeństwa państwa traktować należy, jako *sztukę zmierną do przewencyjnego rozpoznawania zagrożeń w funkcjonowaniu gospodarki narodowej, sprawnego wprowadzania działań zabezpieczających przed stanem nierównowagi ekonomicznej, strategicznej zdolności osiągnięcia zamierzonych celów oraz umiejętności porządkowania chaosu w ekonomicznych sytuacjach kryzysowych*⁴⁹.

Postrzegając zarządzanie bezpieczeństwem ekonomicznym przez pryzmat klasycznych podstaw teorii organizacji i zarządzania, widzieć je trzeba jako problem, którego kontekst winien być rozpatrywany na wszystkich trzech poziomach zarządczych, tzn. operacyjnym, taktycznym i strategicznym. Oczywiście jest, że znaczący w tym zakresie będzie poziom strategiczny, gdyż ranga podejmowanych problemów, a tym samym wypracowywanych decyzji i ich wykonalność wiąże się z koniecznością opracowywania i zatwierdzania dokumentów o charakterze strategicznym. Sprawia to, iż perspektywiczne plany w zakresie zarządzania bezpieczeństwem gospodarczym mają i powinny mieć wymiar długoterminowy i nadrzędny, co implikuje konieczność ich doprecyzowania poprzez liczne uogólnienia, wskazując rozłożenie akcentów w percepcji samego bezpieczeństwa i jego miejsca w ogólnej hierarchii celów strategicznych państwa.

Zarządzanie bezpieczeństwem w dłuższej perspektywie czasowej z natury rzeczy musi być obciążone pewnym ryzykiem zaistnienia innych nieprzewidywalnych zdarzeń i scenariuszy rozwoju sytuacji. Tak więc niezbędne staje się w tym przypadku posługiwanie się estymacją oraz innymi typami wnioskowania⁵⁰.

Do głównych celów holistycznego ujęcia w procesie zarządzania bezpieczeństwem ekonomicznym państwa należy zaliczyć⁵¹:

- zapewnienie równowagi finansów publicznych;
- antycypację przyszłości;
- poszukiwanie partnerów i zwolenników wspólnych inicjatyw na arenie międzynarodowej;
- permanentne wykorzystanie zagrożeń do kreowania szans rozwojowych;
- stałe inteligentne profilowanie rynków wewnętrznych i zewnętrznych z jednoczesnym zabezpieczeniem własnych interesów własnych systemów społeczno-ekonomicznych przed nieuprawnioną ingerencją;
- bardziej efektywne uchwalanie prawa i jego późniejsze respektowanie (zwłaszcza w zakresie przeciwdziałania rozwojowi gospodarki nieoficjalnej i usuwania barier w prowadzeniu działalności gospodarczej);

⁴⁹ Zob. K. Raczkowski, *Percepcja ...*, op. cit., s. 82.

⁵⁰ Tamże, s. 83.

⁵¹ Tamże.

- tworzenie ram wspólnej wizji oraz celów w ramach społeczeństwa obywatelskiego rozwoju (rozumiana i wspólnotowa kultura organizacyjna);
- podejmowanie działań prewencyjnych i zaradczych w obszarze wspierania oraz promocji nauki i techniki – z założeniem ekonomicznej stopy zwrotu w długim okresie.

Nieco inne podejście do kwestii istoty zarządzania bezpieczeństwem gospodarczym kraju, a ściślej rzecz biorąc kierowania gospodarczymi podstawami bezpieczeństwa państwa, rozumianymi jako ta część gospodarki narodowej, która zaspokaja potrzeby systemu bezpieczeństwa stosownie do występujących stanów napięcia i zagrożenia, wynika ze stwierdzenia, że *istotą systemu zarządzania gospodarczymi podstawami bezpieczeństwa państwa jest to, iż zadania dla gospodarki narodowej odnośnie dostarczania dóbr i usług „obronnie przydatnych” ustalane są przez centralne organy władzy ustawodawczej i wykonawczej państwa, a realizują je różnorodne podmioty administracji państwowej, samorządowej i gospodarczej, w zależności od swoich kompetencji, możliwości i obowiązujących uregulowań prawno-administracyjnych*⁵².

Tak ujęty system zarządczy sfery bezpieczeństwa gospodarczego odnosi się zatem do części ogólnej polityki państwa, czyli mechanizmów i procesów pobudzania zorientowanych na dwa obszary: gospodarkę i bezpieczeństwo. W syntetycznym ujęciu jest on zatem systemem kierowania procesami gospodarczymi, których celem zasadniczym jest sprawność systemu bezpieczeństwa państwa.

Opisując w powyższy sposób rolę elementów kierowniczych gospodarczych podstaw bezpieczeństwa państwa, których istota opiera się na tym, że proces decyzyjny realizowany przez podmioty sfery regulacyjnej państwa sprowadza się do utrzymywania swoistego typu balansu pomiędzy potrzebami obronnymi kraju a jego możliwościami gospodarczymi, oraz mając na względzie istotę i zakres realnych mechanizmów występujących w obszarze polityki gospodarczo-obronnej państwa, stwierdzić można, że obszar oddziaływania systemu zarządzania gospodarczymi fundamentami bezpieczeństwa w makroskali obejmuje bardzo szerokie spektrum przedsięwzięć, ukierunkowanych zasadniczo na⁵³:

- określanie kierunków rozwoju gospodarczego z uwzględnieniem syntetycznie wskazanych potrzeb bezpieczeństwa i obrony;
- kształtowanie stosunków własnościowych w sektorze obronnym (bezpieczeństwa) gospodarki;

⁵² Por. S.T. Kurek, *Model systemu zarządzania bezpieczeństwem Polski w wymiarze gospodarczym*, [w:] Zeszyty Naukowe AON 2011 nr 1(82), s. 8.

⁵³ Por. M. Sułek, *Polityka gospodarczo-obronne państwa*, [w:] *Zarys ekonomiki bezpieczeństwa*, red. nauk. J. Płaczek, AON, Warszawa 2009, ss. 74-75.

- określanie zasad funkcjonowania przemysłu obronnego i obronnie zorientowanego (wielkości, struktury produkcyjnej i organizacyjnej, rozmieszczenia przestrzennego);
- opis zasad współpracy gospodarczej z zagranicą w obszarze obrotu sprzętem specjalnego przeznaczenia;
- kształtowanie wielkości, struktury i dyslokacji rezerw mobilizacyjnych;
- określanie sposobów finansowania poszczególnych elementów systemu bezpieczeństwa i obronny (sił zbrojnych, rezerw mobilizacyjnych, infrastruktury obronnej, badań naukowych itp.) oraz następstw perturbacji na rynku wewnętrznym i międzynarodowym;
- sterowanie wielkością i poziomem gotowości mobilizacyjnej gospodarczych podstaw bezpieczeństwa państwa;
- inicjowanie i koordynację prac naukowo-badawczych z obszaru gospodarczo-obronnego, realizowanych zasadniczo przez przedstawicieli nauk o bezpieczeństwie oraz nauk o obronności;
- przygotowanie specjalistycznych kadr zarządzających gospodarczymi (ekonomicznymi) podstawami bezpieczeństwa kraju (bezpieczeństwem gospodarczym).

Przyglądając się obu przytoczonym powyżej podejściom do kwestii zarządzania bezpieczeństwem gospodarczym, możemy wskazać na dwie specyficzne konwencje: ogólnoeconomiczną oraz gospodarczo-obronną.

Jeśli ta pierwsza akcentuje szerokie spektrum problemów wolnorynkowego funkcjonowania systemu gospodarczego, to w podejściu gospodarczo-obronnym nacisk jest położony na ścisłe powiązanie potrzeb gospodarczych społeczeństwa z potrzebami systemu obronnego państwa.

Wydaje się zatem, że niezależnie od spotykanych w teorii problemu argumentów za i przeciw konkretnemu podejściu, w praktyce życia społeczno-gospodarczego, a co za tym idzie również w rozwiązaniach polityczno-prawnych, będziemy spotykali oba rozwiązania.

1.3. Determinanty i funkcje zarządzania bezpieczeństwem gospodarczym

Wskazanie istoty i miejsca bezpieczeństwa gospodarczego państwa umożliwia przejście w kolejnym kroku rozważań do podjęcia próby identyfikacji głównych czynników wpływających na kształt i stan poziomu bezpieczeństwa systemu ekonomicznego kraju. Czynniki owe, noszące miano szeroko rozumianych determinantów⁵⁴ bezpieczeństwa gospodarczego, stanowią bardzo

⁵⁴ Encyklopedyczne ujęcie kategorii „determinanta” jest traktowane jako synonimiczne pojęcie „wyznacznika” lub „wyróżnika” (W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Wyd. Muza S.A., Warszawa 2002, s. 121).

szerokie spektrum wyznaczników określających i warunkujących sprawne kształtowanie sfery tak regulacyjnej, jak i realnej systemu społeczno-gospodarczego każdego kraju. Wszystkie wyróżniki bezpieczeństwa gospodarczego w rzeczywistości dnia dzisiejszego, mieszczące się zasadniczo w praktyce działalności społecznej, ekonomicznej i politycznej, w toku procesów kształtowania i utrzymania bezpieczeństwa ekonomicznego państwa mogą być poddane próbie wyróżnienia poprzez zastosowanie zabiegu metodyczno-metodologicznego, sprowadzającego się do przywołania szeregu kryteriów, takich jak źródła ich alokacji lub też charakter wpływu.

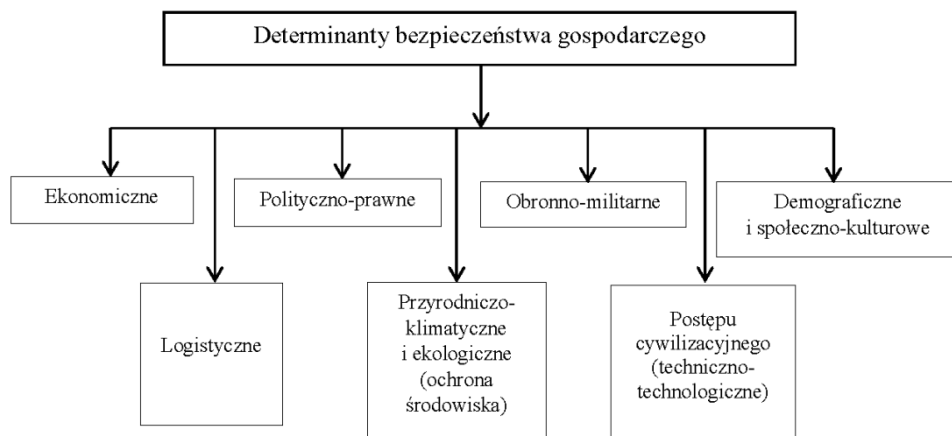
Postępując zatem zgodnie z powyżej wskazanym kierunkiem rozumowania oraz stosując identyfikacyjne kryterium przedmiotowe, przywołać można zasadniczo sześć głównych grup czynników kształtowania bezpieczeństwa gospodarczego, tworzących specyficzne zbiory jego tworzenia i zachowania. Grupami tymi są następujące *determinanty*⁵⁵: ekonomiczne, polityczno-prawne, obronno-militarne, demograficzne i społeczno-kulturowe, przyrodniczo-klimatyczne i ekologiczne oraz postępu cywilizacyjnego – rys. 1.4.

Zasadniczymi spośród wskazanego zbioru determinant są, co rozumiałe, *determinanty ekonomiczne*, pod pojęciem których rozumie się ogólne warunki i trendy ekonomiczne, mające podstawowe znaczenie w realizacji zadań w każdej organizacji i warunkujące w ten sposób funkcjonalną sferę wszystkich systemów państwa, w tym również systemu bezpieczeństwa. Stanowią one fundamentalny zbiór czynników sprawności funkcjonowania systemu bezpieczeństwa.

To bowiem od zasobów ekonomicznych oraz poziomu rozwoju gospodarczego kraju, czyli liczebności, zamożności i przedsiębiorczości jego mieszkańców, poziomu konkurencyjności gospodarki narodowej w relacji z otoczeniem zewnętrznym, dynamiki rozwoju społeczno-gospodarczego, sprawności funkcjonowania mechanizmów rynkowych, stabilności systemu oraz wiarygodności i atrakcyjności inwestycyjnej, zależy wielkość budżetu państwa, czyli ilość środków finansowych, które mogą być przeznaczane w danym roku na realizację ustawowych zadań, jakie suweren nakłada na instytucje i organy administracji państwowej, w tym również te odpowiedzialne za bezpieczeństwo.

W najczęstszym słownikowym ujęciu „determinant” (z łac. *determinans*, d. ~ntis = określający, wyznaczający) jest to „każdy czynnik, którego funkcja polega na wyznaczaniu (determinowaniu) czegoś” (*Słownik wyrazów obcych*, red. J. Tokarski, PWN, Warszawa 1980, s. 148).

⁵⁵ Zob. A. Dziurny, *Identyfikacja determinant konstrukcji modelu bezpieczeństwa ekonomicznego Polski*, [w:] *Nauczyciele i mistrzowie ekonomii i logistyki – Wacław Stankiewicz. Tom I – Ekonomia instytucjonalna wobec problemów bezpieczeństwa i obronności*, red. A. Dziurny i S.T. Kurek, AON (maszynopis), Warszawa 2015, s. 143.



Rys. 1.4. Determinanty bezpieczeństwa gospodarczego

Źródło: opracowanie własne na podstawie A. Dziurny, *Identyfikacja ...*, op. cit., s. 143.

Pomimo tego, iż determinanty te są ściśle sprzężone z pozostałymi czynnikami warunkującymi bezpieczeństwo, to odzwierciedlają jednak przede wszystkim wzajemne relacje i związki na styku gospodarka – społeczeństwo. Dokładniejsze ich rozpoznanie i opisanie musi być zawsze dokonywane według kryteriów przydatności do konstrukcji modelu zarządzania bezpieczeństwem gospodarczym. W tym kontekście rozważań wiodącym staje się kryterium zaliczania poszczególnych determinantów do czynników mających znaczący wpływ na rozwój społeczno-gospodarczy oraz możliwość sprostania pojawiającym się coraz to bardziej skomplikowanym wyzwaniom cywilizacyjnym⁵⁶.

Kolejną, ważną, grupę spośród wskazanych determinant stanowią determinanty *polityczno-prawne*. Występują one i zmieniają się w ramach określonej rzeczywistości systemu społeczno-politycznego oraz przyjętych norm prawnych, warunkujących i kształtujących możliwości realizacji ekonomicznych zadań i funkcji państwa. Z samej istoty państwa demokratycznego wynika, że obszary prawne i polityczne są ze sobą bardzo silnie związane. Wybrany przez dane społeczeństwo ustrój polityczny determinuje zarówno sposób tworzenia, jak i stosowania prawa w danym kraju czy też, szerzej, ugrupowaniu. Realnie uchwalone akty normatywne stanowią z kolei podbudowę stabilności ustrojowej, a co za tym idzie bezpieczeństwa gospodarczego. Funkcjonujący system polityczny jest więc głównym czynnikiem warunkującym sposób kształtowania i budowy przedmiotowego bezpieczeństwa. Poza nim można wskazać jeszcze inne szczegółowe determinanty polityczno-prawne. Kompleksowy ich zbiór, decydujący o formule zapewnienia bezpieczeństwa gospodarczego, można

⁵⁶ A. Dziurny, *Identyfikacja ...*, op. cit., ss. 143-144.

sprowadzić do dwóch zasadniczych płaszczyzn jego szczegółowego kształtowania. Pierwszą z nich tworzy obszar obejmujący podmioty niezbędne do zapewnienia przyjętego poziomu bezpieczeństwa (wyposażone w odpowiednie instrumentarium realizacyjne), na drugi zaś składają się elementy konkretnych zadań do wykonania.

Do trzeciego zbioru czynników decydujących o bezpieczeństwie gospodarczym zaliczyć należy *determinant militarno-obronny*. Wyznaczniki tego typu, pomimo panującego od kilkunastu lat znaczącego odprężenia militarnego w układzie zarówno globalnym, jak i regionalnym, nie mogą być pomijane przy kształtowaniu i realizacji polityki bezpieczeństwa ekonomicznego konkretnego państwa. Argumentem za ich uwzględnieniem jest chociażby sytuacja społeczno-polityczna i militarna na Ukrainie i wynikające z niej zagrożenia. Daleko idące nieprzewidywalności sytuacji oraz rysujące się obecnie tendencje odprężeniowe i rozbrojeniowe nie mogą być traktowane jako gwarant stabilności i eliminacji wszelkich zagrożeń, w tym także ekonomicznych. Czynnikiem gwarantującym pełne bezpieczeństwo nie mogą być również zewnętrzne akceptacje członkostwa kraju, ani w Unii Europejskiej, ani też w Pakcie Północnoatlantyckim. Geostrategiczne położenie państwa, jak np. Polski, sprawia, że bezpieczeństwo i obronność stanowią muszą kluczową kwestię narodowej racji stanu, a tym samym podstawę formułowania i realizacji strategii bezpieczeństwa i obrony. Postrzeganie bezpieczeństwa narodowego przez pryzmat idei nieprzewidywalności i prewencyjnej asekuracji, sygnalizowane w wielu opracowaniach analityków i strategów wojskowych, dostrzegane jest w podstawowych aktach normatywnych kształtowania polityki bezpieczeństwa i strategii obronnej Polski⁵⁷. Jego istota opiera się na założeniu, że w warunkach gospodarki pokojowej system społeczno-gospodarczy – patrząc z punktu widzenia bezpieczeństwa gospodarczego kraju – ma przede wszystkim obowiązek dążenia do zaspokojenia potrzeb ogółu społeczeństwa (w tym też wojska), a także rozwiązywania problemów związanych z przygotowaniem wszystkich swoich składowych do sytuacji zagrożeń bezpieczeństwa, a nawet wojny⁵⁸.

Czwartą grupę determinant bezpieczeństwa gospodarczego stanowią czynniki o charakterze *demograficznym* i *społeczno-kulturowym*. To od tych elementów zależą warunki, w jakich członkowie społeczeństwa są wychowywani oraz w jakich funkcjonują w trakcie swojego życia. Decydują również o tym, jak kształtują się ich podstawowe normy zachowań i jakie wartości są przez nich preferowane. Stanowiąc względnie stabilne podstawy społeczne,

⁵⁷ A. Dziurny, *Identyfikacja ...*, op. cit., s. 144.

⁵⁸ A. Dziurny, *Model bezpieczeństwa ekonomicznego Rzeczypospolitej Polskiej w warunkach globalizacji i regionalizacji zagrożeń oraz wyzwań cywilizacyjnych*, AON, Warszawa 2012, ss. 407-408.

są one przekazywane z pokolenia na pokolenie i znajdują zazwyczaj swoje odbicie w poglądach danych osób na samych siebie, na innych ludzi, organizacje, społeczeństwo, naturę świata, jak również system gospodarczy – jego kształt i realną formę. Także poziom wykształcenia społeczeństwa jest ściśle powiązany z jego kulturą i zdolnościami, w tym zasadniczo z wartościami przez nią przekazywanymi. Stąd też, ten zbiór determinant staje się istotną cechą demograficzną państwa, czyli jego strategicznego zasobu gospodarczego wraz z możliwościami jego wykorzystania teraz i w przyszłości. Z kolei jakość ekonomicznych elementów otoczenia, wyrażająca się głównie poprzez zdolność efektywnego wykorzystania współczesnych zdobyczy technicznych i organizacyjnych, zależy od stopnia wykształcenia danego społeczeństwa, czyli ogólnie rzecz ujmując poziomu solaryzacji, i wynikających z niej zdolności absorpcyjnych nowych technologii przez system ekonomiczny kraju⁵⁹.

Na grupę piątą wyznaczników bezpieczeństwa składają się z kolei determinanty *przyrodniczo-klimatyczne* oraz *ekologiczne*. W warunkach naszego kraju i realiach tu panujących odnoszą się one przede wszystkim do sfery gospodarki żywnościowej, w tym rolnictwa, a zwłaszcza do produkcji roślinnej i zwierzęcej. Te dwa obszary stanowią bowiem główny wskaźnik niezależności żywnościowej kraju, będący bezsprzecznie składową ogólnego bezpieczeństwa gospodarczego. Główną zaś przestrzenią ich charakterystyki jest obszar produkcyjny adaptowany w wyniku ingerencji ludzkiej do wymagań roślin uprawnych oraz zwierząt hodowlanych. W nieco mniejszym stopniu obszarem tym jest pozostała przestrzeń gospodarki żywnościowej, zwłaszcza przemysł rolno-spożywczy. Konieczność uwzględniania wpływu środowiska przyrodniczego na kształtowanie bezpieczeństwa ekonomicznego kraju odczytywać trzeba jako wynik społecznej potrzeby dostrzegania, w procesach wytwarzania żywności, współdziałania człowieka z szeroko rozumianym środowiskiem przyrodniczym, w zakresie jego zasobności i wykorzystania. Kwestia ta, jeśli postrzegać ją jako ochronę środowiska przyrodniczego, stanowi trzecie – po zachowaniu pokoju i zapewnieniu wyżywienia – zadanie stojące obecnie przed społecznością światową⁶⁰. Dla przykładu, dokonując oceny kształtowania bezpieczeństwa gospodarczego w naszym kraju, z punktu widzenia cech środowiska przyrodniczego – zarówno naturalnego, jak i klimatycznego – zauważyć trzeba, że polskie rolnictwo charakteryzuje się niezbyt korzystnymi warunkami rozwoju. Będąca w jego dyspozycji ziemia – jeśli traktować ją jako środek produkcji – nie jest najlepsza ze względu na jej jakość, tzn. rzeźbę terenu, zwiąłość i kamienistość gleb, stosunki naturalne w glebie, jej naturalną

⁵⁹ A. Dziurny, *Identyfikacja ...*, op. cit., s. 145.

⁶⁰ Tamże, s. 146.

żywność oraz rozległość⁶¹. Dominacja w rzeźbie ziemi form płaskich, nizinnych i wyżynnych lub lekko falistych powoduje z kolei zagrożenie erozją gleb wodnych powierzchniowych, jak i wietrznych. Procesy erozji nie przybierają jednak dużych rozmiarów⁶². Nie do końca sprzyjający jawi się także agroklimat rolnictwa, tj. całokształt stanów pogody w długich okresach na danym obszarze, oddziałujących na wzrost roślin i zwierząt, charakteryzujący się takimi cechami, jak: nasłonecznienie, opady, temperatura i wilgotność powietrza. Wszystkie wskazane mankamenty powinny być poważnie brane pod uwagę podczas budowy systemu samowystarczalności żywnościowej państwa.

Siódmym, ostatnim determinantem to logistyka, która jest jednym ze składników decydujących o planowym realizowaniu zadań w ramach dziedzin bezpieczeństwa (w tym gospodarczego), sektorów i transsektorów. Pewne, na czas dostarczane dostawy, w ilościach odpowiadających potrzebom, o wysokiej jakości i skuteczności są czynnikami, od których zależy niezawodność oraz odporność na zagrożenia podmiotów bezpieczeństwa. Nie jest łatwym zadaniem, w przypadku zagrożeń, które pojawiły się nieoczekiwanie, zakłócając np. normalne funkcjonowanie rynku dostawców, dostarczyć produkty i usługi do podmiotów bezpieczeństwa, by one mogły normalnie egzystować. Sprostanie takim wymaganiom wymusza od logistyki, by była ona nowoczesna, oparta o najnowsze techniki i technologie, w tym informatyczne, a także otwarta na współdziałanie i współpracę z innymi ogniwami łańcuchów dostaw.

Podsumowując krótko wszystkie wskazane i omówione determinanty bezpieczeństwa gospodarczego, zaznaczyć należy, że pozostają one ze sobą w ścisłych wzajemnych relacjach i zależnościach, tworząc niejako siatkę wzajemnych powiązań decydujących łącznie o poziomie tworzonego obszaru. Zdawać sobie należy również sprawę z tego, że wszystkie zidentyfikowane grupy czynników nie są tym zbiorem zamkniętym i danym raz na zawsze, a przeciwnie tworzą problem o charakterze otwartym i dynamicznym, co uwidacznia się w ich nieustannej transformacji i przekształcaniu zgodnie z kierunkami rozwoju środowiska gospodarczego funkcjonującego w turbulentnym i bardzo zmiennym otoczeniu zewnętrznym, jak i wewnętrznym. Tak więc wskazana siedmioelementowa grupa determinantów charakteryzuje się różną skalą złożoności strukturalnej wewnętrznej, posiadając swoiste podgrupy środowiskowe, które z powodzeniem mogłyby być wyodrębnione osobno, tworząc samodzielne czynniki sprawcze. Stąd też należy zdawać sobie sprawę z tego, że każda ze wskazanych grup determinantów może efektywnie zostać scharakteryzowana i doprecyzowana zbiorem dodatkowych wyznaczników

⁶¹T. Olszewski, *Geografia rolnictwa Polski*, PWE, Warszawa 1985, ss. 17-23.

⁶²S. Myczkowski, *Człowiek. Przyroda. Cywilizacja. Kształtowanie zasobów przyrody oraz ochrona biosfery*, PWN, Warszawa 1976, s. 290.

i wskaźników, tworzących swoiste „dookreślniki” stanu bezpieczeństwa gospodarczego⁶³.

Oczywiste jest, że wskazane determinanty nie są jedynymi występującymi w literaturze przedmiotu, gdyż z uwagi na różnorodność opracowań i podejść do problemu można spotkać inne zbiory czynników warunkujących bezpieczeństwo gospodarcze państwa, a potwierdzeniem tego są treści zawarte w tabeli 1.2.

Po wskazaniu i krótkim omówieniu zasadniczych czynników wpływających na kształtowanie stanu wyjściowego bezpieczeństwa gospodarczego, a tym samym bezpieczeństwa narodowego, można przejść do identyfikacji funkcji, jaką pełni ten ważny segment bezpieczeństwa w całym systemie zarządzania bezpieczeństwem narodowym.

Tabela 1.2

Klasyfikacja determinant bezpieczeństwa gospodarczego

| Kryterium | Rodzaje determinant |
|------------------------------|---|
| Źródło (pochodzenie) | – wewnętrzne – zewnętrzne |
| | – endogeniczne (pochodzące z wewnątrz) – egzogeniczne (pochodzące z zewnątrz) |
| | – własne – obce |
| | – polityczne – prawne – militarne – technologiczne – ekonomiczne – społeczne – kulturowe – ekologiczne – geograficzne – inne |
| Zasięg (skala) oddziaływania | – międzynarodowe – krajowe – regionalne – lokalne |
| | – megaekonomiczne – makroekonomiczne – mezoekonomiczne – mikroekonomiczne |

⁶³ Por. A. Dziurny, *Model ...*, op. cit., s. 406.

Tabela 1.2 (cd.)

| | |
|---|--|
| Przedmiotowe | <ul style="list-style-type: none"> – rolne i żywnościowe – przemysłowe – logistyka (transport, infrastruktura) – środowisko naturalne – surowcowe i energetyczne – finansowe – informatyczne – budżetowe – walutowe – inne |
| Charakter | <ul style="list-style-type: none"> – wspólne (ogólne) – specyficzne (odrębne) |
| | <ul style="list-style-type: none"> – ilościowe – jakościowe |
| Sprzyjanie bezpieczeństwu | <ul style="list-style-type: none"> – sprzyjające – neutralne – niesprzyjające (zagrożenia) |
| Możliwość kształtowania | <ul style="list-style-type: none"> – kształtowlne – częściowo kształtowlne – niekształtowlne |
| Rozpoznanie | <ul style="list-style-type: none"> – rozpoznane – częściowo rozpoznane – nierozpoznane |
| Ranga (waga) | <ul style="list-style-type: none"> – o dużej randze (najważniejsze) – o przeciętnej randze – o małej randze |
| Dynamika, zmiany (w ujęciach względnym i bezwzględny) | <ul style="list-style-type: none"> – o rosnącym znaczeniu – o niezmiennym się znaczeniu – o malejącym znaczeniu |
| | <ul style="list-style-type: none"> – zmieniające się szybko – zmieniające się powoli – niezmiennym się, stabilne (w danym okresie) |

Źródło: Por. I. Jaźwiński, *Determinanty kształtowania polskiego bezpieczeństwa gospodarczego. Wybrane aspekty*, [w:] Przegląd Strategiczny, 2001, nr 1, ss. 62-63.

Z jego miejsca i roli w ogólnym, realnym modelu zarządczym bezpieczeństwa kraju wynika bezpośrednio, że funkcje te muszą być tożsame z ogólnymi społeczno-politycznymi funkcjami państwa, z tym że ich zakres i intensywność realizacji wynikać będzie z ich umiejscowienia w ogólnej polityce i strategii bezpieczeństwa realizowanej przez organa władzy państwowej i inne podmioty odpowiedzialne za stan bezpieczeństwa kraju i jego obywateli.

Patrząc zatem na funkcje państwa jako na *całokształt działalności w określonej sferze życia społecznego*⁶⁴ przez pryzmat gospodarki, jej specyfiki, roli, zadań i miejsca w kształtowaniu stabilności i bezpieczeństwa narodowego oraz zapewnienia jego obywatelom dobrobytu, wypada wskazać na trzy grupy funkcji bezpieczeństwa ekonomicznego.

Pierwszą z nich tworzą funkcje wymieniane ze względu na przestrzenny (terytorialny) zasięg działania państwa. Są to: *funkcja zewnętrzna*, której treść jest ukierunkowana na różne formy działalności państwa w stosunkach międzynarodowych (np. międzynarodowych stosunkach ekonomicznych, w tym przede wszystkim handlu zagranicznego, przepływów finansowych, przepływów kapitału ludzkiego) oraz *funkcja wewnętrzna* opisywana przez regulowanie stosunków wewnątrzpaństwowych (czyli aspekty organizacyjno-prawne warunków gospodarowania) i organizowanie wybranych dziedzin życia społecznego (w tym przypadku – aspekt ekonomiczny).

Na drugą grupę funkcji składają się te, których identyfikacja jest oparta o dziedziny działalności państwa. Do zbioru tych funkcji zaliczyć trzeba cztery funkcje: *zewnętrzną*, *wewnętrzną*, *gospodarczo-organizatorską* oraz *socjalną*. Pierwsza odnosi się do utrzymywania stosunków ekonomicznych z innymi państwami i organizacjami międzynarodowymi o charakterze biznesowym (np. Międzynarodowy Fundusz Walutowy, Europejski Bank Odbudowy i Rozwoju, Bank Światowy itp.) w celu ochrony interesów narodowych/państwowych. Funkcja wewnętrzna skupia się na zapewnieniu bezpieczeństwa i porządku publicznego wewnątrz państwa ukierunkowanego na swobodę prowadzenia działalności gospodarczej przez podmioty gospodarcze, poprzez m.in. istnienie różnego rodzaju organów kontrolnych i nadzorczych, jak np. Najwyższa Izba Kontroli, Komisja Nadzoru Finansowego, Urząd Kontroli Konkurencji i Konsumentów itp. Trzecia z funkcji, czyli gospodarczo-organizatorska, jak wynika z samej jej nazwy, będzie skupiona wokół działań mających na celu realne wpływanie na procesy i zjawiska ekonomiczne poprzez prowadzenie szeroko rozumianej polityki gospodarczej. Jej istota jest zatem bliska sedna ekonomicznej funkcji regulacyjnej lub inaczej nazywanej funkcji organizacyjno-prawnej państwa w sferze gospodarczej, wykorzystującej całą paletę nakazów, zakazów, zaleceń, postulatów mających na celu stworzenie przyjętej przez rząd struktury systemu społeczno-ekonomicznego. W ramach czwartej i ostatniej sfery aktywności, wskazanej wg dziedziny działalności, czyli funkcji socjalnej, państwo będzie podejmować działania zmierzające do zapewnienia bezpieczeństwa ekonomicznego na poziomie indywidualnym, a więc ukierunkowanym na zagwarantowanie minimum egzystencji jednostek i grup społecznych.

⁶⁴ *Spółeczeństwo i polityka. Podstawy nauk politycznych*, red. K.A. Wojtaszczyk, W. Jakubowski, Ofic. wyd. ASPRA-FR, Warszawa 2003, ss. 233-234.

Grupę trzecią, wskazaną z uwagi na cel działania, tworzą funkcje: adaptacyjna, regulacyjna oraz innowacyjna. Funkcja pierwsza – adaptacyjna – skupia się na działalności zmierzającej do podejmowania aktywności ukierunkowanej na przystosowanie (państwa i społeczeństwa) do zmieniającej się sytuacji geopolitycznej i uwarunkowań cywilizacyjnych, determinującej kształt i rodzaj aktywności ekonomicznej poszczególnych podmiotów i grup społecznych, tak o charakterze narodowym, jak i międzypaństwowym. Treść regulacyjnej funkcji państwa sprowadza się do wpływania na normy i zasady życia społecznego i zachodzące w państwie procesy społeczne, ukierunkowane na realizację zadań gospodarczych i kształtowanie polityki gospodarczej z wolą i kierunkami określonymi przez suwerena (naród). Ostatnią z grupy funkcji tzw. „celowych” państwa jest funkcja innowacyjna. Działalność realizowana w ramach tej funkcji jest z kolei ukierunkowana na inicjowanie nowych procesów i przemian społecznych w środowisku gospodarczym, zmierzających zasadniczo do umocnienia posiadanej międzynarodowej pozycji konkurencyjnej bądź to uzyskania przewagi konkurencyjnej na międzynarodowym rynku towarów i usług, tworząc tym samym trwałe fundamenty umacniania bezpieczeństwa gospodarczego państwa.

Choć wskazane trzy grupy funkcji decydujące o sposobie kształtowania sfery zarządczej bezpieczeństwa gospodarczego nie są jedynymi spotykanymi w literaturze przedmiotu, to wydaje się, iż z uwagi na kontekst prowadzonych rozważań są one na chwilę obecną wystarczające i dobrze opisują materię dociekań. Trzeba jednak mieć na względzie, że na sposób ich wypełnienia zawsze będzie miał przemożny wpływ panujący w państwie „reżim” polityczny, czyli styl rządzenia, na który składa się ogół metod i narzędzi, jakimi posługuje się aparat państwowy, kierując potrzebami wielkich grup społecznych. W przypadku zarządzania bezpieczeństwem gospodarczym przez współczesne, zazwyczaj demokratyczne, państwa będziemy mieli najczęściej do czynienia z wykorzystywaniem szerokiego spektrum narzędzi i instrumentów należących do szeroko rozumianej polityki ekonomicznej, w tym przede wszystkim tej o charakterze fiskalnej, monetarnej i dochodowej, oczywiście z uwzględnieniem i przestrzeganiem trzech podstawowych zasad: suwerenności narodu, pluralizmu (politycznego, społecznego, ekonomicznego i politycznego) oraz podziału władzy (najczęściej na: prawodawczą, wykonawczą i sądowniczą). Z perspektywy bezpieczeństwa gospodarczego, jego poziomu i przyjętego sposobu kształtowania ważne jest także utrwalanie takich podstawowych wartości konstytuujących podstawy gospodarki rynkowej, jak: wolność, równość, sprawiedliwość, ład i porządek, leżące u podstaw ogólnego bezpieczeństwa państwa i jego obywateli⁶⁵.

⁶⁵ Por. A. Urbanek, *Państwo jako podmiot bezpieczeństwa narodowego – ujęcie dziedzinowe*, [w:] *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, red. A. Urbanek, Wyd. Społeczno-Prawne, Słupsk 2013, s. 18.

Traktując zaś bezpieczeństwo ekonomiczne państwa w ujęciu procesowym, w kontekście funkcjonalno-zarządczym, należy zawsze dążyć do ujęcia funkcji zarządzania nim jako celu stałego osiągnięcia „bezpieczeństwa ekonomiczno-społecznego, definiowanego jako niezakłócone funkcjonowanie społeczności i gospodarki w wymiarze jednostkowym i organizacyjnym, stymulowane rozwojowo, zapewniające możliwość uczenia się, dzielenia i wykorzystania wiedzy, dążąc do zrównoważonego zaspokajania potrzeb”⁶⁶. Samo zaś określenie „niezakłócone” w przedstawionym powyżej kontekście rozumowania winno być traktowane jako znajdujące się w dopuszczalnych granicach, określonych wcześniej przez odpowiednie gremia decyzyjne odpowiedzialne za jego zapewnienie. Zmienność poziomów bezpieczeństwa, wynikająca z jego natury i warunków otoczenia, sprawia, że zasadniczym imperatywem zarządczym winno być w jego przypadku przeciwdziałanie utracie sterowalności i zdolności przewidywania zagrożeń.

1.4. Zarządzanie bezpieczeństwem gospodarczym – realia polskiej polityki

Starając się opisać w sposób stosunkowo pełny problematykę zarządzania bezpieczeństwem gospodarczym w Polsce, nie można pominąć tak ważnego aspektu, jak praktyczna strona polityki w tym obszarze. Jakie jest zatem podejście władz do tego elementu polskiej racji stanu? Studiując materiały zawarte na oficjalnych stronach Ministerstwa Gospodarki, opisujących i charakteryzujących problematykę bezpieczeństwa gospodarczego, dowiadujemy się, że bezpieczeństwo to jest jednym z sześciu priorytetów strategicznych działalności wspomnianego ministerstwa. Tak więc można powiedzieć, że za kwestie kształtowania i zapewnienia fundamentów ekonomicznych stabilności naszego kraju odpowiada Minister ds. Gospodarki, który to w ramach zabezpieczenia bezpieczeństwa gospodarczego kraju realizuje przedsięwzięcia zmierzające do⁶⁷:

- dywersyfikacji źródeł i kierunków dostaw nośników energii oraz rozbudowy infrastruktury sieciowej kraju, m.in. poprzez rozwój technologii niskoemisyjnych, zwiększania roli biopaliw w gospodarce, wspierania rozwoju systemów przesyłowych energii elektrycznej, gazu ziemnego, ropy naftowej, monitorowania systemu zapasów ropy naftowej, produktów naftowych i gazu ziemnego;

⁶⁶ K. Raczkowski, *Zarządzanie wiedzą w administracji celnej w systemie bezpieczeństwa ekonomiczno-społecznego*, Difin, Warszawa 2010, s. 132.

⁶⁷ *Bezpieczeństwo gospodarcze*, Ministerstwo Gospodarki [on-line]

<http://www.mg.gov.pl/Bezpieczenstwo+gospodarcze>, 07.12.2015 r., *O bezpieczeństwie gospodarczym*, Ministerstwo Rozwoju, <http://www.mr.gov.pl/>, 12.12.2015 r.

- poprawy efektywności energetycznej, działania w tym zakresie obejmują głównie trzy obszary: zmniejszenie zużycia energii, podwyższenie sprawności wytwarzania energii oraz ograniczenie strat energii w przemyśle i dystrybucji;
- wzrostu wykorzystania energii ze źródeł odnawialnych, w tym biopaliw ciekłych (oznacza to m.in. zwiększenie wykorzystania biomasy, szczególnie biomasy stałej i biogazu do produkcji energii elektrycznej oraz biopaliw transportowych);
- zaspokojenia krajowego zapotrzebowania na węgiel kamienny poprzez wzrost efektywności funkcjonowania górnictwa węgla kamiennego;
- budowy infrastruktury dla energetyki jądrowej (planowane jest wprowadzenie energetyki jądrowej w Polsce od 2021 r.);
- zabezpieczenia potrzeb obronnych państwa, w tym w zakresie przygotowania gospodarki do funkcjonowania w warunkach zagrożenia bezpieczeństwa i w czasie wojny;
- zapewnienia bezpieczeństwa międzynarodowego łańcucha dostaw towarów o znaczeniu strategicznym i skutecznej kontroli obrotu produkowanymi w kraju oraz importowanymi towarami i technologiami „wrażliwymi”.

W celu sprawnej realizacji wskazanych zadań, zgodnie z zapisami regulującymi działalność merytoryczną ministerstwa, wśród jego komórek funkcjonalnych znajduje się Departament Bezpieczeństwa Gospodarczego (DBG), który odpowiada za⁶⁸:

- przygotowania obronne w dziale administracji rządowej – gospodarka;
- koordynację działań w zakresie zarządzania kryzysowego oraz współpracę międzynarodową w tym zakresie;
- problematykę rezerw strategicznych, kontrolę obrotu z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa;
- współpracę międzynarodową w dziedzinie przemysłu obronnego i kontaktów z NATO;
- prowadzenie spraw w zakresie działania ministra jako organu wyższego stopnia w sprawach należących do właściwości Urzędu Dozoru Technicznego;
- realizację zadań wynikających z członkostwa Rzeczypospolitej Polskiej w międzynarodowych organizacjach i w reżimach nieproliferacyjnych, jak: Porozumienie z Wasseenaar, Grupa Australijska, Reżim Kontroli Technologii Rakietowych, Grupa Dostawców Jądrowych, Organizacja ds. Zakazu Broni

⁶⁸ *Regulamin organizacyjny Ministra Gospodarki*, załącznik do Zarządzenia Ministra Gospodarki z dnia 16 listopada 2012 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Gospodarki, Dz. U. MG z dnia 21 grudnia 2012 r. poz. 24, s. 11.

Chemicznej, Konwencji o zakazie broni biologicznej i toksynowej, OBWE i ONZ.

W obszarze bezpośredniego zainteresowania wspomnianego departamentu są także przedsięwzięcia związane z restrukturyzacją przemysłu obronnego, wykonywaniem działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, amunicją oraz wyrobami i technologiami specjalnymi, a także używaniem materiałów wybuchowych przeznaczonych do użytku cywilnego.

Prowadzi on również sprawy z zakresu bezpieczeństwa technicznego i przemysłowego, w tym związanego z wymaganiami dla wybranych grup wyrobów, dozorem technicznym oraz bezpieczeństwem i higieną pracy, nieobjętego kompetencjami innych departamentów.

Ważkim aspektem działalności Departamentu Bezpieczeństwa Gospodarczego Ministerstwa Gospodarki jest także to, iż jego pracownicy biorą udział w pracach wybranych komitetów i grup roboczych Komisji Europejskiej, Rady Unii Europejskiej.

Starając się niejako uszczegółwić zakres odpowiedzialności omawianego podmiotu administracji rządowej, należy wskazać, że jako komórka wiodąca w zakresie bezpieczeństwa gospodarczego państwa, realizuje on następujące procesy⁶⁹:

- pozamilitarne przygotowania obronne;
- ochrona obowiązkowa obszarów, obiektów, urządzeń i transportów ważnych dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa;
- ustalanie terenów zamkniętych w odniesieniu do przedsiębiorców będących we właściwości Ministra Gospodarki;
- zarządzanie kryzysowe;
- prowadzenie polityki państwa w zakresie rezerw strategicznych;
- prowadzenie spraw dotyczących problematyki gospodarczo-obronnej rozpatrywanej w ramach Zespołu Trójstronnego ds. Społeczno-Gospodarczych Warunków Restrukturyzacji Zakładów Przemysłowego Potencjału Obronnego;
- wspieranie działań restrukturyzacyjnych podmiotów przemysłowego potencjału obronnego w oparciu o środki z prywatyzacji;
- opiniowanie wniosków o wydanie/zmianę koncesji na wytwarzanie i obrót materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym;
- kontrola przedsiębiorców wykonujących działalność gospodarczą w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym;

⁶⁹ Tamże, ss. 11-12.

- rozpatrywanie odwołań przedsiębiorców od decyzji wojewodów w zakresie pozwoleń na nabywanie, przechowywanie lub używanie materiałów wybuchowych;
- prowadzenie spraw dotyczących NSIP⁷⁰ – wspieranie udziału polskich przedsiębiorców w przetargach organizowanych przez NATO;
- wydawanie zezwoleń, certyfikatów importowych oraz poświadczeń oświadczenia końcowego użytkownika;
- realizacja postanowień Konwencji o zakazie broni chemicznej;
- kontrola zgodności obrotu towarami, technologiami i usługami o znaczeniu strategicznym z wymogami prawnymi;
- współpraca międzynarodowa w zakresie kontroli obrotu towarami i technologiami o znaczeniu strategicznym;
- wydawanie pozwoleń na prowadzenie działalności z wykorzystaniem toksycznych związków chemicznych;
- rozstrzyganie spraw przez Ministra Gospodarki jako organu wyższego stopnia w stosunku do Prezesa Urzędu Dozoru Technicznego.

Jak wynika z zaprezentowanego powyżej stanowiska gremiów decyzyjnych naszego państwa, odnoszących się do kształtowania ekonomicznych fundamentów bezpieczeństwa krajowi, w Polsce mamy do czynienia z podejściem gospodarczo-obronnym w tej materii. Dodatkowo, z analizy rodzaju przedsięwzięć realizowanych przez Ministerstwo Gospodarki wynika, że zapewnienie bezpieczeństwa gospodarczego krajowi, jest utożsamiane przede wszystkim z obszarem tzw. bezpieczeństwa energetycznego. Jak się wydaje takie podejście nie jest na dzień dzisiejszy wystarczające, biorąc chociażby pod uwagę kryzys ekonomiczny z roku 2008, który to przecież nie miał charakteru *energetycznego*, a *spekulacyjno-finansowy*. Dodatkowo, bardzo ograniczony i zbyt wąski sposób postrzegania bezpieczeństwa gospodarczego przez gremia decyzyjne naszego państwa ukazują wyniki dociekań różnorodnej proweniencji teoretyków problemu, chociażby te przywołane we wcześniejszej części niniejszego opracowania.

⁷⁰ NSIP – NATO *Security Investment Programme* to Program Inwestycji NATO w Dziedzinie Bezpieczeństwa stworzony w celu wspólnego finansowania projektów umożliwiających osiągnięcie przez Sojusz Północnoatlantycki określonych zdolności obronnych. Obejmuje on realizację przedsięwzięć związanych z budową, rozbudową i remontami infrastruktury wojskowej oraz pozyskaniem zasobów materialnych niezbędnych do osiągnięcia tych zdolności, [w:] *Inwestycje NATO w Polsce*, <https://www.bbn.gov.pl/>, 29.01.2016.

2. BEZPIECZEŃSTWO SYSTEMÓW LOGISTYCZNYCH

Identyfikacja zagrożeń systemów logistycznych oraz rozpoznania podatności na powstanie sytuacji niebezpiecznych w takich sektorach bezpieczeństwa gospodarczego, jak np. transport (samochodowy i kolejowy), gospodarka magazynowa, żywność, ekologia – pozwala na racjonalizację wyboru środków (organizacyjnych, prawnych, technicznych) zapewniających funkcjonowanie (zgodnie z przeznaczeniem) systemu w niebezpiecznym środowisku. Niekwestionowany udział w zapewnieniu pożądanego poziomu bezpieczeństwa systemów logistycznych zabezpieczających funkcjonowanie dziedzin, sektorów, transsektorów bezpieczeństwa ma współdziałanie, które ma strukturę synchronistyczną, tj. zmieniającą się w czasie. Współpraca, stopień synchronizacji elementów w systemach i podsystemach decydują o niezawodności realizowanych procesów logistycznych i o wielkości efektu synergicznego.

2.1. Logistyczne uwarunkowania funkcjonowania podmiotu bezpieczeństwa

Zapewnienie bezpieczeństwa dowolnego podmiotu indywidualnego lub zbiorowego w ramach zintegrowanego systemu bezpieczeństwa narodowego Polski nie jest możliwe bez konieczności użycia wydzielonych, odpowiednio wyszkolonych i wyposażonych sił i środków, zapewniających przetrwanie i realizację interesów danego podmiotu. Liczba wydzielonych sił i środków na potrzeby sektorów bezpieczeństwa gospodarczego zależy od wielkości zagrożeń zewnętrznych pochodzących z otoczenia systemu, a także zagrożeń wewnętrznych, które są „skumulowane” w nim samym. Ponadto zależy od odporności systemu na zagrożenia (jego niezawodności⁷¹), a także od dysponowanego potencjału wykonawczego i informacyjno-decyzyjnego. Wydzielone zasoby stanowią element systemu bezpieczeństwa gospodarczego w ramach podsystemu kierowania i wykonawczego, w którym jedną z kluczowych funkcji pełni logistyka.

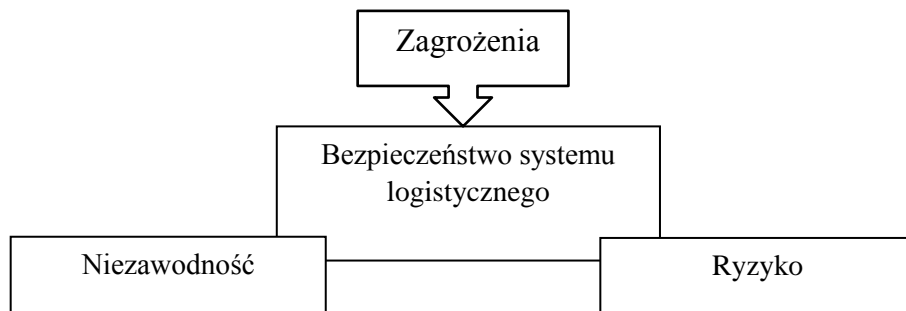
W literaturze przedmiotu logistyka ta jest nazwana „logistyką bezpieczeństwa” lub „logistyką w bezpieczeństwie” i obejmuje wiedzę oraz umiejętności potrzebne do kształtowania racjonalnych strumieni rzeczowych i związanych z nimi strumieni informacji oraz projektowania (kształtowania)

⁷¹ Niezawodność systemu logistycznego to zespół właściwości, które opisują jego gotowość do ciągłego zachowania stanu zdolności podczas wykonywania procesów logistycznych, na określonym poziomie.

struktur i procesów w celu zaspokojenia potrzeb „określonych” podmiotów (instytucji) występujących w systemie bezpieczeństwa narodowego (w tym gospodarczego) pod warunkiem racjonalności nakładów i kosztów. Logistyka systemów bezpieczeństwa, jak każda współczesna organizacja, funkcjonuje w środowisku turbulentnym i trudno przewidywalnym. Te uwarunkowania powodują, że struktura, kompetencje, zarządzanie logistyką bezpieczeństwa itp. są nierozdzielnie związane i zależne od współczesnych paradygmatów bezpieczeństwa, do których zalicza się⁷²:

- wyzwania (sytuacje problemowe generujące dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzygnięciu spraw bezpieczeństwa),
- zagrożenia (pośrednie lub bezpośrednie destrukcyjne oddziaływania na podmiot),
- szanse (niezależne od woli podmiotu okoliczności sprzyjające realizacji interesów oraz osiągnięciu celów podmiotu w dziedzinie bezpieczeństwa),
- ryzyka (możliwości negatywnych dla danego podmiotu skutków własnego działania w sferze bezpieczeństwa).

Należy podkreślić, że ze względu na zagrożenia nie wystarczy posiadać dobrze zorganizowaną logistykę dla podmiotów bezpieczeństwa. Trzeba jeszcze mieć na uwadze sprawnie i skutecznie zorganizowane bezpieczeństwo w logistyce w sensie morfologicznym, funkcjonalnym i informacyjnym. To pozwoli realizować procesy logistyczne na poziomie akceptowalnym dla podmiotu bezpieczeństwa. Mówimy wtedy o bezpieczeństwie logistyki (systemu logistycznego).



Rys. 2.1. Składowe bezpieczeństwa systemu logistycznego

Źródło: opracowanie własne.

⁷² Por. J. Gryz, *Kształtowanie strategicznego zarządzania bezpieczeństwem narodowym*, [w:] *Strategia bezpieczeństwa narodowego Polski*, red. nauk. J. Gryz, PWE, Warszawa 2013, s. 96.

Należy uwzględnić, że w ujęciu systemowym bezpieczeństwo systemu logistycznego dowolnego podmiotu bezpieczeństwa jest związane z: zagrożeniami, niezawodnością⁷³ oraz ryzykiem (rys. 2.1)⁷⁴. Do oceny tych wielkości stosujemy miary ilościowe lub jakościowe, pamiętając o jednolitym podejściu dla określonego systemu logistycznego.

Analiza treści Strategii Narodowych z roku 2003, 2007, 2014 i Białej Księgi z 2013 r., pozwala stwierdzić, że określenie „logistyka”, „logistycznych” i „logistycznego” jest używane dziewięciokrotnie, co świadczy, o niedocenianiu logistyki dla wszelkich działań gospodarczych, ochronnych, obronnych, społecznych (załącznik 2.1). Natomiast w *Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022* 16 razy użyto przytoczonych wyżej określeń. Problem ten poruszył również B. Rzeczyński z Wyższej Szkoły Bezpieczeństwa w Poznaniu, który w artykule *Logistyka w systemie bezpieczeństwa narodowego Polski* napisał: „Można tylko domniemywać, że autorzy i instytucja, która opracowanie dokumentów firmuje, czyli Ministerstwo Spraw Zagranicznych, nie rozumieją aksjologii logistyki i jej decydującej funkcji w realizacji strategii bezpieczeństwa narodowego”⁷⁵.

Logistyka podmiotu bezpieczeństwa jest częścią logistyki bezpieczeństwa gospodarczego, która z kolei jest wkomponowana w strukturę systemu bezpieczeństwa narodowego i zlokalizowana oraz umiejscowiona w podsystemach funkcjonalnych: Ministerstwie Obrony Narodowej, Spraw Wewnętrznych, Skarbu, Administracji i Cyfryzacji, Zdrowia, Finansów, Środowiska, Gospodarki, Rolnictwa i Rozwoju Wsi, Skarbu Państwa, Transportu, Budownictwa i Gospodarki Morskiej, a także Agencji Wywiadu, Służby Wywiadu Wojskowego, Straży Granicznej, instytucjach administracji rządowej i samorządowej, organizacjach pozarządowych, podmiotach usługowych i produkcyjnych.

Liczne autorskie artykuły i monografie⁷⁶, dotyczące logistyki bezpieczeństwa, prowadzą do szeregu następujących wniosków.

Pierwszy. Logistykę bezpieczeństwa, bez względu na jej miejsce funkcjonowania, należy traktować jako system działania, który powinien być

⁷³ Por. P. Sienkiewicz, *Teoria i inżynieria systemów*, [w:] Inżynieria ... op. cit., s. 11.

⁷⁴ Szerzej na temat zagrożeń i ryzyka w następnym podrozdziale.

⁷⁵ B. Rzeczyński, *Logistyka w systemie bezpieczeństwa narodowego Polski*, [w:] *Logistyka* 5/2011, s. 1266.

⁷⁶ Najważniejsze z nich to: *Organizacja i funkcjonowanie systemów logistycznych*, Difin, Warszawa 2011, *Logistyka w bezpieczeństwie* (wyd. 1 i 2), Difin, Warszawa 2010 i 2011, *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa 2015, *Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce*, [w:] *Logistyka* 2011/2, *Logistyka w sytuacjach kryzysowych*, [w:] *Logistyka* 2011/3, *Bezpieczeństwo systemów logistycznych*, [w:] *Gospodarka materiałowa i logistyka* 2014/5.

ujmowany w określonych kategoriach i zależnościach holistyczno-systemowych. Systemy logistyczne Sił Zbrojnych, Policji, Państwowej Straży Pożarnej, Straży Granicznej, podmiotów ratowniczych, dowolnego podmiotu produkcyjnego i usługowego, w logistyce bezpieczeństwa powinny działać zgodnie z jego zasadami organizacyjnymi i funkcjonalnymi.

Wykorzystując „wyróżniki nowoczesnego podejścia systemowego”, można podać następujące cechy praktycznego działania rozpatrywanego systemu⁷⁷: logistykę traktuje się jako obiekt badań i analizy, system logistyczny należy do „większego” systemu (np. systemu logistycznego Sił Zbrojnych, który jest podsystemem logistyki NATO), system logistyczny składa się z podsystemów oraz funkcjonują metody racjonalizacji systemu logistycznego (np. wykorzystanie automatycznej identyfikacji, systemów informatycznych itd.). Każdy proces logistyczny można realizować na kilka sposobów – wariantów (wielowariantowość, np. zaopatrywanie może odbywać się transportem własnym lub zamówionym, zakupy bezpośrednio lub poprzez zamówienie publiczne). Ponadto ma miejsce świadome posługiwanie się modelem systemu logistycznego o określonym poziomie rozdzielczości, co jest niezbędne do rozwiązywania odpowiednich problemów, np. w obszarze kierowania, informatyzacji, jakości, konfiguracji, ryzyka i innych.

Zadania realizowane przez podsystemy logistyczne w logistyce bezpieczeństwa (SLwLB) są wykonywane dzięki racjonalnym funkcjom zarządzania i nowoczesnym instrumentom organizacyjnym oraz regułom decyzyjnym. Jedną z nich są reguły logistyczne, takie jak np. 4W, tzn. strumienie zasileń powinny docierać do miejsca przeznaczenia we właściwym czasie, we właściwych ilościach, we właściwym miejscu i o właściwej jakości. Istotnym problemem jest skoordynowanie przepływu strumienia w celu maksymalnego skrócenia czasu oraz zmniejszenia strat.

Podstawowym zadaniem SLwLB jest zaspokojenie potrzeb podmiotu bezpieczeństwa, tak by mógł on realizować swoje żywotne interesy (dotyczące jego istnienia) i wymagania (np. związane z jakością istnienia, trwania) w czasie pokoju, kryzysu, zagrożenia i wojny.

Drugi. System logistyczny w logistyce bezpieczeństwa, niezależnie od miejsca funkcjonowania (np. w SZ RP, w Policji, w Państwowej Straży Pożarnej, w dowolnym podmiocie) jest przeznaczony dla zaspokojenia potrzeb bezpieczeństwa podmiotu; tworzą go⁷⁸:

- podsystem kierowania – przeznaczony do planowania, organizowania, skoordynowania i monitorowania wysiłku logistycznego oraz utrzymywania wydzielonych zasobów (podległych sił i środków) w odpowiedniej gotowości i zdolności do wykonywania zadań;

⁷⁷ Por. M. Brzeziński, *Systemy w logistyce*, WAT, Warszawa 2007, ss. 22, 82.

⁷⁸ Por. *Doktryna logistyczna SZ RP DD/4*, Sztab. Gen. Warszawa 2004, s. 21.

- podsystem materiałowy – przeznaczony do planowania, organizowania i zaspokajania potrzeb w zakresie realizacji procesu zaopatrywania na rzecz określonego podmiotu (np. wojsk, policji, strażaków, potrzebujących pomocy) oraz świadczenie na ich rzecz usług gospodarczo-bytowych;
- podsystem techniczny – przeznaczony do planowania, organizowania i realizowania przedsięwzięć związanych z eksploatacją sprzętu, maszyn i urządzeń, tj. jego użytkowania oraz zabezpieczenia technicznego, utrzymującego go w odpowiedniej sprawności technicznej;
- podsystem transportu – przeznaczony do planowania, organizowania i realizowania przedsięwzięć związanych z przemieszczaniem i zaopatrzeniem;
- podsystem medyczny – obejmujący obszar z zakresu ewakuacji medycznej oraz logistyki w części dotyczącej sił i środków medycznych, takich jak zaopatrywanie medyczne, ewakuacja poszkodowanych, rannych i chorych;
- podsystem infrastruktury – obejmujący odpowiednie organy kierowania zajmujące się wszystkimi przedsięwzięciami dotyczącymi utrzymania obiektów stacjonarnych, tymczasowych, niezbędnych do zaspokojenia potrzeb kwaterunkowych, przechowywania oraz remontu, sprzętu technicznego i zabezpieczenia.

Relacje łączące elementy systemu logistycznego wynikają z podległości służbowej i funkcjonalnej. Występują ponadto procesy współdziałania i informacyjne wynikające z potrzeby komunikowania.

Trzeci. System logistyczny bezpieczeństwa w bezpieczeństwie gospodarczym możemy również traktować jako zbiór organów kierowania oraz wykonawczych sprzężonych relacjami informacyjnymi i zasileniowymi, przeznaczonych do utrzymania ciągłości procesów logistycznych. Dotyczy to takich instytucji, jak: jednostki wojskowe, komendy główne i podległe im organizacje policji, straży pożarnej, służby granicznej, biura ochrony rządu, obrony cywilnej. Również system logistyczny bezpieczeństwa w bezpieczeństwie gospodarczym traktujemy jako organizację złożoną z organów kierowania oraz jednostek i urządzeń logistycznych sprzężonych ze sobą relacjami, przeznaczoną do realizacji dostaw zaopatrzenia i świadczenia usług logistycznych dla celów szkolenia i zabezpieczenia działań zgodnie z kompetencjami oraz zadaniami.

Można to zapisać jako:

$$SLwLB = \langle E, R \rangle \rightarrow \max C$$

gdzie: E – zbiór elementów systemu SLwLB, R – zbiór relacji (stosunków, sprzężeń), C – cel działania systemu SLwLB, którym jest pożądaný poziom zabezpieczenia interesów podmiotu bezpieczeństwa.

Aktualnie system logistyczny w logistyce bezpieczeństwa jest zbudowany na bazie logistyki stacjonarnej wzmacnianej potencjałem mobilnym przy szerokim wykorzystaniu możliwości i zasobów gospodarki narodowej.

Przykładem systemu logistyki bezpieczeństwa w bezpieczeństwie gospodarczym może być logistyka funkcjonująca w Ministerstwie Spraw Wewnętrznych. Bazując na definicjach i Rozporządzeniu Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych oraz ustawie z dnia 16 marca 2001 r. o Biurze Ochrony Rządu, system logistyczny MSW (SLMSW) składa się z następujących podstawowych podsystemów:

SLMSW = <SLKGP, SLKGPSP, SLKGSZ, SLBOR, SLSOCK;
SLJKGP, SLJKGPSP, SLJKGSZ, SLJBOR, SLJSOCK; SLGK, R>

gdzie: SLKGP – system logistyczny Komendy Głównej Policji;

SLKGPSP – system logistyczny Komendy Głównej Państwowej Straży Pożarnej;

SLKGSZ – system logistyczny Komendy Głównej Straży Granicznej;

SLBOR – system logistyczny Biura Ochrony Rządu;

SLSOCK – system logistyczny Szefa Obrony Cywilnej Kraju;

SLJKGP – system logistyczny jednostek Komendy Głównej Policji;

SLJKGPSP – system logistyczny jednostek Komendy Głównej Państwowej Straży Pożarnej;

SLJKGSZ – system logistyczny jednostek Komendy Głównej Straży Granicznej;

SLJBOR – system logistyczny jednostek Biura Ochrony Rządu;

SLJSOCK – system logistyczny jednostek Szefa Obrony Cywilnej Kraju;

SLGK – system logistyczny gospodarki kraju;

R – zbiór relacji pomiędzy podsystemami oraz pomiędzy systemem i otoczeniem.

Zadania i zakres kompetencyjny MSW wymaga również stworzenia określonego systemu logistycznego, który powinien być dostosowany do zadań, potencjalnych zagrożeń oraz pożądanego poziomu bezpieczeństwa, jaki musi być mu zapewniony. Ilość i jakość środków (organ wykonawczy), niezbędnych do zapewnienia danemu podmiotowi pożądanego poziomu bezpieczeństwa, ich organizacja (organ kierowniczy) po wystąpieniu zagrożenia (zajścia zdarzenia niepożądanego), zależy od jego rodzaju i skali oraz prognozy możliwości wystąpienia również zagrożeń innych rodzajów.

Przykładowo system logistyczny (SL) jednostek policji, państwowej straży pożarnej, straży granicznej, biura ochrony rządu, obrony cywilnej może się składać z następujących podsystemów:

SL= <SZ, SUSB, SRM, SP, ST, SM, SF, SPZ, SE, SO, R>

gdzie: SZ – podsystem zaopatrzenia;
SUSB – podsystem usług socjalno-bytowych;
SRM – podsystem ratownictwa (np. medycznego, technicznego, wodno-nurkowego, wysokościowego, chemicznego);
SP – podsystem produkcji (produkcję należy traktować tak samo jak usługę);
ST – podsystem transportu;
SM – podsystem magazynowania;
SF – podsystem finansowy;
SPZ – podsystem zamówień;
SE – podsystem ekologistyki (logistyki zwrotnej);
SO – podsystem ochrony;
R – zbiór relacji pomiędzy podsystemami oraz pomiędzy systemem i otoczeniem.

W literaturze przedmiotu można znaleźć wiele rodzajów i klasyfikacji systemów logistycznych według różnych kryteriów. Na podstawie kryterium instytucjonalnego, rozpatrując w skali ogólnogospodarczej, można wyodrębnić następujące cztery systemy i podsystemy logistyczne:

- mikrologistyczny, tj. system obejmujący wszystkie procesy logistyczne wewnątrz jednostkowych organizacji, np. system logistyczny podmiotu gospodarczego, instytucji, systemu gospodarczego, np. komendy powiatowej policji (kpp) czy komendy powiatowej państwowej straży pożarnej (KP PSP);
- metalogistyczny, tj. system stanowiący integrację podsystemów mikrologistycznych kooperujących systemów gospodarczych (łańcuch logistyczny), np. system bezpieczeństwa powiatu stworzony przez KPP; KP PSP, jednostkę wojskową itp.;
- makrologistyczny, będący wyrazem integracji procesów logistycznych w skali całej gospodarki (np. system funkcjonujący w ramach krajowego centrum koordynacji ratownictwa i ochrony ludności);
- zewnętrzny system logistyczny (międzysystem), integrujący procesy logistyczne między dostawcami a odbiorcami.

2.2. Klasyfikacja zagrożeń w kontekście bezpieczeństwa systemów logistycznych

Każde działania w logistyce zarówno w sferze planowania, jak i realnej są obarczone ryzykiem, które może być wywołane pojawiającym się niebezpieczeństwem (zagrożeniami) bądź zakłóceniami.

Wartość ryzyka (jego ewaluacja) w systemach logistycznych możemy zapisać jako⁷⁹:

$$\text{RYZYKO} = f(\text{ZAGROŻENIE, PODATNOŚĆ, KONSEKWENCJE}) \quad (1)$$

lub

$$\text{VaR} = P \cdot S_x \cdot P_d \cdot E_x \quad (2)$$

gdzie: P – prawdopodobieństwo wystąpienia ryzyka,

VaR – ewaluacja ryzyka,

S_x – wartość możliwych strat,

P_d – podatność na ryzyko określającą stopień, w jakim dany system (obiekt) jest podatny na zagrożenia i poziom potencjalnych skutków,

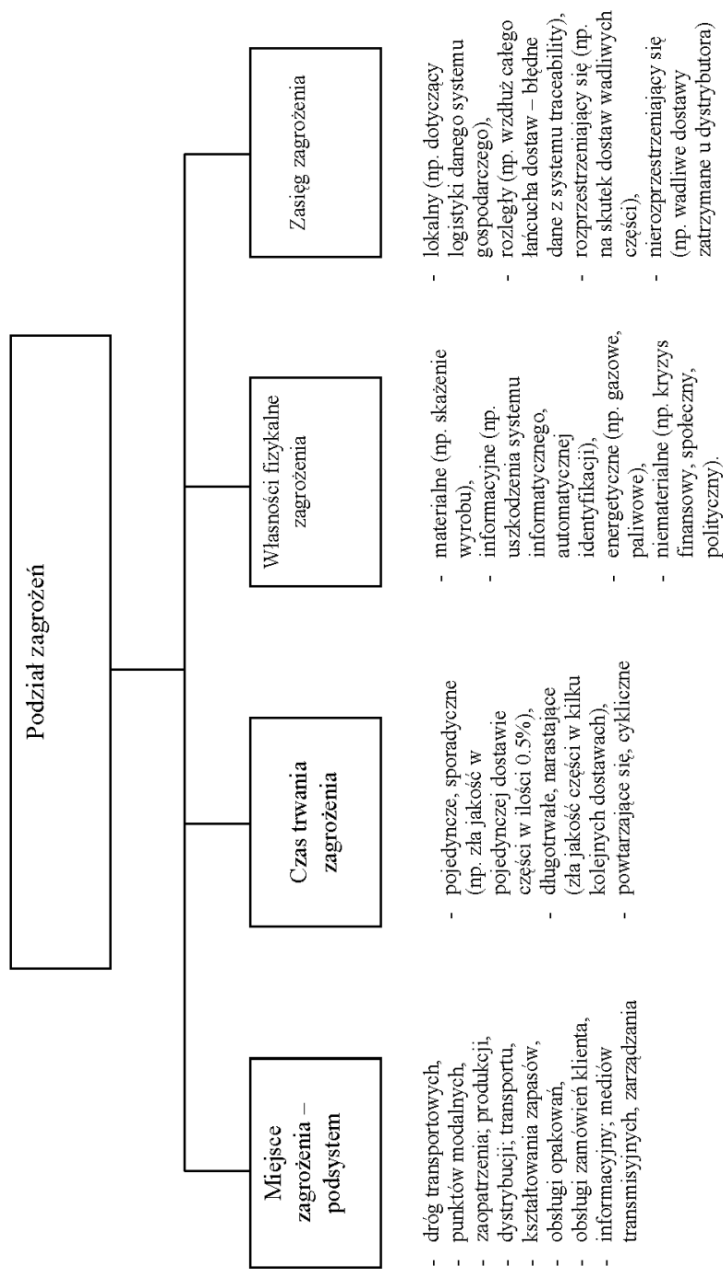
E_x – współczynnik ekspozycji określający stopień, w jakim system (obiekt) jest ważny z punktu widzenia wystąpienia zagrożenia.

Zarówno w formule (1), jak i (2) istotnym czynnikiem są zagrożenia, które mają istotny wpływ na bezpieczeństwo systemu logistycznego i dlatego konieczne jest przewidywanie ich wystąpienia na podstawie danych historycznych oraz ich wykrywanie (monitorowanie) i identyfikacja. Tak zebrane dane z wykorzystaniem systemów informatycznych (np. OLAP⁸⁰) pozwalają prognozować skutki, przewidywać siły i środki do ich przeciwdziałania oraz sposoby prowadzenia działań ratowniczych.

Zastosowanie modeli matematycznych pozwala na ocenę ilościową zagrożeń, a wykorzystanie technik heurystycznych (w tym oceny ekspertów) pomaga dokonać ich ewaluacji jakościowej.

⁷⁹ P. Sienkiewicz, H. Świeboda, *Ryzyko w inżynierii systemów bezpieczeństwa*, [w:] *Inżynieria systemów bezpieczeństwa*, red. nauk. P. Sienkiewicz, PWN, Warszawa 2015, s. 41; P. Zaskórski, *Informacja ciągłości działania determinantą bezpieczeństwa organizacji*, [w:] *Nie-bezpieczny świat Systemy Informacja Bezpieczeństwo*, AON, Warszawa 2015, s. 449.

⁸⁰ OLAP (ang. *Online Analytical Processing*) są narzędziem pozwalającym na wielowymiarową analizę danych biznesowych zgromadzonych w hurtowni danych oraz na spersonalizowany dostęp do wyników analizy za pomocą wybranych mediów komunikacji. Umożliwiają analizę danych na najniższym poziomie szczegółowości, jak również pozwalają na różnorodne uogólnienia i podsumowania danych. Jeśli dane w bazie są wstępnie przetworzone, przeliczone i przygotowane do prezentacji, to wydajność wyszukiwania i szybkość reakcji na zapytanie użytkownika jest maksymalna. OLAP pozwala na wielowymiarową analizę danych zainicjowaną przez końcowego użytkownika z jego stacji roboczej w trakcie pracy na komputerze, obejmuje on także możliwości manipulacji wymiarami oraz złożone mechanizmy raportowania i wizualizacji danych, [w:] A. Szymonik, *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Difin, Warszawa 2011, s. 260.



Rys. 2.2. Zagrożenia dla systemów logistycznych

Źródło: opracowano własne.

Niezwykle pomocna w ocenie „szkodliwości” zagrożeń dla bezpieczeństwa systemu logistycznego jest ich pełna identyfikacja poprzez podział (klasyfikację) z uwzględnieniem miejsca zagrożenia, czasu trwania, własności fizykalnych, zasięgu.

Zagrożenia dla funkcjonowania systemów logistycznych można podzielić na cztery grupy.

Do pierwszej grupy zalicza się klęski żywiołowe i zdarzenia wywołane przyczynami cywilizacyjnymi, takimi jak 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, chemiczne oraz katastrofy górnicze, budowlane, a także komunikacyjne, awarie sieci energetycznych.

Do drugiej grupy zalicza się zdarzenia godzące w porządek konstytucyjny państwa (państw), terroryzm, blokady dróg, nielegalne demonstracje, konflikty na tle etnicznym, masowa migracja.

W trzeciej grupie wyróżnia się mechanizmy, które mają na celu niszczenie bądź zniekształcanie informacji przesyłanej, przetwarzanej, przechowywanej dla potrzeb systemów logistycznych. 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 logistycznych. 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 logistyczny, zakłócając przepływ strumienia rzeczowego i informacji.

Zakłócenia te można podzielić ze względu na (rys. 2.2)⁸¹:

- miejsce zagrożenia – podsystem:
 - ✓ dróg wszystkich gałęzi transportu (tj. drogowego, kolejowego, powietrznego, wodnego, morskiego),
 - ✓ punktów modalnych⁸² sieci logistycznej nazywanych często punktami transportowymi (np. magazyny, samodzielne punkty kontenerowe, lotniska, porty, centra logistyczne itp.),
 - ✓ urzędzeń pomocniczych ułatwiających obsługę dróg i punktów transportowych,

⁸¹ Por. P. Sienkiewicz, *Teoria i inżynieria bezpieczeństwa systemów*, [w:] Zeszyty Naukowe AON nr 1(66)2007, s. 254.

⁸² Mianem punktów modalnych (najbardziej prawdopodobnych) sieci logistycznej określa się wszystkie miejsca zatrzymywania się produktów, tzn. magazyny, punkty i węzły transportowe oraz fabryki, sieci dystrybucji itd.

- ✓ zarządzania (np. brak pełnej identyfikacji i skutków zagrożeń, przeszacowanie możliwości, niewłaściwa interpretacja wyników, brak narzędzi do optymalizacji i symulacji działań, nieuwzględnienie rosnących cen energii i transportu, niespodziane upadłości usługodawców logistycznych, brak kontroli nad pracownikami, którzy postępują nieetycznie, dopuszczając się defraudacji mienia lub innych nadużyć między innymi przy wyborze dostawcy),
- ✓ zaopatrzenia (np. wydłużone, nieoptymalne i absorbujące nadmiernie kadre kierowniczą procedury przetargowe i zakupowe, niespójne kryteria wyboru dostawcy, wybór dostawcy jedynie na podstawie najniższej ceny, nieterminowość procesu zakupowego, zła jakość, cena, ilość, niewłaściwy asortyment, przekupstwo, łapownictwo, brak możliwości pozyskania komponentów do wytwarzania, brak buforowego zapasu),
- ✓ produkcji (np. niedomagania systemów wytwarzania, zniszczenia, ubytki, kradzieże zasobów, brak dostępności fachowego personelu, przerwy produkcyjne, awarie, pożary, powodzie, katastrofy, sfalszowanie produktu),
- ✓ dystrybucji (np. zignorowanie nowych produktów, nowych producentów, kradzieże, warunki atmosferyczne, zła jakość wyrobów gotowych, kryzys gospodarczy, lekceważenie zarządzania relacjami z klientem i przepływem wyrobów w łańcuchu dostaw),
- ✓ transportu (np. zakłócenia spowodowane pożarami, eksplozją, wypadkiem środka transportu, zmyciem 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. zniszczenie wyrobów w transporcie na skutek złego doboru opakowań, niedostarczenie opakowań na czas na skutek złych warunków klimatycznych, zanieczyszczenie środowiska),
- ✓ obsługi zamówień klienta (np. zakłócenia spowodowane brakiem zapasów, błędnymi zamówieniami i fakturami, brakiem możliwości zlokalizowania produktu, nieterminowością, a także uszkodzone wyroby dostarczone do klienta, brak reakcji na reklamacje i opóźnienia, pożary, kradzieże, zniszczenia),
- ✓ informacyjny (np. utrata poufności, integralności oraz możliwości dysponowania, naturalne zagrożenia, jak pożary, zakłócenia klimatyczne, elektrostatyka, ataki bierne i aktywne, przypadkowe błędy);

- czas trwania:
 - ✓ krótkotrwałe, sporadyczne,
 - ✓ długotrwałe, narastające,
 - ✓ powtarzające się, cykliczne;
- własności fizykalne:
 - ✓ materialne (np. wprowadzenie składnika powodującego tzw. bioterroryzm, zła jakość procesów produkcji, transportu czy magazynowania, wynikająca np. z różnorodności stosowanych systemów jakości w tej samej branży, np. ISO, HACCP⁸³, BRC⁸⁴, IFS⁸⁵, SQF⁸⁶),

⁸³ HACCP pochodzi od nazwy w języku angielskim (*Hazard Analysis and Critical Control Points*), co tłumaczy się jako: Analiza Zagrożeń i Krytyczne Punkty Kontroli. Termin ten określa system postępowania w firmach mających do czynienia z żywnością, służący zapewnieniu bezpieczeństwa zdrowotnego tej żywności, [w:] A.J. Wiktor, *Charakterystyka systemu HACCP*, <http://www.polhaccp.com/podstawy.htm>, 05.01.2014.

⁸⁴ British Retail Consortium (BRC) opracowało w 1998 roku Standardy i Procedury dla firm dostarczających żywność pod marką własną do sieci brytyjskich hipermarketów. Obecnie obowiązuje nowe wydanie normy BRC Nr 6/2011 roku. Standard ten jest znany nie tylko w całej Europie, ale również na pozostałych kontynentach. Standard BRC sumuje wymagania zawarte w normie ISO 9001, Codex Alimentarius, GMP i GHP oraz definiuje wymagania, które muszą zagwarantować bezpieczeństwo i wymagany, powtarzalny poziom jakości wyrobu gotowego. Dodatkowym elementem, na który zwraca się dużą uwagę jest zgodność wyrobu z prawem żywnościowym, [w:] *Globalny BRC Bezpieczeństwa Żywności Standardowy*, <http://www.haccp-iso22000.pl/brc.html>, 05.01.2014.

⁸⁵ IFS – *International Food Standard* to jednolity standard bezpieczeństwa opracowany dla wszystkich producentów żywności i uczestników łańcucha żywnościowego, a w szczególności dla zakładów spożywczych dostarczających żywność do sieci handlowych pod marką własną. Standard został opracowany w 2000 roku w ramach Global Food Safety Initiative przez zrzeszenia Federalnych Związków Handlowych BDH (Niemcy) oraz Federacji Stowarzyszeń Handlu i Dystrybucji FCD (Francja). Podstawowym zamysłem twórców standardu było ujednoczenie zasad oceny, procedur auditowych oraz reguł kwalifikowania dostawców. Standard został opracowany jako narzędzie do okresowej, niezależnej i obiektywnej oceny producentów i dystrybutorów żywności. Obecnie IFS staje się przepustką do współpracy ze znaczną częścią sieci handlowych Europy Zachodniej. Szczególną popularnością cieszy się w Niemczech i we Francji, jest zatem wymagany przez sieci handlowe pochodzące z tego właśnie obszaru, [w:] *IFS International Food Standard*, <http://www.bheuroconsult.pl>, 06.01.2014.

⁸⁶ SQF jest przeznaczony dla zakładów przemysłu spożywczego (SQF 2000), jak również dla gospodarstw rolnych (SQF 1000). Jest jednym z globalnych schematów bezpieczeństwa i jakości żywności akceptowanych przez GFSI. Jest on popularny zwłaszcza w USA i Australii. System jest bardzo atrakcyjny ze względu na szeroką gamę informacji dostępnych na stronie internetowej www.sqfi.com wraz z całkowitą, bezpłatną dokumentacją: kodem, przewodnikiem, zasadami i przebiegiem audytu oraz inne. SQF 1000/2000 jest podzielony na 3 poziomy certyfikujące: poziom 1 – podstawy

- ✓ informacyjne (np. uszkodzenia systemu informatycznego, automatycznej identyfikacji, nieprawdziwe dane o produkcji na opakowaniach),
- ✓ energetyczne (np. gazowe, paliwowe),
- ✓ niematerialne (np. kryzys finansowy, polityczny, społeczny);
- zasięg:
 - ✓ lokalny, dotyczący logistyki danego systemu gospodarczego, będącego np. pojedynczym ogniwem łańcucha dostaw,
 - ✓ rozległy wzdłuż całego łańcucha dostaw w wymiarze lokalnym lub globalnym,
 - ✓ rozprzestrzeniający się (np. na skutek dostawy zatrutej żywności),
 - ✓ nierozprzestrzeniający się (np. na skutek zatrzymania wysyłki wadliwych produktów do masowych odbiorców).

Ciekawą typologię zagrożeń bezpieczeństwa, którą można wykorzystać w logistyce bezpieczeństwa zaprezentował P. Sienkiewicz w artykule *Teoria i inżynieria bezpieczeństwa systemów*⁸⁷. Zagrożenia bezpieczeństwa systemów zostały zaprezentowane w trzech grupach: związane z postępowaniem człowieka, niezwiązane z postępowaniem człowieka, katastrofy naturalne.

Zaprezentowane podziały zakłóceń pokazują szerokie spektrum i wieloaspektowość niekorzystnych działań, jakie mogą wystąpić w funkcjonowaniu procesów w łańcuchu dostaw. Z punktu widzenia funkcji i poziomów zarządzania zakłócenia mogą wynikać z:

- niewłaściwych założeń na potrzeby planowania strategicznego, niewłaściwej oceny opcji strategicznych;
- utraty reputacji i odpowiedzialności społecznej przez zdarzenia wywołujące długotrwałą krytykę ze strony rządu lub ze strony mediów międzynarodowych;
- nieodpowiednich lub zawodnych procesów wewnętrznych, stosowanych technologii produkcji, magazynowania i dystrybucji, działań pracowników, niewłaściwie funkcjonujących procesów;
- zewnętrznych, nieprzewidywalnych działań klientów, dostawców, konkurentów, nowych uczestników rynku, usług substytucyjnych, a także ze zmian w otoczeniu zewnętrznym;
- złych relacji z interesariuszami, niewłaściwej struktury organizacyjnej systemu delegowania uprawnień i odpowiedzialności, braku lub niewła-

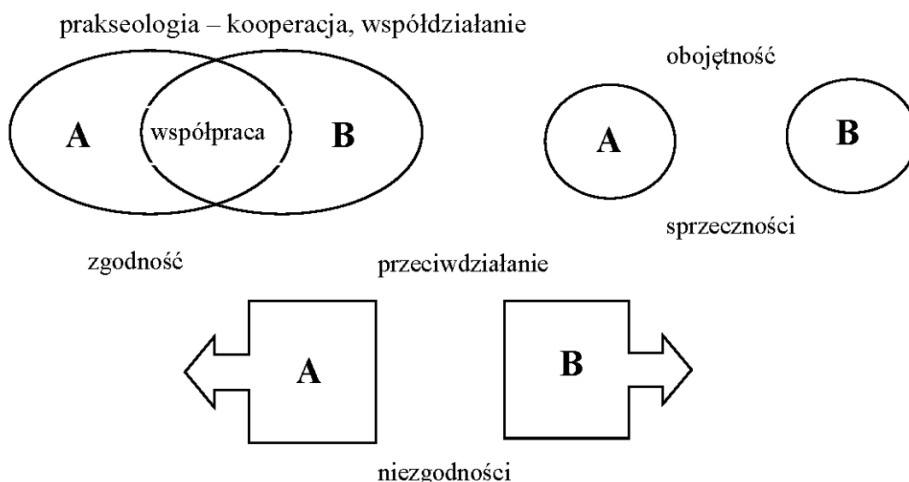
bezpieczeństwa żywności, programy wstępne, poziom 2 – certyfikowany system HACCP, poziom 3 – Całkowity system zarządzania bezpieczeństwem i jakością, [w:] *Certyfikacja zgodności z normą Safe Quality Food (SQF)*, <http://www.sigmaquality.pl/> 26.07.01.2014.

⁸⁷ Por. P. Sienkiewicz, *Teoria i inżynieria systemów*, [w:] *Inżynieria systemów bezpieczeństwa*, PWE, Warszawa 2015, s. 9.

- ściwych zasad postępowania pracowników i kierowników komórek organizacyjnych;
- niezgodności z przepisami prawa powszechnie obowiązującego, regulacji wewnętrznych oraz zobowiązań umownych,
 - niedopowiedniego poziomu bezpieczeństwa fizycznego aktywów i osób;
 - niewłaściwego zarządzania zasobami teleinformatycznymi, wynikającymi z nieaktualnej i przestarzałej technologii teleinformatycznej oraz braku spójności strategii teleinformatycznej, a także spowodowanymi zakłóceniami w funkcjonowaniu infrastruktury teleinformatycznej;
 - funkcjonowania środowiska naturalnego – trwałe, poważne zniszczenie środowiska; utrata użyteczności komercyjnej, rekreacyjnej czy konserwatorskiej skutkująca dużymi konsekwencjami finansowymi uczestników łańcucha dostaw.

2.3. Współdziałanie systemów logistycznych w czasie działań kryzysowych

O współdziałaniu możemy mówić, jeśli mamy działania przynajmniej dwupodmiotowe i są one czymś wspólnie zajęte (rys. 2.3)⁸⁸. Zakłada się trzy możliwe wzajemne relacje: współpracę, obojętność, przeciwdziałanie.



Rys. 2.3. Formy relacji we współdziałaniu

Źródło: zob. A. Szymonik, *Logistyka i zarządzanie łańcuchem dostaw*, część 2, Difin, Warszawa 2010, s. 57.

⁸⁸ Por. J. Wolejszo, *Teoretyczne aspekty współdziałania*, [w:] *Współdziałanie systemów dowodzenia wojsk operacyjnych i wsparcia krajowego*, AON, Warszawa 2005, s. 14.

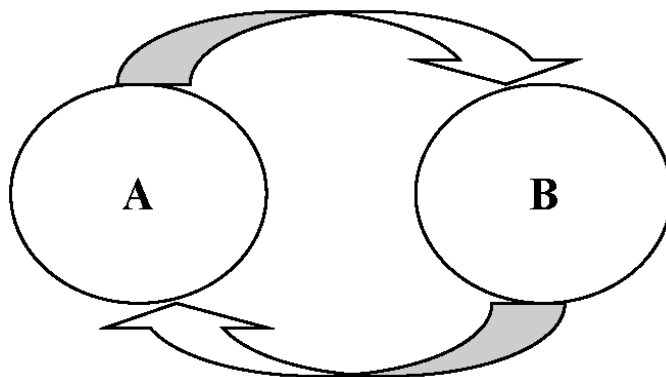
Przyjąć więc można, że podmiot **A** kooperuje – jest partnerem (rys. 2.4) z podmiotem **B** wtedy i tylko wtedy, gdy zachowanie sprawcze **A** wpływa na wyniki zachowania sprawczego **B** lub gdy działanie **B** w podobny sposób wpływa na rezultat działania **A**⁸⁹. Tak rozumiana kooperacja, współdziałanie obejmuje zarówno jej pozytywną, jak i negatywną stronę.

Z uwagi na cel działania współdziałanie, relacje mogą przyjąć formę⁹⁰: zgodności, sprzeczności, niezgodności.

Współdziałanie niejednokrotnie jest rozumiane jako⁹¹: współpraca, kordynacja, synchronizacja, synergia, współgranie.

Często z pojęciem współdziałania jest utożsamiana koordynacja działań, która *polega na włączaniu do działania elementów niezbędnych do osiągnięcia zamierzonego wyniku, w odpowiedniej jakości, ilości i we właściwym czasie. Dotyczy ona zarówno tworzenia, jak i funkcjonowania i rozwoju systemu oraz stanowi zasadniczą składową funkcję organizowania, będąc zarazem czynnikiem łączącym wszystkie funkcje zarządzania w jeden złożony proces*⁹².

Prakseologia współdziałania (racjonalnego)



Rys. 2.4. Zależności pomiędzy podmiotami

Źródło: opracowanie własne.

⁸⁸ Por. S.J. Sokołowski, *Szkice prakseologiczne*, Warszawa 1988, s. 88.

⁹⁰ N. Klatka, *Konflikt i gra*, Warszawa 1972, s. 86.

⁹¹ Por. *Internetowy słownik synonimów języka polskiego online*, <http://www.synonimy.pl/>, 25.09.2014.

⁹² Por. *Organizacja i zarządzanie. Zarys problematyki*, red. nauk. A Stabryła, J. Trzeciecki, Akademia Ekonomiczna w Krakowie, Kraków 1986, s. 293.

Koordinacja może wystąpić w zakresie np. zaopatrzenia, zbytu produktów, usług, a istota działań polega na tym, że:

- każdy z uczestników otrzymuje zadanie zgodnie ze swą specjalnością i możliwościami,
- organizujący dąży do maksymalnego wykorzystania możliwości poszczególnych elementów,
- wszystkie działania poszczególnych elementów zbliżają całość organizacyjną do osiągnięcia założonego celu działania.

Koordinacja jest postrzegana również jako jedna z funkcji zarządzania, obok planowania, organizowania, czyli pozyskiwania i alokacji zasobów, motywowania, kontrolowania oraz decydowania. Postrzegana jest jako działania zapewniające współdziałanie wzajemne wymienionych funkcji⁹³.

Współdziałanie jest również utożsamiane z synchronizacją działań. Pojęcie to jest definiowane, między innymi, jako: doprowadzenie zmian kilku wielkości fizycznych do synchronizmu, jednoczesności, zgodności w czasie⁹⁴; koordynacja w czasie co najmniej dwóch zjawisk (procesów), tzn. dążenie do równoległego, niezależnego ich przebiegu skoordynowanego w czasie lub do jednoczesnego ich zakończenia⁹⁵; doprowadzenie dwóch lub więcej zjawisk, procesów, czynności itp. do zgodności ich przebiegu w czasie⁹⁶.

Synchronizacja działań to koordynacja w czasie i od niej różni się tym, że: jest organizowana między np. ogniwami łańcucha dostaw celowo połączonymi do wykonania konkretnego zadania, natomiast uczestnicy są częściami (ogniwami) z tej samej całości (łańcucha dostaw), lecz z uwagi na specjalizację wykonują zadania cząstkowe.

Analiza powyższych definicji sugeruje, że zawsze kiedy mówimy o współdziałaniu, mamy na myśli tylko takie działania wielopodmiotowe, gdzie uczestnicy świadomie i dobrowolnie przyczyniają się do osiągnięcia celu wspólnego bądź celu jednego z uczestników działania.

Wobec tego celem współdziałania jest zapewnienie sprawności osiągnięcia efektu końcowego (celu) wspólnych działań.

Natomiast istota współdziałania będzie się sprowadzać do działania wspólnego przy zachowaniu autonomii sprawców tego działania.

Można przyjąć, że tylko takie działania wielopodmiotowe są określane mianem współdziałania, w których zachodzą następujące warunki⁹⁷: występują przynajmniej dwa podmioty, jest określony zgodny lub wspólny cel działania,

⁹³ Por. *Wstęp do informatyki gospodarczej*, pod red. A. Rokickiej-Broniatowskiej, SGH, Warszawa 2006, s. 129.

⁹⁴ W. Kopaliński, *Słownik wyrazów obcych*, <http://www.sloownik-online.pl/> 23.10.2014.

⁹⁵ Por. *Organizacja i zarządzanie ...*, op. cit. s. 293.

⁹⁶ W. Kopaliński, *Słownik wyrazów obcych*, <http://sjp.pwn.pl/> 23.10.2014.

⁹⁷ Por. J. Wołęjszo, *Teoretyczne aspekty...*, op. cit., ss. 15-16.

podmioty świadomie i dobrowolnie zgadzają się na udział w osiągnięciu celu wspólnego lub celu jednego z nich, przynajmniej jedna ze stron musi podejmować działania wspomagające działanie drugiej.

Współdziałanie może dotyczyć podmiotów, które: pozostają ze sobą w stosunku służbowej zależności (np. logistyka jednostki wojskowej, w skład której wchodzi siły i środki rozmieszczone w strukturze pułku czy brygady); są elementami tej samej struktury systemu (np. Komendy Powiatowej Policji, podporządkowane właściwej Komendzie Wojewódzkiej Policji); są elementami różnych struktur (np. jednostki wojskowej, Komendy Powiatowej Policji, Powiatowej Straży Pożarnej, Wodnego Ochotniczego Pogotowia Ratunkowego, Państwowej Inspekcji Sanitarnej).

Dla naszych potrzeb uważam, że można współdziałanie systemów logistycznych w logistyce bezpieczeństwa zdefiniować jako: *współpracę sił i środków logistycznych zaangażowanych podmiotów w celu zachowania ciągłości i skuteczności akcji ratowniczych od momentu otrzymania sygnału o zdarzeniu lub zagrożeniu poprzez dysponowanie zasobów ratowniczych i informowania, jak również w procesie realizacji zadań na miejscu zdarzenia do czasu jego zakończenia.*

Współczesne współdziałanie systemów logistycznych w praktyce, w czasie działań kryzysowych, zostało wykształtowane i uwarunkowane w wyniku pojawiających się nowych zagrożeń. Tylko skoordynowane wewnętrznie procesy logistyczne w sposób efektywny mogą się przyczynić do przeciwdziałania wszelkim zagrożeniom państwa, w szczególności politycznym, gospodarczym, psychospołecznym, ekologicznym i militarnym.

Współdziałanie procesów logistycznych jest realizowane w dwóch podsystemach, tj. kierowania i wykonawczego.

W skład systemu kierowania, w zależności od rodzaju i stopnia zagrożenia, mogą wchodzić komórki logistyczne, które są nieodłącznymi elementami takich instytucji, jak np.: Wojewódzki Zespół Zarządzania Kryzysowego (WZZK), Powiatowy Zespół Zarządzania Kryzysowego (PZZK) czy Gminny Zespół Zarządzania Kryzysowego (GZZK).

Podsystem kierowania procesami logistycznymi realizuje przedsięwzięcia związane z: planowaniem, przygotowaniem zasobów logistycznych, motywowaniem, kontrolowaniem, koordynacją i podejmowaniem decyzji stosownie do skali zagrożeń.

Logistyczne podsystemy wykonawcze tworzą siły i środki pozostające we właściwościach ministrów kierujących działami administracji rządowej, centralnych organów administracji rządowej, wojewodów, organów samorządu terytorialnego oraz innych podmiotów odpowiedzialnych za realizację ustawowo określonych zadań w zakresie bezpieczeństwa narodowego.

Skład sił i środków zapewniających sprawne i skuteczne realizowanie zadań związanych z logistyką jest zróżnicowany, bowiem obejmuje on najwyższe

instytucje rządowe, ale i także pojedyncze (w tym ochotnicze) podmioty w terenie.

Podsystem wykonawczy to między innymi: obrona narodowa wraz Siłami Zbrojnymi RP, Policja, Straż Graniczna, Biuro Ochrony Rządu, Państwowa Straż Pożarna, Ochotnicza Straż Pożarna, Wodne Ochotnicze Pogotowie Ratunkowe, Górskie Ochotnicze Pogotowie Ratunkowe, Tatrzańskie Ochotnicze Pogotowie Ratunkowe, Obrona Cywilna, Państwowa Inspekcja Sanitarna, pogotowie gazowe, pogotowie energetyczne, Straż Miejska, Państwowe Ratownictwo Medyczne, saperzy, Wydziały Zarządzania Kryzysowego Obrony Ludności i Obrony Cywilnej, Społeczna Krajowa Sieć Ratunkowa, inne.

Podstawowym zadaniem logistyki podsystemów wykonawczych jest:

- ewakuacja ludności – jeden ze środków zbiorowej ochrony ludności i ma na celu ochronę życia i zdrowia ludzi, zwierząt, ratowanie mienia, w tym zabytków ruchomych oraz ważnej dokumentacji, w przypadku wystąpienia wszelkiego rodzaju zagrożeń;
- realizacja akcji ratunkowych, które organizuje się i prowadzi w celu ratowania i udzielania pomocy ludności poszkodowanej w wyniku działań zbrojnych, klęsk żywiołowych i innych podobnych zdarzeń, w tym zagrożeń środowiska;
- walka z pożarami, która polega na zapobieganiu możliwości ich powstania, przeciwdziałaniu rozprzestrzenianiu się ognia, gaszeniu pożarów oraz wykonywaniu pomocniczych działań ratowniczych;
- odkażanie i inne działania ochronne, które obejmuje prowadzenie wśród ludności zabiegów sanitarnych, odkażania i dezaktywacji obiektów, odzieży, środków transportu, urządzeń i materiałów oraz odkażanie zwierząt gospodarskich, a także usuwanie i unieszkodliwianie pozostałości po przeprowadzonych zabiegach;
- doraźne przywrócenie działania niezbędnych służb użyteczności publicznej, które realizuje się w razie:
 - ✓ zniszczenia lub uszkodzenia instalacji i urządzeń zapewniających ludności dostawę wody pitnej, ciepła, światła i gazu,
 - ✓ uruchomienia transportu publicznego zapewniającego przewóz osób i podstawowego zaopatrzenia,
 - ✓ uszkodzenia zakładów pracy wytwarzających artykuły pierwszej potrzeby;
- doraźne grzebanie zmarłych, które organizuje się w przypadku masowych zgonów lub dużej liczby zabitych, w celu zapobieżenia epidemii bądź ograniczenia jej rozprzestrzeniania (czynności związane z grzebaniem zmarłych wykonują odpowiednie służby komunalne i sanitarne);
- pomoc w ratowaniu dóbr niezbędnych do przetrwania – polega ona na określeniu minimalnego zapasu żywności i dóbr, gwarantującego przeżycie ludności oraz funkcjonowanie zakładu pracy, gminy, powiatu, województwa i państwa, a także na planowanym gromadzeniu i rozśrodkowaniu ich

- zasobów utrzymywanych w gospodarstwach domowych oraz ratowaniu ich przed zniszczeniem lub skażeniem w przypadku wystąpienia zagrożeń;
- zaopatrzenie ludności w artykuły konsumpcyjne, które obejmuje:
 - ✓ zaopatrzenie w artykuły żywnościowe z uwzględnieniem ich reglamentacji oraz dystrybucji (sprzedaż),
 - ✓ zaopatrzenie w wodę pitną z uwzględnieniem jej dystrybucji w przypadku awarii sieci wodociągowej,
 - ✓ zaopatrzenie w artykuły przemysłowe powszechnego użytku z uwzględnieniem reglamentacji wybranego asortymentu,
 - ✓ zaopatrzenie w produkty naftowe z uwzględnieniem reglamentacji paliw samochodowych,
 - ✓ dostawy energii elektrycznej i surowców energetycznych (węgla, gazu) dla celów komunalnych.

3. BEZPIECZEŃSTWO TRANSPORTU, GOSPODARKI MAGAZYNOWEJ, ŻYWNOŚCIOWE

Zgodzić się należy, że nowoczesne, nowatorskie spojrzenie na zarządzanie bezpieczeństwem gospodarczym w kontekście relacji i zależności wynikających z bezpieczeństwa wybranych systemów logistycznych pozwala osiągnąć efekt synergii. Pomocnym w tym są analizy i rozważania oparte o przepisy prawne, organizacyjne, techniczne oraz o merytoryczne zestawienia, wykresy, tabele, o nowe i przyszłe uwarunkowania mające wpływ na funkcjonowanie wybranych, ważnych sektorów bezpieczeństwa gospodarczego, takich jak: transport (ze szczególnym uwzględnieniem transportu samochodowego i kolejowego), infrastruktura magazynowa, żywność.

3.1. Nowe i przyszłe uwarunkowania wpływające na bezpieczeństwo transportu

Nowoczesna gospodarka nie może funkcjonować bez bezpiecznego, zrównoważonego, ekologicznego i konkurencyjnego transportu lądowego, lotniczego i morskiego. Unia Europejska dokłada wielu starań, poprzez opracowywanie strategii w „Białej Księdze transportu” i przyznawaniu środków finansowych, by sprzyjał on ekonomicznemu rozwojowi i jednocześnie nie szkodził środowisku⁹⁸.

W okresie wzmożonej mobilności społeczeństwa polityka transportowa uwzględnia nowe wyzwania i rozwiązania szeregu problemów w wymiarze europejskim oraz globalnym, które mają wpływ na bezpieczeństwo transportu. Do nich możemy zaliczyć:

Po pierwsze. Opublikowany w Białej Księdze transportu *Plan utworzenia jednolitego europejskiego obszaru transportu – dążenie do osiągnięcia konkurencyjnego i oszczędnego zasobowo systemu transportu* jest daleko siężnym dokumentem o bardzo ambitnie wytyczonych celach. Nadrzędnym celem podjęcia przyszłych działań ma być ostateczne stworzenie jednolitego europejskiego obszaru transportu. Ma to być obszar, w którym sektor transportu będzie charakteryzował się wysokim poziomem konkurencyjności i dodatkowo będzie bardzo oszczędnie wykorzystywał nieodnawialne surowce naturalne.

⁹⁸ Zob. Biała Księga, *Plan utworzenia jednolitego europejskiego obszaru transportu – dążenie do osiągnięcia konkurencyjnego i zasobooszczędnego systemu transportu*, KOM(2011) 144 wersja ostateczna, Bruksela, dnia 28.3.2011.

Te oczekiwania mają być w sytuacji, gdy⁹⁹:

- nastąpi zmniejszenie o połowę liczby samochodów o napędzie konwencjonalnym w transporcie miejskim do 2030 r., a ich całkowita eliminacja z miast nastąpi do 2050 r.; osiągnięcie zasadniczo wolnej od emisji CO₂ logistyki w dużych ośrodkach miejskich do 2030 r.;
- do 2030 r. 30% drogowego transportu towarów na odległościach większych niż 300 km będzie przeniesione na inne środki transportu, np. kolej lub transport wodny, zaś do 2050 r. powinno to być ponad 50% tego typu transportu;
- nastąpi ukończenie szybkiej europejskiej sieci kolejowej do 2050 r.;
- do 2050 r. większa część ruchu pasażerskiego na średnie odległości będzie odbywać się koleją;
- nastąpi utworzenie do 2030 r. w pełni funkcjonalnej ogólnounijnej multimodalnej sieci bazowej TEN-T¹⁰⁰, zaś do 2050 r. będzie to wysokiej jakości i przepustowości sieć;
- do 2050 r. nastąpi połączenie wszystkich lotnisk należących do sieci bazowej z siecią kolejową, najlepiej z szybkimi kolejami oraz wszystkie najważniejsze porty morskie będą miały dobre połączenie z kolejowym transportem towarów oraz, w miarę możliwości, systemem wodnego transportu śródlądowego;
- do 2020 r. zostanie zmodernizowana infrastruktura zarządzania ruchem lotniczym (SESAR¹⁰¹) oraz będą zakończone prace nad Wspólnym Europejskim Obszarem Lotniczym;
- do 2020 r. zostanie wprowadzony równoważny system zarządzania transportem lądowym i wodnym (ERTMS¹⁰², ITS¹⁰³, SSN i LRIT¹⁰⁴, RIS¹⁰⁵)

⁹⁹ Tamże.

¹⁰⁰ TNT-T (*Trans-European Transport Networks*, TEN-T) – program UE dotyczący sieci drogowych, kolejowych, wodnych i powietrznych.

¹⁰¹ SESAR – *Single European Sky ATM Research* – Jednolita Europejska Przestrzeń Powietrzna ma przyczynić się m.in. do zwiększenia poziomu bezpieczeństwa w lotnictwie cywilnym, poprawy efektywności operacyjnej (zwiększenie przepustowości przestrzeni powietrznej) i kosztowej (zmniejszenia kosztów jednostkowych), a także ograniczenia negatywnego oddziaływania lotnictwa na środowisko, [w:] *Transport lotniczy: Jednolita Europejska Przestrzeń Powietrzna*, <http://www.europarl.europa.eu/>, 11.05.2015.

¹⁰² ERTMS – Europejski System Zarządzania Ruchem Kolejowym (European Railway Traffic Management System) – stanowi jedno z kluczowych przedsięwzięć, których celem jest zapewnienie jak największej interoperacyjności transportu, szczególnie kolei w Europie. Europejski System Zarządzania Ruchem Kolejowym (ERTMS) obejmuje zunifikowaną europejską radiołączność pociągową GSM-R (Global System for Mobile Communications – Railway) i zunifikowany europejski system bezpiecznej kontroli jazdy pociągu ETCS (European Train Control System). Obydwa systemy są istotnymi

oraz będzie oddany do użytku europejski system nawigacji satelitarnej (Galileo);

- nastąpi przejście na pełne zastosowanie zasad „użytkownik płaci” i „zanieczyszczający płaci”.

Po drugie. Transport i jego wpływ na gospodarkę oraz życie człowieka spowodował, że stał się on przedmiotem zainteresowania ważnych instytucji i organów UE, do których zaliczamy w: Komisji Europejskiej (organ wykonawczy) – Wydziały Mobilność i Transport oraz Gospodarka Morska i Rybołówstwo; Parlamencie Europejskim – Komisja Transportu i Turystyki; Radzie Unii Europejskiej – Transport, Telekomunikacja i Energia; Europejskim Komitecie Ekonomiczno-Społecznym – Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego; Komitecie Regionów – Komisja Polityki Spójności Regionalnej; Europejskim Banku Inwestycyjnym – Sieci Transeuropejskie; Agencjach UE: Europejska Agencja Bezpieczeństwa Morskiego, Europejska Agencja Bezpieczeństwa Lotniczego, Europejska Agencja Kolejowa, Agencja Wykonawcza ds. Konkurencyjności i Innowacyjności (EACI), Europejski Organ Nadzoru Globalnego Systemu Nawigacji Satelitarnej GNSS.

składnikami europejskiej polityki likwidacji barier w transporcie, zarówno w wymiarze barier technicznych na sieciach kolejowych wewnątrz granic UE, jak i w zakresie budowania wspólnego rynku w zakresie produktów i usług na rzecz kolei, [w:] *Europejski System Zarządzania Ruchem Kolejowym*, <http://www.dobralogistyka.pl/>, 11.05.2014.

¹⁰³ ITS – (*Intelligent Transportation Systems*) to systemy, które stanowią szeroki zbiór różnorodnych technologii (telekomunikacyjnych, informatycznych, automatycznych i pomiarowych) oraz technik zarządzania stosowanych w transporcie w celu ochrony życia uczestników ruchu, zwiększenia efektywności systemu transportowego oraz *ochrony zasobów środowiska naturalnego*, [w:] A. Koźlak, *Inteligentne systemy transportowe jako instrument poprawy efektywności transportu*, <http://www.cati.org.pl/>, 11.05.2014.

¹⁰⁴ SSN – *SafeSeaNet* służący do monitorowania ruchu morskiego na europejskich wodach, LRIT (*Long-range Identification and Tracking*) – służący do śledzenia oraz identyfikacji wszystkich statków na świecie pływających pod banderą UE, [w:] *SSN LRIT imdate training*, <http://www.emsa.europa.eu>, 11.05.2014.

¹⁰⁵ RIS – *River Information Service* usługa informacji rzecznej – usługę tę wprowadzono celem podwyższenia poziomu bezpieczeństwa i efektywności żeglugi śródlądowej i obniżenia jej szkodliwego wpływu na środowisko naturalne poprzez świadczenie serwisu informacyjnego dla jednostek pływających i wprowadzenie systemów kontroli i zarządzania ruchem na śródlądowych drogach wodnych, [w:] *Usług informacji rzecznej (RIS)*, <http://www.google.pl/#hl=pl>, 1205.2014.

Wszystkie państwa członkowskie są zobowiązane czynnie brać udział w pracach tych instytucji oraz wypełniać zobowiązania wynikające z pracy tych organów.

Po trzecie. Celem stworzenia bezpiecznego transportu w UE zaplanowano szereg przedsięwzięć dla transportu lądowego, morskiego i lotniczego.

Po czwarte. Rosnące ceny benzyny i oleju napędowego są utrapieniem transportowców i konsumentów. Analiza wskaźników cen towarów i usług konsumpcyjnych podawanych przez GUS pokazuje, że np. na przestrzeni lat 2010-2015 ceny materiałów pędnych i smarów rosły najczęściej, nawet o kilkanaście procent w stosunku do roku poprzedniego.

Jak wynika z badań, najpoważniejszym składnikiem kosztów funkcjonowania przedsiębiorstwa transportowego jest koszt zakupu materiałów pędnych, na które, w przypadku firmy pojazdów klasy EURO5 i naczep chłodniczych, składa się przede wszystkim olej napędowy, a także dodatek do paliwa AdBlue oraz różnego rodzaju uszlachetniacze, stosowane przede wszystkim w sezonie zimowym. Jeśli doliczymy jeszcze do tego koszty osobowe, to okazuje się, że jest to prawie 60% kosztów uzyskania przychodów firmy (tabela 3.1).

Tabela 3.1

Zestawienie kosztów funkcjonowania przedsiębiorstwa międzynarodowego transportu samochodowego

| Rodzaj kosztów | % kosztów całkowitych |
|---|-----------------------|
| Paliwo i inne materiały pędne | 38,01 |
| Wynagrodzenie i delegacje pracowników | 17,46 |
| Oplaty leasingowe i amortyzacja sprzętu | 10,90 |
| Oplaty drogowe | 9,25 |
| Naprawa i serwisowanie sprzętu | 8,26 |
| Ubezpieczenia (bez pracowniczych) | 5,24 |
| Dokumenty celne i przewozowe | 3,06 |
| Ogumienie pojazdów | 1,83 |
| Komunikacja | 1,75 |
| Nieautoryzowane wydatki na Wschodzie | 1,32 |
| Podatki (bez pracowniczych) | 1,05 |
| Wydatki biurowe | 0,92 |
| Inne | 0,95 |

Źródło: J. Łacny, *Benchmarking kosztów w polskich przedsiębiorstwach międzynarodowego transportu drogowego ładunków w 2012*, [w:] *Logistyka 2/2013*, s. 12.

Należy zaznaczyć, że koszty paliwa w przeliczeniu na 1 km kształtują się różnie w zależności od relacji transportowych, i tak w przypadku rynku¹⁰⁶: UE – 1,23 zł/km (40,6%); krajów wschodnich – 1,01 zł/km (37,6%), krajowego – 1,18 zł/km (45,1%).

Każda podwyżka cen paliw powoduje wzrost kosztów przewozu. Firmy transportowe, aby nie działać poniżej progu rentowności podnoszą ceny za swoje usługi, za które w końcowym efekcie płacą przedsiębiorstwa zlecające przewozy (np. producenci lub dystrybutorzy) czy konsumenci finalni.

Po piąte. Zatory komunikacyjne paraliżują zarówno ruch drogowy, jak i lotniczy. Kosztują Europę około 1 proc. rocznego PKB, co więcej, zarówno wielkość transportu towarowego, jak i pasażerskiego w przyszłości wzrośnie¹⁰⁷. I tak np. w Londynie, Kolonii, Amsterdamie i Brukseli kierowcy spędzają w korkach ponad 50 godzin rocznie, a w Utrechcie, Manchesterze i Paryżu – ponad 70 godzin¹⁰⁸. Wiele do zrobienia jest również w obszarze komunikacji samochodami osobowymi. Fakt zapełnienia samochodu – 1,5 osoby – i dobowy czas wykorzystania – 1 godzina – podpowiada, że należy uruchomić programy, które powinny te tendencje zmienić¹⁰⁹. Nadchodzi czas rezygnacji z indywidualnego podejścia (posiadania własnego auta) na korzyść zbiorowego (alternatywne środki transportu), co znaczenie wpłynie na rozładowanie zatłoczonych tras przejazdowych. Obecnie oprócz profesjonalnych oferentów flot samochodowych pojawiają się platformy wspierane aplikacjami internetowymi lub dla smartfonów, wykorzystując koncepcję *peer – to – peer*, tj. każdy z każdym, umożliwiające prywatnym użytkownikom włączenie się w rynek i organizowanie wymiany usług bez wnoszenia własnej floty pojazdów. Profesjonalnie zarządzane floty samochodów osobowych i rowerów są znaczącą siłą napędową mobilności w obszarach miejskich. Carsharing¹¹⁰ od dawna stanowi segment transportu miejskiego, ale jest wciąż ofertą niszową.

¹⁰⁶ Por. M. Osińska, W. Zalewski, *Ekonometryczna analiza przychodów i kosztów w przedsiębiorstwie transportowym na tle koniunktury w branży*, [w:] *Logistyka* 6/2012, s. 903.

¹⁰⁷ Zob. *Polityka transportowa UE*, <http://europa.eu/>, 10.03.2014.

¹⁰⁸ Por. *INRIX European National Traffic Scorecard 2010*, <http://ec.europa.eu/>, 10.03.2014.

¹⁰⁹ Por. M. Ucieszyński, *Infrastruktura transportowa a efektywność procesów logistycznych*, [w:] *Logistyka* 2/2012, s. 31.

¹¹⁰ Carsharing (współwłasność) – to system, który na razie sprawdza się głównie w Niemczech, a eksperymentalnie wprowadzany jest w innych krajach, m.in. w Czechach. Polega na tym, że kilku użytkowników posiada jeden samochód – wspólnie dzielą się oni kosztami utrzymania, paliwa i napraw. Opłata miesięczna zależy także od czasu korzystania z samochodu i liczby przejechanych kilometrów. Kluczyki oddaje się do specjalnych sejfów na stacjach carsharingu, [w:] *Ekojazda w trzech odstonach*, <http://ulicaekologiczna.pl>, 14.07.2014.

Po szóste. Infrastruktura – nie jest jednakowo rozwinięta we wszystkich krajach UE. Na przykład w większości krajów położonych we wschodniej części UE brakuje linii szybkich kolei, a tradycyjne linie kolejowe są często w złym stanie. Nawet w krajach UE, charakteryzujących się relatywnie dobrym poziomem rozwoju infrastruktury transportowej, stały wzrost zapotrzebowania na profesjonalną obsługę transportową i logistyczną podmiotów gospodarczych sprawia, że infrastruktura nie zawsze odpowiada oczekiwaniom przedsiębiorców i potrzebom współczesnego rozwoju ekonomicznego. Tak więc, podobnie jak w Polsce, we wszystkich krajach UE poziom rozwoju infrastruktury jest postrzegany jako jedna z 15 podstawowych barier rozwoju przedsiębiorstw¹¹¹.

Sieć transportowa w Polsce, mimo realizowanych inwestycji infrastrukturalnych, wciąż charakteryzuje się niską jakością i stanowi poważne zagrożenie dla efektywnego funkcjonowania łańcuchów dostaw. Na poważne ograniczenia infrastrukturalne w Polsce wskazują także badania Światowego Forum Gospodarczego w odniesieniu do globalnej konkurencyjności gospodarki (tabela 3.2). Pod względem dostępności i przepustowości naszych portów lotniczych jesteśmy na 101. miejscu na świecie, infrastruktury portów – na 99., a infrastruktury kolejowej – na 75. miejscu. Ogółem pod względem dostępności i jakości polskiej infrastruktury transportowej raport klasyfikuje nasz kraj na 58. miejscu w 2015 roku na 140 państw.

Tabela 3.2

Poziom rozwoju infrastruktury w Polsce z perspektywy badań Światowego Forum Gospodarczego

| Wyszczególnienie | 2005 | 2014 | 2015 |
|--|------|------|------|
| Miejsce w rankingu światowym (na 140 państw) | 70 | 69 | 58 |

Źródło: P. Boguszewski, *Globalny raport konkurencyjności 2015-16*, Światowego Forum Gospodarczego, Warszawa, 30 września 2015 r., Departament Stabilności Finansowej, s. 22.

Po siódme. Polityka Unii Europejskiej jest skierowana między innymi na rozwój transportu, który tworzy miejsca pracy, wpływa na rozwój gospodarczy i nie szkodzi środowisku naturalnemu. Do tej gałęzi zaliczamy między innymi transport kolejowy, pod warunkiem, że przewyżczy takie przeszkody, jak¹¹²: zrównanie pod względem prawa przewoźników krajowych i zagranicznych

¹¹¹ R. Rolbicki, *Infrastruktura transportowa a efektywność procesów logistycznych*, [w:] *Logistyka*, 2/2012, s. 36.

¹¹² M. Rabsztyń, [w:] *Biuletyn informacyjny infrastruktury nr 6/2013*, Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, Warszawa 2013, ss. 10-11.

(krajowe przewozy pasażerskie są w większości zamknięte dla konkurencji, zarówno wewnętrznej, jak i zagranicznej, większość krajowych pociągów pasażerskich kursuje na podstawie umów z państwowymi przewoźnikami, które są zawierane z nimi bezpośrednio, bez przetargów); uproszczenie procedur wejścia nowych przewoźników na rynek poprzez zmniejszenie kosztów administracyjnych i konieczności spełnienia 11 tys. przepisów technicznych (procedura dopuszczenia do eksploatacji nowego pojazdu szynowego może trwać do dwóch lat i kosztować 6 mln €, uzyskanie świadectwa bezpieczeństwa ruchu może kosztować do 70 tys. €); uwolnienie potencjału kolei, poprzez zastąpienie narodowej polityki poszczególnych państw działaniami międzynarodowymi (należy stworzyć sieć zarządców infrastruktury, którzy będą rozwijać TEN-T *Trans-European Transport Network* – sieć korytarzy towarowych oraz ERMTS *European Rail Traffic Network* – europejski system sterowania pociągami); ujednoczenie norm i przepisów w krajach UE poprzez przekazanie uprawnień krajowych do Europejskiej Agencji Kolejowej (ERA – *European Railway Agency*), która będzie dopuszczała pojazdy kołowe do ruchu i wydawała świadectwa bezpieczeństwa dla wszystkich kolei w UE.

Po ósme. Konkurencja – europejski sektor transportowy musi stawić czoła narastającej presji konkurencji na szybko rozwijających się światowych rynkach transportu.

Po dziewiąte. Firmy transportowe, realizując procesy usługowe w wymiarze krajowym i europejskim, szczególną uwagę muszą zwracać na bezpieczeństwo: *ludzi, ładunków i procesów realizowanych w łańcuchu dostaw, ekologiczne i socjalne.*

Bezpieczeństwo ludzi w rzeczywistości dotyczy wszystkich gałęzi transportu, to jednak ze wszystkich rodzajów transportu najbardziej niebezpiecznym i kosztownym społecznie, a jednocześnie najszerzej używanym w przewozach pasażerskich jest transport drogowy (wypadki drogowe stanowią około 95% wszystkich wypadków w transporcie)¹¹³. Dlatego też bezpieczeństwo na drogach jest priorytetem w tym zakresie. Jego poprawa wymaga podjęcia działań, które przyczynią się do istotnego zmniejszenia liczby zabitych – zgodnie z wytycznymi IV Europejskiego Programu Działań na rzecz Bezpieczeństwa Ruchu Drogowego 2011-2020, ogłoszonego przez Komisję Europejską oraz Planem Globalnym dla Dekady Działań na rzecz Bezpieczeństwa Ruchu Drogowego 2011-2020 ogłoszonym przez Zgromadzenie Ogólne ONZ.

Problemy, w znacznej mierze, rozwiązują inteligentne systemy transportowe (ITS). Jak wynika z prowadzonych badań wpływają one na poprawę

¹¹³ *Strategia rozwoju transportu do 2020 roku (z perspektywą do 2030 roku)*, Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, Warszawa, dnia 22 stycznia 2013 r.

realizowanych procesów transportowych. Systemy autonomiczne ITS, wdrożone w państwach członkowskich UE, nie są interoperacyjne z różnych powodów, m.in. ze względu na brak możliwości wymiany danych i dlatego Komisja Europejska podjęła działania zmierzające do poprawy tego stanu rzeczy, o czym świadczą dokumenty: dyrektywa 2010/40/UE, mandat M/453, decyzja 2011/453/UE.

W transporcie kolejowym podstawowymi czynnikami wpływającymi na stan bezpieczeństwa są: stan techniczny infrastruktury kolejowej, stan techniczny taboru kolejowego, funkcjonowanie przejazdów kolejowych.

Poprawa bezpieczeństwa ruchu na przejazdach kolejowych wymaga realizacji następujących kierunków interwencji: obserwacja (w tym filmowanie) przejazdów, na których nagminnie dochodzi do naruszania przepisów; oznaczanie szczególnie niebezpiecznych przejazdów kolejowych tablicami informacyjnymi; intensywniejsza modernizacja tych przejazdów; likwidacja (w miarę możliwości) skrzyżowań jednopoziomowych na rzecz skrzyżowań dwupoziomowych (wiaduktów i tuneli).

Bezpieczeństwo lotnictwa cywilnego jest obecnie postrzegane jako proces monitorowania i utrzymywania określonego poziomu bezpieczeństwa poprzez kontrolę organizacyjną. Organizacja Międzynarodowego Lotnictwa Cywilnego (ICAO) w swoich normach i zalecanych praktykach nakazuje konieczność zapewnienia systemowego podejścia, czyli wprowadzania systemu zarządzania bezpieczeństwem opartego na zarządzaniu ryzykiem. W Polsce bezpieczeństwo w transporcie lotniczym będzie ściśle związane i dostosowane do europejskich i światowych standardów. Wyeliminowany zostanie obecnie bierny system bezpieczeństwa na rzecz systemu opartego na zarządzaniu ryzykiem. Polska, jako członek Unii Europejskiej, będzie zatem w najbliższych latach podejmować aktywne działania w zakresie przewidywania potencjalnych zagrożeń dla bezpieczeństwa lotnictwa cywilnego i wdrażania takich rozwiązań, które będą służyć całemu systemowi, a nie wyłącznie wybranym jego elementom. Na potrzeby wdrażania SRT (Strategii Rozwoju Transportu) zostanie opracowany *Krajowy Program Bezpieczeństwa w Lotnictwie Cywilnym (KPBLC)*, który szczegółowo określi kryteria bezpieczeństwa lotniczego. Jednocześnie *Programowi* będzie towarzyszyć kilka rozporządzeń uszczegóławiających zasady funkcjonowania poszczególnych jego elementów.

Wysiłki na rzecz efektywnego systemu bezpieczeństwa żeglugi morskiej będą oparte na realizacji następujących kierunków: doskonalenie standardów bezpiecznego uprawiania żeglugi przez statki morskie; ochrona żeglugi i portów przed zagrożeniami terrorystycznymi i kryminalnymi; rozwój Morskiej Służby Poszukiwania i Ratownictwa (SAR) oraz poprawa współpracy wszystkich służb uczestniczących w akcjach ratowniczych na morzu; zintegrowanie systemów

usług informacyjnych VTS/VTMS i RIS¹¹⁴; budowa i doskonalenie Krajowego Systemu Bezpieczeństwa Morskiego (w skład systemu wchodzi: System Nadzoru i Monitorowania Bezpieczeństwa Ruchu Morskiego (SMRM), Krajowa Sieć Stacji Bazowych Systemu Automatycznej Identyfikacji Statków (AIS-PL), System Wczesnego Ostrzegania (EWS).

Bezpieczeństwo ładunków i procesów realizowanych w łańcuchu dostaw, zarówno w górnej, jak i w dolnej części stanowi obszar nie tylko zainteresowania jego uczestników, ale wymaga szczególnej troski pod kątem sprawności i skuteczności zarządzania nim. Bezpieczeństwo dostaw to między innymi ochrona „end-to-end”, która wyraża się między innymi w poprawie poziomu ochrony łańcucha dostaw bez zakłócania swobodnego przepływu towarów, wprowadzeniu certyfikatów ochrony z uwzględnieniem obowiązujących systemów, wspólnej ocenie ochrony obejmującej wszystkie rodzaje transportu, dążeniu do współpracy międzynarodowej w walce z terroryzmem i inną działalnością przestępczą, taką jak piractwo¹¹⁵.

W 2008 roku ukazała się norma ISO 28000: 2007 – *System zarządzania bezpieczeństwem łańcucha dostaw*, przeznaczona dla wszystkich organizacji biorących udział w procesie dostaw produktów, na każdym jego etapie, począwszy od wyboru kontrahentów, poprzez transport, spedycję, odprawy celne, magazynowanie itp.

Nadrzędnym celem systemu zarządzania bezpieczeństwem łańcucha dostaw wg ISO 28000 jest zapewnienie odpowiedniego poziomu bezpieczeństwa, poprzez wdrożenie i utrzymanie zabezpieczeń, przez każdego uczestnika łańcucha, tak aby zapewnić bezpieczeństwo całości. O sile łańcucha świadczy siła jego najsłabszego ogniwa¹¹⁶. Jako najważniejsze korzyści płynące z wdrożenia i funkcjonowania systemu zarządzania bezpieczeństwem łańcucha dostaw wg specyfikacji ISO 28000: 2007 można wskazać na¹¹⁷: uświadomienie ryzyka związanego z poszczególnymi etapami działań realizacji procesów logistycznych poprzez identyfikację zagrożeń oraz oszacowanie prawdopodobieństwa ich zaistnienia oraz skutków ich wystąpienia; zwiększenie pewności ciągłości dostaw poprzez stworzenie prewencyjnych procedur postępowania w obszarze poszczególnych zagrożeń, co wpływa na zwiększenie niezawodności realizowanych dostaw w ramach łańcucha dostaw, a w efekcie i zadowolenie

¹¹⁴ VTS – Służby Kontroli Ruchu Statków, VTMS – Europejski System Monitoringu Ruchu Statków i Informacji – *Vessel Traffic Monitoring and Information System*, RIS – Rzeczny System Informacyjny.

¹¹⁵ Biała Księga, *Plan utworzenia jednolitego europejskiego obszaru transportu – dążenie do osiągnięcia konkurencyjnego i zasobooszczędnego systemu transportu*, KOM(2011) 144 wersja ostateczna, Bruksela, dnia 28.03.2011, s. 41.

¹¹⁶ Por. A. Szymonik, *Eurologistyka Teoria i Praktyka*, Difin, Warszawa 2013, s. 137.

¹¹⁷ Zob. *ISO 28000 Bezpieczeństwo w łańcuchu dostaw*, <http://www.lrqqa.pl/>, 01.11.2015.

klienta; optymalizację procesów w ramach łańcucha dostaw poprzez stworzenie procedur pozwalających realizować zamierzone cele nie tylko w warunkach normalnych, nieodbiegających od codziennych uwarunkowań.

W zakresie bezpieczeństwa ekologicznego i socjalnego transport zaliczany jest do gałęzi gospodarki znacząco przyczyniających się do zanieczyszczenia powietrza (tlenki azotu, tlenek węgla, lotne związki organiczne, pyły i cząstki stałe), czy też do emisji gazów cieplarnianych. System transportu oparty o zasadę zrównoważonego rozwoju powinien utrzymywać harmonię układu komunikacyjnego z jego otoczeniem przyrodniczym, kulturowym oraz społeczno-gospodarczym, polegającą na korzystaniu z istniejących zasobów w sposób umożliwiający ciągłość ich użytkowania i zachowania dla przyszłych pokoleń.

W kontekście ochrony środowiska polski transport musi sprostać rysującym się na horyzoncie wyzwaniom i ograniczeniom zewnętrznym, takim jak: unijna polityka ochrony środowiska, w tym w szczególności klimatu, oraz ograniczeń emisyjnych (w tym emisji gazów cieplarnianych, bowiem transport odpowiada za mniej więcej jedną czwartą emisji gazów cieplarnianych w UE, emisja ta w 2008 roku rozkłada się następująco: 12,8% generuje transport lotniczy, 13,5% transport morski, 0,7% kolej, 1,8% żegluga śródlądowa, a 71,3% transport drogowy)¹¹⁸; nasilająca się walka o dostęp do coraz bardziej ograniczonych zasobów paliw kopalnych (ropa, gaz), co przekłada się na szybki wzrost cen paliw i tym samym pogarszanie efektywności ekonomicznej transportu, a w szerszym wymiarze konkurencyjności całej gospodarki.

Transport przyszłościowy, który w niewielkim stopniu będzie negatywnie wpływał na środowisko, będzie oparty na wspieraniu: różnorodności gałęziowej i komplementarności środków transportu w obrębie systemu połączeń krajowych i międzynarodowych; rozwiązań organizacji transportu najmniej zanieczyszczających środowisko; zarządzania popytem na ruch transportowy; wdrażania nowoczesnych technologii transportowych redukujących negatywne oddziaływanie transportu na środowisko.

Działania praktyczne będą skierowane na promowanie efektywności energetycznej poprzez rozwój transportu intermodalnego w przewozie ładunków, promowanie energooszczędnych technologii, na inwestowanie w gospodarke niskoemisyjną, poprzez m.in. wspieranie projektów z zakresu transportu przyjaznego środowisku (transport kolejowy, transport morski oraz żegluga śródlądowa); na dążenie do stworzenia warunków sprzyjających przenoszeniu przewozów z dróg na kolej, w szczególności na odległości powyżej 300 km;

¹¹⁸ *Biała Księga Plan utworzenia jednolitego europejskiego obszaru transportu – dążenie do osiągnięcia konkurencyjnego i zasobooszczędnego systemu transportu* /* COM/2011/0144 końcowy */, <http://ec.europa.eu/>, 10.03.2014.

na promowanie ekologicznie czystych środków transportu, zasilanych alternatywnymi źródłami energii (np. wykorzystujących ogniwa paliwowe i wodór, napędy elektryczny, gazowy, hybrydowy, sprężonym powietrzem) – wraz ze stworzeniem na terenie całego kraju sieci stacji ładowania lub wymiany baterii elektrycznych oraz sieci tankowania wodoru; na zmniejszanie kongestii transportu, w szczególności w obszarach miejskich między innymi poprzez zwiększanie udziału transportu zbiorowego w przewozie osób, zintegrowanie transportu w miastach (łącznie z dojazdami podmiejskimi), optymalizację i integrację przewozów miejskich oraz regionalnych systemów transportu osób, promocję ruchu pieszego, rowerowego, organizację i rozwój systemów dostaw w miastach oraz eliminację ciężkiego ruchu towarowego oraz przewozów masowych ładunków niebezpiecznych przez tereny intensywnego zainwestowania miejskiego; na upowszechnianie nowych form mobilności społeczeństwa poprzez: dostępność informacji o podróżach, zintegrowane taryfy, wydzielanie obszarów zamieszkania bez dostępu dla samochodów, rozwój systemu telepracy, szersze korzystanie z video-konferencji, rozwiązania wspólnego podróżowania i wspólnego korzystania z pojazdu; na modernizację i rozbudowę infrastruktury transportowej (liniowej i punktowej) odpowiadającej unijnym oraz krajowym standardom i wymogom ekologicznym; na unowocześnianie taboru wszystkich gałęzi transportu (pojazdów oraz innych niezbędnych urządzeń i wyposażenia) w celu doprowadzenia go do stanu odpowiadającego unijnym oraz krajowym standardom i wymogom ochrony środowiska; na wdrażanie innowacyjnych systemów zarządzania ruchem transportowym w poszczególnych gałęziach oraz interoperacyjnych, przyczyniających się do zmniejszenia presji środowiskowych generowanych przez transport (ITS – transport drogowy, ERTMS – transport kolejowy, SESAR – transport lotniczy, VTMS – transport morski, RIS – transport wodny); na wdrożenie technicznych środków ograniczania wibracji i hałasu, wywoływanych w trakcie budowy lub modernizacji połączeń transportowych oraz w czasie eksploatacji infrastruktury przez pojazdy (np. pociągi towarowe w miastach); na ciągły monitoring (wskaźników) wpływu transportu na środowisko¹¹⁹.

3.2. Determinanty bezpieczeństwa w transporcie

Transport samochodowy

W najważniejszych dokumentach dotyczących systemu bezpieczeństwa narodowego, tj. Konstytucji RP, Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2003, 2007, 2014, Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 wiele miejsca poświęca się transportowi, podkreślając jego rolę i znaczenie dla właściwego

¹¹⁹ Por. A. Szymonik, *Eurologistyka Teoria i Praktyka*, Difin, Warszawa 2013, s. 139.

funkcjonowania gospodarki narodowej oraz wszystkich dziedzin i sektorów bezpieczeństwa.

W Białej Księdze Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, w dziedzinie bezpieczeństwa gospodarczego dla podniesienia rangi i ważności wyodrębniono sektor, który został nazwany „transportowy”. W tym samym dokumencie określenie *transport*, w różnym znaczeniu i kontekście jest używane ponad 40 razy.

Na uwagę zasługuje również fakt, że we wszystkich wymienionych dokumentach podkreśla się, iż jednym z ważniejszych zadań państwa w najbliższych latach jest rozbudowa i modernizacja sieci transportowej oraz zapewnienie wysokiego poziomu usług transportowych, które są nie tylko istotnym elementem rozwoju gospodarczego kraju, ale również mają znaczenie dla systemu bezpieczeństwa państwa.

Jest rzeczą oczywistą, że nowoczesna sieć drogowa i kolejowa, rozwinięta sieć śródlądowych dróg wodnych, lotnisk, portów morskich oraz infrastruktura dostępu do tych portów, sprawny system transportu publicznego umożliwiają rozwój polskiej gospodarki, wzmacniają jej powiązanie z gospodarką światową, a także są ważnym składnikiem bezpieczeństwa narodowego oraz terytorialnie zrównoważonego rozwoju kraju¹²⁰.

Jednym z głównych celów polityki transportowej UE, w tym i Polski, jest wzrost udziału w rynku przyjaznych dla środowiska gałęzi transportu, w tym kolei, żeglugi morskiej i żeglugi śródlądowej – zintegrowanych w intermodalnych systemach transportowych – oraz ograniczenie udziału transportu drogowego na europejskich rynkach transportowych.

Tabela 3.3

Przewozy ładunków – stan na 31.12. 2014 r.

| Wyszczególnienie | 2005 | 2010 | 2013 | 2014 |
|----------------------------|--------|--------|--------|--------|
| W milionach ton, w tym: | 1422,6 | 1795,6 | 1848,3 | 1840,0 |
| Transport kolejowy | 269,6 | 234,6 | 232,6 | 227,9 |
| Transport samochodowy | 1079,8 | 1491,3 | 1553,1 | 1547,9 |
| Transport rurociągowy | 54,3 | 56,2 | 50,7 | 49,8 |
| Transport morski | 9,4 | 8,4 | 7,0 | 6,8 |
| Transport śródlądowy wodny | 9,6 | 5,1 | 5,0 | 7,6 |
| Transport lotniczy | 0,03 | 0,04 | 0,04 | 0,04 |

Źródło: na podstawie, *Mały rocznik statystyczny Polski 2015*, Główny Urząd Statystyczny, Warszawa 2015, s. 317.

¹²⁰ Por. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014, pkt. 23.

Tabela 3.4

Przewozy pasażerów – stan na 31.12. 2014 r.

| Wyszczególnienie | 2005 | 2010 | 2013 | 2014 |
|-------------------------------|--------|-------|-------|-------|
| W milionach pasażerów, w tym: | 1046,9 | 838,0 | 739,6 | 709,8 |
| Transport kolejowy | 258,1 | 261,3 | 269,8 | 268,3 |
| Transport samochodowy | 782,0 | 569,7 | 460,0 | 431,5 |
| Transport morski | 0,7 | 0,7 | 0,6 | 0,6 |
| Transport śródlądowy wodny | 1,4 | 1,4 | 1,5 | 1,6 |
| Transport lotniczy | 4,6 | 5,0 | 7,7 | 7,8 |

Źródło: na podstawie, *Mały rocznik statystyczny Polski 2015*, Główny Urząd Statystyczny, Warszawa 2015, s. 318.

Transport intermodalny jest wciąż, mimo wielu promujących inicjatyw podejmowanych przez UE oraz państwa członkowskie, niekonkurencyjny w stosunku do transportu drogowego i to zarówno pod względem cenowym, jak również jakości usług. Relatywnie niska efektywność funkcjonowania terminali intermodalnych oraz brak ujednoczonych oraz kompatybilnych na poziomie międzynarodowym systemów informacyjnych w lądowych i morsko-lądowych łańcuchach intermodalnych należą do podstawowych barier ograniczających rozwój transportu intermodalnego w Europie.

Niewystarczająca zdolność obsługowa, długi czas operacji przeładunkowych, częsty brak kompatybilności między taborem a wyposażeniem do obsługi jednostek intermodalnych, zbyt mały zakres nowoczesnych systemów informacyjnych dla klientów terminali – to główne słabe strony terminali intermodalnych w Europie.

Rozwój gospodarczy, zapotrzebowanie na usługi transportowe w relacjach Wschód-Zachód, znoszenia ceł oraz ograniczeń ilościowych w przewozach między państwami sprzyjają popytowi na przewozy ładunków i pasażerów (tabele 3.3 i 3.4).

Rozwój transportu samochodowego w Polsce po 1989 roku, kiedy zostały dokonane zmiany ustrojowe i przeobrażenia gospodarcze, a w konsekwencji nastąpiła zmiana kierunków polskiego handlu zagranicznego, wpłynął na długoterminowe planowanie polityki transportowej państwa. Liberalizacja rynku sprawiła, że w 1989 roku liczba małych i średnich firm powiększyła się niemal dwukrotnie – do 860 tys.¹²¹. Obecnie zarówno przedsiębiorstwa prywatne, jak i państwowe świadczą swoje usługi dla wszystkich usługobiorców na równych prawach.

¹²¹ Por. L. Mindur, *Przewozy międzynarodowego transportu drogowego w Polsce po transformacji gospodarczej*, [w:] *Logistyka* 4/2015, s. 1427.

Na uwagę zasługuje podkreślenie, że w przewozach międzynarodowych ładunków transportem samochodowym wykonywanych przez polskich przewoźników w Unii Europejskiej stanowią 25%, co lokuje Polskę na pierwszej pozycji przed Hiszpanią i Niemcami. W 2014 r. około 30 tys. polskich przedsiębiorstw trudniących się zarobkowym towarowym transportem drogowym posiadało licencje wspólnotowe i dysponowało ok. 164,5 tys. pojazdów samochodowych. Dodatkowo w międzynarodowych przewozach osób funkcjonuje 3,5 tys. przedsiębiorstw, posiadających 12 tys. pojazdów. Transport samochodowy jest zatem jednym z ważniejszych czynników kreujących wzrost konkurencyjności gospodarki Polski¹²².

Zaprezentowane tabele, wykresy i analizy dotyczące transportu, świadczą, że jest to dziedzina, która przez ostatnie lata jest w ciągłym rozwoju, a pozycja jej się umacnia. Przychody firm transportu samochodowego to 89 960 mln zł w 2013 roku, a więc jest to znacząca kwota w stosunku do budżetu ogółem za 2013 r, który wynosi 279 151 mln zł¹²³. Jest też znaczącym pracodawcą. Daje pracę 730 000 osobom, czyli 5% wszystkich zatrudnionych (w liczbie tej jest transport i gospodarka magazynowa)¹²⁴.

Należy podkreślić, że transport drogowy jest czynnikiem koordynującym i integrującym poszczególne elementy gospodarki w jedną całość. Wynika to również z podstawowych funkcji, jakie spełnia transport drogowy w gospodarce i realizacji zadań w ramach dziedzin i sektorów bezpieczeństwa narodowego: konsumpcyjnej – oznaczającej możliwość zaspokajania potrzeb przewozowych poprzez świadczenie usług przewozu, produkcyjnej – oznaczającej możliwości zaspokajania potrzeb produkcyjnych poprzez świadczenie usług przewozowych, a tym samym stworzenia warunków dla takiej działalności wytwórczej oraz funkcjonowania rynku produkcji, integracyjnej – która pozwala integrować państwo i społeczeństwo poprzez usługi transportowe (jest ona bardzo ważnym czynnikiem wyrównywania szans dla różnych regionów kraju).

Obserwujemy w Polsce rozwój sieci komunikacyjnych, szczególnie jest to widoczne w transporcie drogowym. Na koniec 2014 r. Polska posiadała 3025,7 km dróg szybkiego ruchu, w tym 1553,2 km autostrad (wykres 3.1) oraz 1472,7 km dróg ekspresowych¹²⁵. Mimo znacznego wzrostu długości autostrad w 2014 r. jest to nadal jeden z najniższych wskaźników w Unii Europejskiej (na 1000 km² powierzchni kraju długość autostrad stanowiła niespełna 5 km, natomiast na 100 tys. ludności kraju przypadało 3,6 km, podczas gdy w 2011 r. średnia dla 28 krajów UE wyniosła odpowiednio 16 km i 14 km)¹²⁶.

¹²² Tamże, s. 1427.

¹²³ *Rocznik Statystyczny Rzeczypospolitej Polskiej 2014*, Główny Urząd Statystyczny, Warszawa 2015, s. 537, 647.

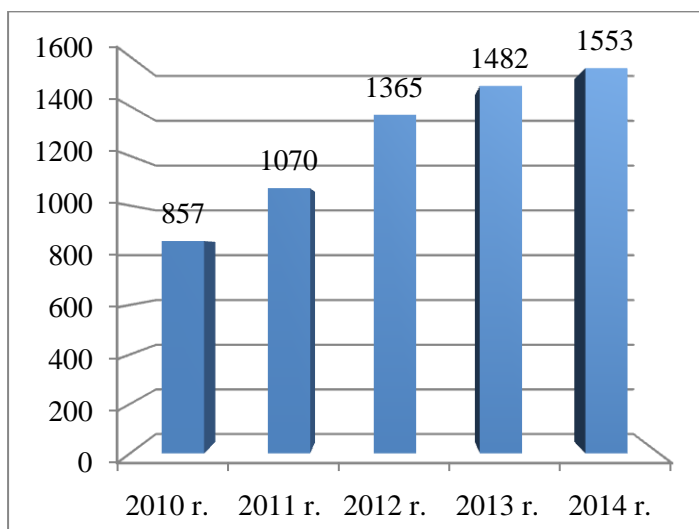
¹²⁴ Tamże, s. 239 i 241.

¹²⁵ *Raport roczny za 2014 r.*, 30 grudnia 2014 r., Generalna Dyrekcja Dróg Krajowych i Autostrad, <http://www.gddkia.gov.pl/pl>, 20.03.2015.

¹²⁶ *EU Transport In figures. Statistical Pocketbook 2014*, s. 76.

Wykres 3.1

Długość autostrad w Polsce w latach 2010-2014, w km



Źródło: opracowanie własne na podstawie *Transport, wyniki działalności. Roczniki statystyczne GUS*, Warszawa 2004-2014.

Transport samochodowy należy do najlepiej rozwijających się. Dzieje się tak dlatego, że jest to transport szybki, łatwy w użyciu, korzystny w przewozie osób na małe odległości, umożliwia dostawę towaru bezpośrednio do odbiorcy (od drzwi do drzwi), można się nim dostać wszędzie tam, gdzie nie ma dostępu, np. kolej, statek. Charakteryzuje się dużą prędkością przewozową, łatwym przystosowaniem pojazdów samochodowych do różnych postaci ładunków, łatwością dostosowania potencjału przewozowego do zmieniających się w czasie i przestrzeni zadań przewozowych. Spadające ceny samochodów również mają wpływ na rozwój transportu drogowego. Ilość pojazdów samochodowych i ciągników, zarejestrowanych na dzień 31.12.2014 roku, wzrosła w porównaniu z rokiem 2005 prawie ogółem o prawie 10 mln sztuk (tj. o około 60%), w tym samochodów osobowych około 8 mln, a samochodów ciężarowych, ciągników siodłowych, balastowych, rolniczych 1,5 mln szt. – tabela 3.5.

Transport, to nie tylko rozwój i postęp, ale również sfera, z którą są związane wypadki, do których dochodzi nie tylko na polskich drogach, o czym się często zapomina, również na terenie firm w tzw. transporcie wewnętrznym.

Analiza wypadków obejmuje skutki: dla ludzi, gospodarki, mienia, infrastruktury (w tym krytycznej), środowiska, infrastruktury¹²⁷.

Tabela 3.5

Stan pojazdów samochodowych i ciągników (w tys. szt.) zarejestrowanych na 31.12.2014 r.

| Wyszczególnienie | 2005 | 2010 | 2013 | 2014 |
|---|-------|-------|-------|-------|
| Ogółem, w tym: | 16816 | 23037 | 25684 | 26472 |
| Samochody osobowe | 12339 | 17240 | 19389 | 20004 |
| Autobusy | 80 | 97 | 103 | 106 |
| Samochody ciężarowe i ciągniki siodłowe | 2305 | 2982 | 3242 | 3341 |
| Ciągniki balastowe i rolnicze | 1243 | 1566 | 1633 | 1669 |
| Motocykle | 754 | 1013 | 1153 | 1190 |

Źródło: opracowano na podstawie, *Mały rocznik statystyczny Polski 2015*, Główny Urząd Statystyczny, Warszawa 2015, s. 323.

Skutki dla ludzi – pod uwagę bierze się przede wszystkim potencjalną ilość: ofiar śmiertelnych, rannych lub poważnie chorych (wymagających hospitalizacji, ewakuowanych). Ponadto, wskazuje się skutki dla życia codziennego. W zakresie skutków pośrednich mogą być też wskazane skutki społeczne (np. możliwy wzrost bezrobocia), jak również skutki związane z trwałą niezdolnością do pracy oraz skutki psychiczne.

Porównując różne gałęzie transportu w UE, w kontekście ryzyka śmierci pasażera okazuje się, że najbezpieczniejszym jest transport lotniczy. Natomiast najwięcej ludzi ginie w transporcie drogowym – tabela 3.6.

Tabela 3.6

Ryzyko wystąpienia ofiar śmiertelnych w zależności od rodzaju transportu, w EU w latach 2008 -2012

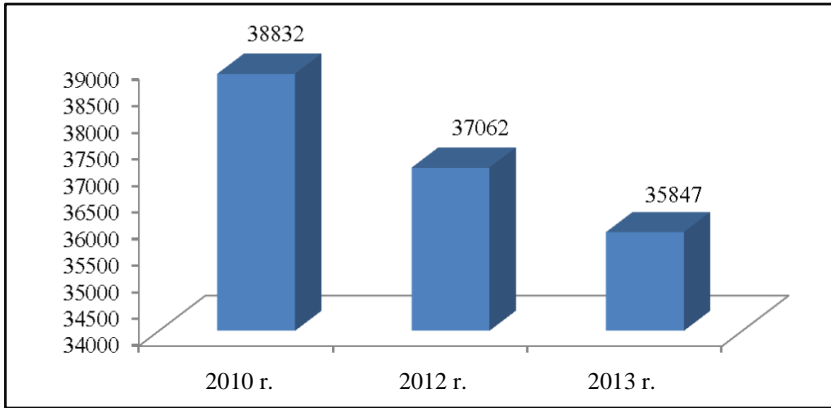
| Rodzaj transportu wybrany przez użytkownika | Liczba ofiar śmiertelnych na miliard pasażerokilometrów |
|---|---|
| Pasażer linii lotniczych | 0,06 |
| Pasażer kolei | 0,13 |
| Użytkownik autobusu | 0,20 |
| Użytkownik samochodu osobowego | 3,14 |
| Dwukołowy z silnikiem | 48,94 |

Źródło: *Railway safety performance in the European Union 2014*, European Railway Agency, s. 13.

¹²⁷ *Ocena ryzyka na potrzeby zarządzania kryzysowego Raport o zagrożeniach bezpieczeństwa narodowego*, Rządowe Centrum Bezpieczeństwa, Warszawa 2013, s. 13.

Wykres. 3.2

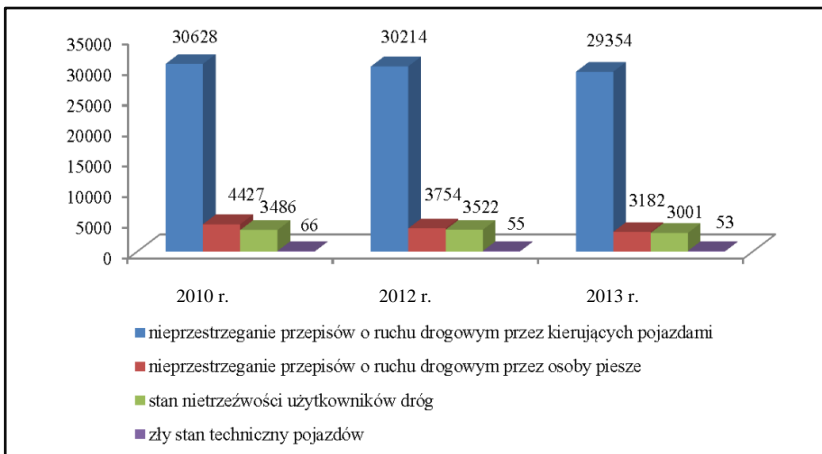
Ilość wypadków drogowych na 10 tys. pojazdów samochodowych i ciągników zarejestrowanych



Źródło: opracowanie własne na podstawie *Rocznik Statystyczny Rzeczypospolitej Polskiej 2014*,
Główny Urząd Statystyczny, Warszawa 2015, s. 548.

Wykres 3.3

Ważniejsze przyczyny wypadków drogowych



Źródło: opracowanie własne na podstawie *Rocznik Statystyczny Rzeczypospolitej Polskiej 2014*,
Główny Urząd Statystyczny, Warszawa 2015, s. 548.

Skutki dla gospodarki, mienia, infrastruktury – należy brać pod uwagę, że mogą być to zarówno skutki krótkoterwale, jak i długoterminowe. W analizie skutków dla mienia, w tym infrastruktury, określa się „zakłócenia” lub „zniszczenia”, jakie mogą wystąpić.

Analizując skutki dotyczące mienia, należy zwrócić uwagę na skutki bezpośrednie i pośrednie (efekt domina) lub skutki odłożone w czasie. O ile jest to możliwe wskazuje się szacunkowe koszty strat oraz koszty odbudowy.

Skutki dla środowiska – w ramach analizy skutków dla środowiska, oprócz określenia niekorzystnego wpływu danego scenariusza na środowisko, należy wskazać, które skutki są odwracalne/odnawialne, a które powodują całkowite zniszczenie/degradację środowiska. Przy opisie tych skutków ważne jest wskazanie możliwych przedziałów czasowych.

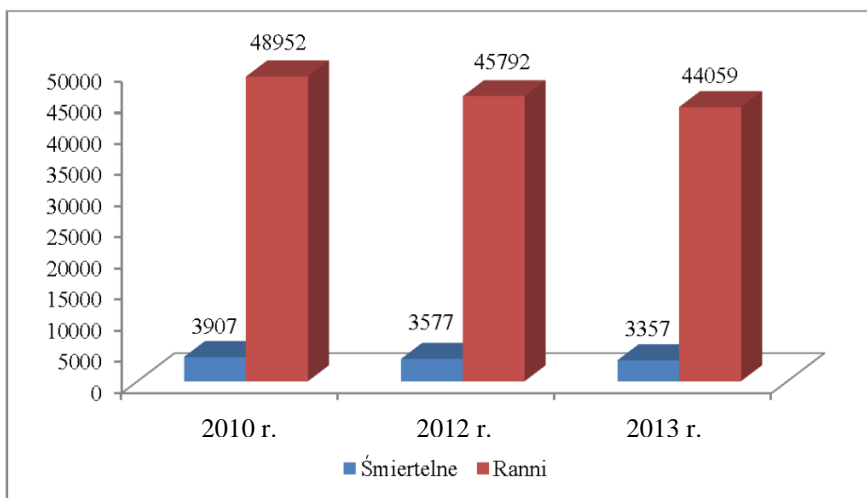
Polska w ujęciu negatywnym jest krajem przodującym w UE w dziedzinie wypadków, czego potwierdzeniem są dwa wskaźniki¹²⁸.

Pierwszy. Największą liczbę osób zabitych w 2013 roku odnotowano we Włoszech – 3385 osób, w Polsce – 3357 oraz w Niemczech – 3339.

Drugi. Najwyższy wskaźnik zabitych na 100 wypadków odnotowano w Polsce – 9,4 oraz w Rumunii – 7,5, zaś najwyższy wskaźnik rannych na 100 wypadków zanotowano na Cyprze – 145,9, we Włoszech – 142,0 oraz w Hiszpanii – 139,4.

Wykres 3.4

Ofiary wypadków drogowych



Źródło: opracowanie własne na podstawie *Rocznik Statystyczny Rzeczypospolitej Polskiej 2014*,
Główny Urząd Statystyczny, Warszawa 2015, s. 548.

Ostatnie dane zaprezentowane przez Główny Urząd Statystyczny oraz Komendę Główną Policji dotyczące wypadków w ruchu drogowym obejmują: ogólne dane o motoryzacji, czasie i miejscu powstawania wypadków, rodzaju

¹²⁸ Por. *Wypadki drogowe w Polsce w 2014 roku*, Komenda Główna Policji, Biuro Prewencji i Ruchu Drogowego, Wydział Ruchu Drogowego, Warszawa 2015, s. 80.

wypadków, przyczyny i sprawcy wypadków, ofiary wypadku, bezpieczeństwo osób pieszych i innych niechronionych uczestników ruchu, nietrzeźwych uczestników ruchu drogowego, wypadki ze skutkiem śmiertelnym. Przykładowe dane zostały zaprezentowane na wykresie 3.2, 3.3, 3.4.

Bezpieczeństwo transportu determinują następujące podstawowe wskaźniki: czynnik ludzki, środek transportu, środowisko¹²⁹. To one decydują o poziomie bezpieczeństwa na drogach.

Czynnik ludzki jest powszechnie uznawany za najważniejszy, a jego działanie najczęściej wpływa na powstawanie zdarzeń nadzwyczajnych. Przyczynami tego mogą być: zły stan zdrowia, niewystarczające zdolności przewidywania i wnioskowania, niewystarczająca wiedza i doświadczenie, różne przejściowe stany emocjonalne, presja czasu, nienormalne stany psychiczne.

W procesie transportowym człowiek występuje jako: uczestnik aktywny (kierowca samochodu, pilot samolotu, sternik, dyspozytor, podróżujący itp.) oraz uczestnik pasywny (przygodny przechodzień, człowiek zagrożony wypadkiem drogowym itp.).

Środek transportu wpływa na bezpieczeństwo poprzez swoje właściwości. Są one określone przez zbiór czynników konstrukcyjnych i eksploatacyjnych oraz dbałość (systematyczne przeglądy) o środek transportu i jego konserwację.

Środki transportu w obszarze bezpieczeństwa transportu należy rozpatrywać w kontekście: bezpieczeństwa aktywnego, umożliwiającego prewencję i naprawę błędów czynnika ludzkiego lub też innych wskaźników ruchu (urządzenia techniczne ułatwiające panowanie nad środkiem transportu i podwyższające jakość oraz szybkość reagowania kierowcy włącznie z czynnościami decyzyjnymi), bezpieczeństwa pasywnego wpływającego na powstanie i wielkość skutków niebezpiecznego zdarzenia (urządzenia techniczne i elementy pasywne, których celem jest ochrona człowieka w momencie wypadku i bezpośrednio po nim).

Środowisko to zbiór organizacyjnych, technicznych, społeczno-psychologicznych i innych warunków oddziałujących na człowieka i środek transportu. Stworzenie optymalnego środowiska do realizacji transportu jest sprawą obejmującą wiele dyscyplin fachowych i naukowych. Podstawowe elementy tworzące środowisko w transporcie to: obiekty transportowe (drogi transportu i obiekty na nich terminale transportowe itp.), urządzenia transportowe (urządzenia zabezpieczające, urządzenia pomocnicze i serwisowe, oznakowanie dróg itp.), systemy kierowania w transporcie (systemy informacyjne, systemy zautomatyzowane, organizacja kierowania ruchem itp.), otoczenie dróg transportu (przeszkody, przewężenia, obiekty rozpraszające uwagę itp.), warunki meteorologiczne (czas przewozu, pora roku, aktualny stan dróg transportu itp.), prawo transportowe (ustawy i przepisy prawne, wewnętrzne zasady eksploatacji itp.).

¹²⁹ T. Molková, *Hodnocení kvality v dopravním a přepravním procesu*, DF JP Pardubice 2009, s. 15.

Nie bez przyczyny w najważniejszych dokumentach dotyczących systemu bezpieczeństwa narodowego (tj. w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2003, 2007, 2014, Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022) wiele miejsca poświęca się zapobieganiu katastrofom, wypadkom komunikacyjnym, *dzięki korzystaniu z nowoczesnej infrastruktury transportowej, z unowocześnionych parków taborowych oraz z integralnych systemów zarządzania przewozami obniżają się koszty w gospodarce, przyczyniając się jednocześnie do obniżenia presji na środowisko*¹³⁰.

W Białej Księdze szczególną rangę nadano kontroli bezpieczeństwa ruchu drogowego i ochrony transportu – poprzez monitorowanie przestrzegania przepisów obowiązujących w zakresie wykonywania transportu drogowego i przewozu osób i rzeczy, mające na celu eliminowanie wszelkich negatywnych zjawisk w transporcie drogowym, a także zadania z zakresu przestrzegania przepisów porządkowych, ochrony życia i zdrowia ludzi oraz mienia na obszarze kolejowym (np. Inspekcja Transportu Drogowego, Straż Ochrony Kolei)¹³¹.

Transport kolejowy

Polska posiada wyjątkowo dobre i dogodne warunki geograficzno-prze-strzenne do rozwoju transportu lądowego, w tym kolejowego. Analizując sytuację transportu kolejowego po 1989, można stwierdzić, iż jego rozwój i modernizacja nie były tak widoczne jak w przypadku transportu samochodowego. Złożyło się na to kilka powodów, a między innymi to, że koniec XX wieku charakteryzował się spowolnieniem gospodarczym, procesami urynkowania gospodarki, transformacją ustrojową, prywatyzacją, wahaniem kursu złotego, przewagą importu nad eksportem, silnym zadłużeniem zagranicznym.

Sytuacja ekonomiczna Polski spowodowała, że transport kolejowy maksymalnie eksploatowano – był w miarę nowoczesny i integrował działy i gałęzie gospodarki wieloletnimi więzami kooperacji. Zamrożono inwestycje, remonty i modernizacje w tym obszarze. Transport kolejowy w tym okresie charakteryzował się wysokim nasyceniem kadrowym. Zatrudnienie w tym transporcie i jego otoczeniu było wysokie. W wyniku takiej polityki rozwoju transportu gałęzią transportu, która najbardziej traciła był transport kolejowy. Ograniczone nakłady i opóźnienia rozwojowe były także przyczyną błędów w strukturze inwestycji, szczególnie w infrastrukturze kolei. W efekcie nastąpił gwałtowny wzrost dekapitalizacji środków trwałych¹³².

¹³⁰ Por. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014, pkt. 23.

¹³¹ Por. *Biała Księga Bezpieczeństwa Narodowego...* op. cit., s. 179.

¹³² Por. W.J. Rogalski, *Transport kolejowy jako ogniwo w łańcuchu dostaw gospodarki polskiej*, [w:] *Logistyka* 2014/6, s. 13697.

Wiek XXI to okres, kiedy w dalszym ciągu na pierwszym planie był transport samochodowy w związku z EURO 2012, transport kolejowy modernizowano w miarę przydzielanych i posiadanych środków finansowych w sposób niewystarczający, o czym świadczy *Informacja o wynikach kontroli Bezpieczeństwo ruchu kolejowego w Polsce*, przeprowadzonej przez NIK w 2013 roku. Okazało się, że pod względem bezpieczeństwa w transporcie kolejowym Polska znajduje się na jednym z ostatnich miejsc w Europie. Ogólny poziom bezpieczeństwa w ruchu kolejowym, określany miernikiem wypadków¹³³, jest gorszy tylko w Rumunii, zaś miernik ciężkości wypadków jest w Polsce najgorszy w Europie¹³⁴.

Do dokonania oceny stanu bezpieczeństwa ruchu kolejowego jest brana pod uwagę liczba zaistniałych wypadków kolejowych oraz analiza ich przyczyn i skutków, a także występujących zagrożeń. Liczba wypadków kolejowych jest pochodną m.in. wielkości wykonywanych przewozów, intensywności ruchu kolejowego, stanu technicznego eksploatowanej sieci linii kolejowych oraz stanu technicznego pojazdów kolejowych.

W 2014 roku licencjonowane przewozy towarowe realizowało 67 przedsiębiorców. Licencjonowaną działalność przewozową realizowały między innymi¹³⁵:

- trzy spółki Grupy PKP: PKP Cargo SA, PKP LHS Sp. z o.o. (na wydzielonej organizacyjnie linii szerokotorowej) oraz PKP Energetyka Sp. z o.o. (przewozy wyłącznie na własne potrzeby utrzymaniowo-naprawcze infrastruktury energetycznej);
- sześć spółek Grupy CTL: CTL LOGISTICS SA, CTL Rail Sp. z o.o., CTLTrain Sp. z o.o., X-TRAIN Sp. z o.o., CTL Express Sp. z o.o., CTL Reggio Sp. z o.o.;
- sześć spółek Grupy DB Schenker: DB Schenker Rail Polska SA, DB Schenker Rail, SPEDKOL Sp. z o.o., DB Schenker Rail Zabrze SA, DB Schenker Rail COALTRAN, Sp. z o.o., NZTK Wola Sp. z o.o., DB Schenker Rail Rybnik SA;
- osiemnastu przewoźników towarowych: PUK KOLPREM Sp. z o.o., POL-MIEDŹ TRANS Sp. z o.o., LOTOS KOLEJ Sp. z o.o., TRANSODA Sp. z o.o., KP „KOTLARNIA” SA, ZIK Sandomierz S.J., RAIL POLSKA

¹³³ Liczba ofiar znaczących wypadków wyrażonej w FWSI (FWSI – przyjęta w prawie unijnym umowna miara liczby ofiar wypadków, w której zabici uwzględniani są z wagą 1, a ciężko ranni z wagą 0,1) w stosunku do pracy eksploatacyjnej mierzonej w milionach pociągokilometrów (FWSI/mln pociągokilometrów).

¹³⁴ *Informacja o wynikach kontroli bezpieczeństwa ruchu kolejowego w Polsce*, KIN-4114-01/2012 Nr ewid. 73/2013/I/12/003/KIN, s. 8.

¹³⁵ Por. A. Szymonik, *Ekonomika transportu dla potrzeb logistyka(i), Teoria i Praktyka*, Difin, Warszawa 2013, s. 99; *Ocena Funkcjonowania Rynku Transportu Kolejowego i Stanu Bezpieczeństwa Ruchu Kolejowego w 2014 roku*, www.utk.gov.pl/, 28.10.2015.

Sp. z o.o., KOLEJ, BAŁTYCKA S.A., ORLEN KOL-TRANS Sp. z o.o., GATX Rail Poland Sp. z o.o., EURONAFT TRZEBINIA Sp. z o.o., Lubelski Węgiel Bogdanka SA, PTK Koltar, Tarnów Sp. z o.o., STK Wrocław SA, MAJKOLTRANS Sp. z o.o., Freightliner PL, Sp. z o.o., Hagens Logistics Sp. z o.o., ITL Polska Sp. z o.o. oraz CEMET SA,

- sześć spółek realizujących wyłącznie przewozy bezpośrednio związane z budową, utrzymaniem i modernizacją infrastruktury kolejowej: DOLKOM Sp. z o.o., Przedsiębiorstwo Napraw Infrastruktury Warszawa Sp. z o.o., Pomorskie Przedsiębiorstwo Mechaniczno-Torowe Sp. z o.o., PNiUIK w Krakowie Sp. z o.o., PRKiI Wrocław SA oraz PRK KRAKOW SA.

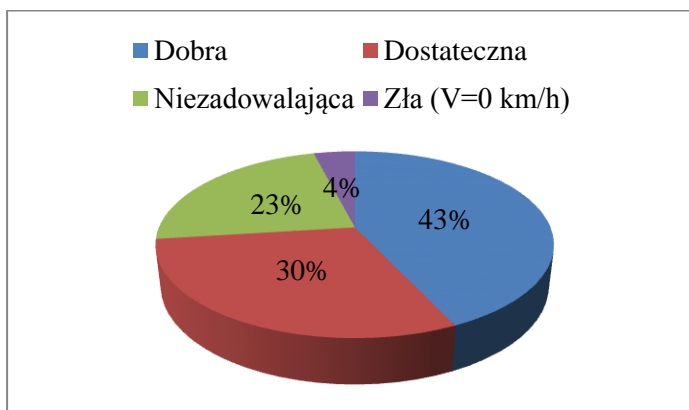
Według kryterium masy największy udział w rynku transportu kolejowego, w 2014 r., posiada Grupa PKP Cargo 47,94%, na kolejnych miejscach są: Grupa DB Schenker 18,55%, Grupa PKP LHS 4,66%. W 2014 r. udział przewoźników wg wykonanej pracy przewozowej na pierwszym miejscu jest Grupa PKP Cargo 56,69%, na drugim Lotos Kolej 8,87%, na trzecim PKP LHS 7,06%.

W tym samym czasie infrastrukturą kolejową w Polsce zarządzało 9 podmiotów, przy czym podstawowa sieć tej infrastruktury (93,2%) jest zarządzana przez PKP PLK SA.

Jednym z istotnych czynników obniżających poziom bezpieczeństwa ruchu kolejowego w Polsce jest niezadowolający stan techniczny ok. 27% infrastruktury kolejowej, co wynika głównie z wieloletniego jej niedofinansowania. W zakresie nawierzchni stan ten ilustrują dane na wykresie 3.5.

Wykres. 3.5

Stan techniczny nawierzchni kolejowej na dzień 31.12.2012



Źródło: *Informacja o wynikach kontroli bezpieczeństwa ruchu kolejowego w Polsce*, KIN-4114-01/2012 Nr ewid. 73/2013/I/12/003/KIN, s. 17.

Tabela 3.7

Przewozy ładunków w Polsce

| Wyszczególnienie | 2005 | 2010 | 2013 | 2014 |
|----------------------------|--------|--------|--------|--------|
| W milionach tonokilometrów | 228216 | 308073 | 347887 | 349587 |
| Transport kolejowy | 49972 | 48795 | 50881 | 50083 |

Źródło: *Mały rocznik statystyczny Polski 2015*, Główny Urząd Statystyczny, Warszawa 2015, s. 317.

Tabela 3.8

Tabor kolejowy w Polsce

| Wyszczególnienie | 2005 | 2010 | 2012 | 2013 |
|-------------------------------|--------|-------|-------|-------|
| Lokomotywy elektryczne | 1865 | 1905 | 1849 | 1838 |
| Lokomotywy spalinowe | 2520 | 2358 | 2264 | 2194 |
| Elektryczne zespoły spalinowe | 1341 | 1213 | 1226 | 1268 |
| Wagony towarowe | 103234 | 89270 | 91483 | 87726 |
| Wagony do przewozu podróżnych | 4495 | 3795 | 3356 | 3083 |

Źródło: opracowanie własne na podstawie *Rocznik Statystyczny Rzeczypospolitej Polskiej 2014*, Główny Urząd Statystyczny, Warszawa 2015, s. 542.

Tabela 3.9

Przewozy w milionach pasażerokilometrów w Polsce

| Wyszczególnienie | 2005 | 2010 | 2013 | 2014 |
|--------------------------------|-------|-------|-------|-------|
| W milionach pasażerokilometrów | 56183 | 47985 | 50088 | 51603 |
| Transport kolejowy | 18157 | 17921 | 16797 | 16061 |

Źródło: *Mały rocznik statystyczny Polski 2015*, Główny Urząd Statystyczny, Warszawa 2015, s. 318.

Na przestrzeni kilku ostatnich lat w Polsce nastąpił liczbowy wzrost przewożonego ładunku w tonokilometrach (tabela 3.7) i taboru (tabela 3.8), co ma wpływ na kondycję i ilość przedsiębiorstw trudniących się przewozami kolejowymi.

Analizując tabele i dane umieszczone w *Roczniku statystycznym Rzeczypospolitej Polskiej 2014* i *Małym roczniku statystycznym Polski 2015*, nasuwają się wnioski, że w 2014 roku: transportem kolejowym w Polsce przewożono zaledwie 14,0% ogółu przewożonych ładunków (w tonokilo-

metrach) oraz że w 2013 nastąpił znaczny spadek liczby wagonów towarowych i do przewozu osób.

W przewozach w milionach pasażerokilometrów w Polsce transportem kolejowym, porównując rok 2014 z 2005, można zauważyć, że utrzymuje się on na niezmiennym poziomie. W 2014 roku na 51603 mln pasażerokilometrów, na kolej przypadło 16061, co stanowi 31% ogółu pasażerokilometrów – tabela 3.9.

Zaprezentowane wielkości w sposób niekwestionowany argumentują, że bezpieczeństwo transportu kolejowego to fundamentalny element jego sprawnego funkcjonowania w czasie przewozu ładunków i pasażerów.

Transport kolejowy jest drugim, po samochodowym, w kontekście ilości przewożonych ładunków i pasażerów, a na pewno pierwszym w obszarze bezpieczeństwa i dbałości o środowisko. Jednak z przykrością należy stwierdzić, że z danych Europejskiej Agencji Kolejowej (ERA, *European Railway Agency*) wynika, że jedna piąta śmiertelnych ofiar wypadków na kolei w Unii Europejskiej (UE) ginie na polskiej sieci w sytuacji, gdy ludność Polski stanowi tylko jedną trzynastą populacji UE.

Tabela 3.10

Ekonomiczne skutki wypadków kolejowych w Polsce w 2012 r.

| Ekonomiczne skutki z podziałem na: | Całkowity koszt wszystkich wypadków (PLN) | Względny koszt wszystkich wypadków [w PLN na mil poc.km] |
|--|---|--|
| Liczbę zabitych i ciężko rannych pomnożoną przez wartość zapobiegania ofiarom w ludziach (VPC ¹³⁶) | 166.966.852,50 | 760.669,03 |
| Szkody w środowisku | 299.200,00 | 1.363,10 |
| Koszty szkód materialnych w pojazdach kolejowych lub infrastrukturze kolejowej | 18.774.545,29 | 85.533,24 |
| Opóźnienia spowodowane wypadkami | 525.980,00 mln. | |

Źródło: *Informacja o wynikach kontroli bezpieczeństwa ruchu kolejowego w Polsce*, KIN-4114-01/2012 Nr ewid. 173/2013/I/12/003/KIN, s. 23.

W 2012 r. ekonomiczne skutki dla polskiego społeczeństwa, wynikające z liczby ofiar śmiertelnych i osób ciężko rannych, wyrażone w VPC¹³⁷ (wartość

¹³⁶ VPC (wartość zapobiegania ofiarom w ludziach) – dla ofiary śmiertelnej przyjęto 341 tys. €, a dla osoby ciężko rannej 46,5 tys. €.

¹³⁷ VPC (wartość zapobiegania ofiarom w ludziach) – wartość, jaką społeczeństwo ponosi w związku z ofiarami wypadków, która nie stanowi podstawy do rekompensaty

zapobiegania ofiarom w ludziach) oszacowano na ok. 167 mln zł, zaś z tytułu szkód materialnych w pojazdach kolejowych i infrastrukturze kolejowej na 18,8 mln zł (szacunek ten dotyczy wyłącznie wypadków powstałych z winy zarządcy infrastruktury kolejowej, tj. Spółki PKP Polskie Linie Kolejowe (PKP PLK SA)¹³⁸ – tabela 3.10.

Tabela 3.11

Zestawienie przyczyn zdarzeń i wypadków kolejowych, w Polsce
w latach 2011 i 2012

| Kategoria wypadku | Liczba wypadków | Liczba wypadków | Ofiary wypadku – zabici | Ofiary wypadku – zabici | Ofiary wypadku – ciężko ranni | Ofiary wypadku – ciężko ranni |
|------------------------------|-----------------|-----------------|-------------------------|-------------------------|-------------------------------|-------------------------------|
| | 2011 r. | 2012 r. | 2011 r. | 2012 r. | 2011 r. | 2012 r. |
| Kolizje | 58 | 42 | 3 | 16 | 7 | 63 |
| Wykolejenia | 154 | 107 | 2 | 0 | 34 | 0 |
| Na przejazdach i przejściach | 243 | 259 | 62 | 60 | 51 | 40 |
| Z udziałem osób | 370 | 271 | 251 | 186 | 118 | 89 |
| Pożary | 4 | 1 | 0 | 0 | 0 | 0 |
| Inne | 0 | 4 | 0 | 0 | 0 | 3 |
| Razem | 829 | 684 | 318 | 262 | 210 | 195 |

Źródło: *Informacja o wynikach kontroli bezpieczeństwo ruchu kolejowego w Polsce*, KIN-4114-01/2012 Nr ewid. 73/2013/I/12/003/KIN, s. 60.

dla uczestników wypadków, podawana corocznie w Biuletynie Informacji Publicznej na stronie Prezesa Urzędu Transportu Kolejowego. Ustalana jest w oparciu o badania preferencji w ramach projektu HEATCO – *Developing Harmonised European Approaches for Transport Costing and Project Assess*. Na VPC składa się wartość bezpieczeństwa, tj. wartość gotowości do płacenia (WTP *Willingness to pay*) oparta na badaniach preferencji przeprowadzonych w Rzeczypospolitej Polskiej oraz pośrednie i bezpośrednie ekonomiczne koszty wypadków oszacowane w Rzeczypospolitej Polskiej, na które składają się koszty leczenia i rehabilitacji, koszty sądowe, koszty poniesione przez Policję, koszty prywatnych dochodzeń związanych z wypadkami, koszty akcji ratunkowej i koszty ubezpieczenia, a także straty w produkcji (wartość towarów i usług, które mogłyby powstać, gdyby wypadek się nie wydarzył), wg Dyrektywy Komisji 2009/149/WE z dnia 27 listopada 2009 r. zmieniającej dyrektywę 2004/49/WE Parlamentu Europejskiego i Rady w odniesieniu do wspólnych wskaźników bezpieczeństwa oraz wspólnych metod obliczania kosztów wypadków – Załącznik I *Wspólne wskaźniki bezpieczeństwa*, pkt 5 (Dz.U.UE.L.2009.313.65).

¹³⁸ *Informacja o wynikach kontroli bezpieczeństwo ruchu kolejowego w Polsce*, KIN-4114-01/2012 Nr ewid. 73/2013/I/12/003/KIN, s. 8.

Zgodnie z *Ustawą z dnia 28 marca 2003 r. o transporcie kolejowym* bezpieczeństwo jest ściśle związane z ilością nieszczęśliwych zdarzeń, do których zaliczamy: wypadki¹³⁹, poważne wypadki¹⁴⁰, incydenty^{141,142}.

Analizując zestawienie przyczyn i liczbę zdarzeń w transporcie kolejowym w latach 2011 i 2012, można stwierdzić, że mają one tendencje spadkowe, bowiem wypadków było mniej o 145, a liczba ofiar wypadków zmniejszyła się o 71 – tabela 3.11. Powodów do radości jednak nie ma, bowiem w analogicznym okresie w całej UE – 27 państw, w 2012 roku ofiar śmiertelnych było 1133 (w Polsce 262), poważnie rannych 1016 (w Polsce 195), co argumentuje, że w obszarze bezpieczeństwa w ruchu kolejowym jest jeszcze wiele do zrobienia.

Bezpieczeństwo komunikacyjne w transporcie kolejowym jest zależne od trzech grup czynników, tj. technicznych (związanych z infrastrukturą kolejową, w tym ze stanem drogi kolejowej, systemami sterowania ruchem – np. czuwak aktywny, samoczynne hamowanie pociągów, hamowanie obszarowe, systemami telekomunikacyjnymi, systemami zasilania oraz z taborem kolejowym), prawnych (związanych z wdrażaniem aktów prawa europejskiego, krajowego, instrukcji wewnętrznych i procedur, których bezwzględne przestrzeganie minimalizuje ryzyko dojścia do wypadku kolejowego – załącznik 3.1) oraz kadrowych (kompetencji, kwalifikacji oraz doświadczenia i doskonalenia zawodowego personelu kolejowego).

3.3. Telematyka w bezpieczeństwie procesów transportowych

Telematyka transportu jest to dział wiedzy o transporcie, integrujący informatykę i telekomunikację w zastosowaniach dla potrzeb zarządzania i sterowania ruchem w systemach transportowych, stymulujący działalność techniczno-organizacyjną umożliwiającą podniesienie efektywności i bezpieczeństwa eksploatacji tych systemów. Poszczególne rozwiązania telematyczne współpracują ze sobą, często pod kontrolą czynnika nadrzędnego.

¹³⁹ Wypadek – niezamierzone nagłe zdarzenie lub ciąg takich zdarzeń z udziałem pojazdu kolejowego, powodujące negatywne konsekwencje dla zdrowia ludzkiego, mienia lub środowiska; do wypadków zalicza się w szczególności: kolizje, wykolejenia, zdarzenia na przejazdach, zdarzenia z udziałem osób spowodowane przez pojazd kolejowy będący w ruchu, pożar pojazdu kolejowego.

¹⁴⁰ Poważny wypadek – wypadek spowodowany kolizją, wykolejeniem pociągu lub innym podobnym zdarzeniem: z przynajmniej jedną ofiarą śmiertelną lub przynajmniej pięcioma ciężko rannymi lub powodujący znaczne zniszczenie pojazdu kolejowego, infrastruktury kolejowej lub środowiska, które mogą zostać natychmiast oszacowane przez komisję badającą wypadek, na co najmniej 2 miliony euro, mający oczywisty wpływ na regulację bezpieczeństwa kolei lub na zarządzanie bezpieczeństwem.

¹⁴¹ Incydent – każde zdarzenie inne niż wypadek lub poważny wypadek, związane z ruchem pociągów i mające wpływ na jego bezpieczeństwo.

¹⁴² *Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym*, s. 13.

Telematyka w procesach transportowych jest utożsamiana z takim pojęciami, jak Inteligentne Systemy Transportowe i Inteligentny Transport.

Inteligentne Systemy Transportowe (ITS) obejmują szeroki zakres rozwiązań technologicznych mających na celu poprawę transportu poprzez zwiększenie mobilności i bezpieczeństwa w ruchu drogowym. Systemy te łączą w sobie wiele elementów i działań mających na celu usprawnienie lub poprawę szeroko rozumianego transportu w zakresie komunikacji, prewencji, sterowania i zarządzania ruchem, wykrywania zdarzeń, dozoru czy też eliminacji wykroczeń drogowych itd. W skład systemu ITS wchodzi między innymi: centra zarządzania ruchem, zintegrowane systemy zarządzania ruchem, systemy sterowania ruchem, w tym sterowania sygnalizacjami świetlnymi, systemy zarządzania transportem publicznym, systemy monitoringu wizyjnego CCTV¹⁴³, systemy monitoringu wizyjnego ARTR¹⁴⁴, systemy nadzoru prędkości, znaki zmiennej treści, systemy dynamicznego ważenia pojazdów, systemy mierzenia wysokości pojazdów, systemy informacji parkingowej.

Inteligentny Transport (IT) – to współpracujące ze sobą dwa układy: inteligentna droga oraz inteligentny pojazd, czyli pojazd wyposażony w urządzenia utrzymujące ciągłą, szczególnie bezprzewodową, wymianę informacji z urządzeniami zainstalowanymi nad/pod drogą lub jej poboczem.

Każdy system telematyczny w transporcie można opisać poprzez określenie jego struktury¹⁴⁵: **funkcjonalnej** (obsługuje elektroniczne transakcje w ramach płatności za korzystanie z infrastruktury drogowej, dostarcza informacji w sytuacjach zagrażających życiu i zdrowiu uczestników ruchu drogowego, zarządza ruchem, w tym nie tylko ruchem na drogach miejskich i zamiejskich, ale także w przypadku zdarzeń nadzwyczajnych w ruchu drogowym – incydentów, wspomaga zarządzanie operacjami transportu publicznego, w tym także taborem transportowym, wspomaga kierowców prowadzących pojazdy –

¹⁴³ Skrót CCTV pochodzi od angielskich słów: *Closed Circuit TeleVision* i oznacza telewizję połączoną w układzie zamkniętym. Ogólnie przez system CCTV rozumiemy zespół współpracujących urządzeń do odbioru, przetwarzania, przekazywania oraz archiwizacji i wyświetlania obrazu oraz dźwięku w obiektach monitorowanych. W skład systemu CCTV wchodzi: kamery przemysłowe, obiektywy, urządzenia rejestrujące obraz, monitory, zasilacze, przewody transmisyjne lub systemy bezprzewodowe, [w:] *System telewizji przemysłowej*, <http://www.it-site.pl/cctv.htm>, 17.07.2014.

¹⁴⁴ ARTR służy do rozpoznawania i wyszukiwania pojazdów samochodowych identyfikowanych na podstawie numerów rejestracyjnych. System rejestruje pojazd, wraz z oznaczeniem czasu i miejsca jego pobytu, oraz automatycznie rozpoznaje i przypisuje numery rejestracyjne samochodu z numerami wpisanymi w systemie jako poszukiwane, [w:] P. Szmigiel, A. Szmigiel, M. Stawowy, *Wybrane metody identyfikacji pojazdów w systemie telematyki transportu* <http://www.czasopismologistyka.pl>, 17.07.2014.

¹⁴⁵ K. Bartczak, *Technologie informatyczne i telekomunikacyjne jako podstawa tworzenia systemów telematycznych w transporcie*, [w:] *Współczesne procesy i zjawiska w transporcie*, USz, Szczecin 2006, ss. 14-17.

nawigacja, wspomaga informacyjnie pasażerów przed i w czasie podróży, wspomaga przestrzeganie przepisów prawnych dotyczących poruszania się po drogach, wspomaga zarządzanie operacjami transportowymi), **fizycznej** (kształtowana jest przez centra systemu, czyli miejsca, gdzie gromadzi się zebrane dane i je przetwarza za pomocą komputerów, np. centra sterowania ruchem – TCC, centra informacji – TIC, centra zarządzania ładunkami i pojazdami itp., pobocza drogi, czyli miejsca, gdzie istnieją urządzenia do pomiaru ruchu, zbierania opłat, dostarczania informacji kierowcom itp., pojazdy, czyli miejsca, będące środkami transportu, gdzie zainstalowano odpowiednie systemy elektroniczne – pokładowe, zdolne do elektronicznej wymiany informacji z otoczeniem, urządzenia osobiste, będące w posiadaniu kierowcy lub pasażera, które umożliwiają im elektroniczną łączność z innymi elementami systemu telematycznego, urządzenia zainstalowane na jednostkach ładunkowych, np. kontenerach, naczepach, które mają możliwość elektronicznego przekazywania lub odbierania informacji z otoczeniem, kioski, czyli urządzenia dostępne w miejscach publicznych, które umożliwiają w ograniczony sposób dostęp do zasobów informacji zgromadzonych w bazach danych w systemie transportowym), **komunikacyjnej** (poszczególne fizyczne miejsca systemu telematycznego, połączone pomiędzy sobą elektronicznie w ramach określonego systemu łączności – utworzenie odpowiedniej struktury komunikacyjnej systemu telematycznego w transporcie wymaga doboru odpowiednich technologii informatycznych i telekomunikacyjnych, które są ogólnodostępne na rynku komercyjnym).

Monitorowanie samochodowych środków transportowych

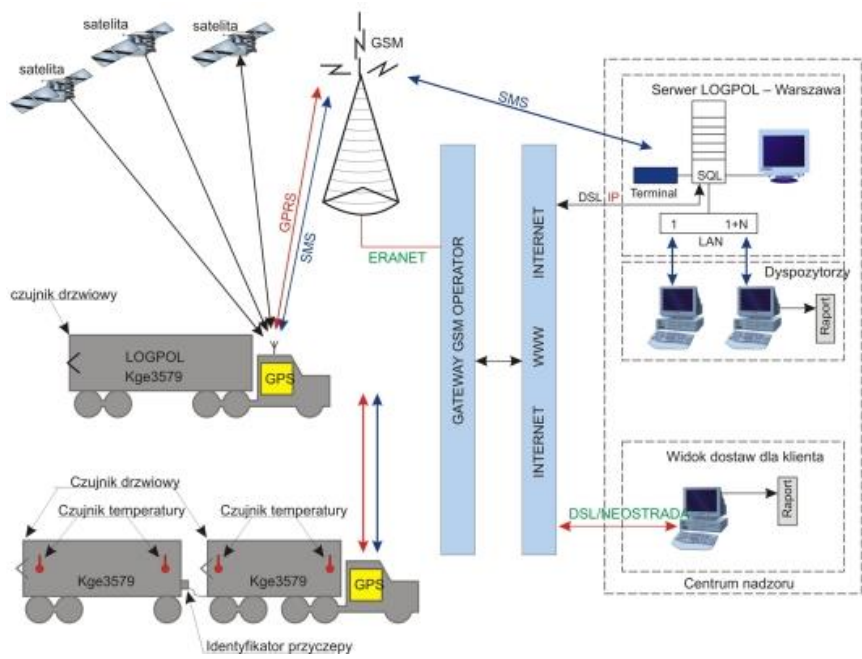
Rozwój transportu (w roku 2014 w Polsce było 26472 tys. szt. zarejestrowanych pojazdów samochodowych i ciągników oraz około 26000 firm transportowych¹⁴⁶) oraz nowych technologii informatycznych, telekomunikacyjnych umożliwi wprowadzanie zintegrowanych usług, polegających na ciągłym określaniu położenia pojazdów oraz automatycznym nadzorowaniu przewozów w transporcie krajowym i międzynarodowym.

Narastające zatłoczenie na drogach i szlakach kolejowych, zmienne warunki pogodowe, różne – pojawiające się nagle – zdarzenia na drogach i na kolei mają duży wpływ na jakość i bezpieczeństwo wykonywania zadań transportowych. Coraz ważniejsza w transporcie oraz w akcjach poszukiwawczych i ratunkowych staje się łączność ruchoma.

Wiele firm, w tym polskich, produkuje wiele urządzeń, które w połączeniu z innymi technikami i technologiami stanowią system ustalania pozycji i danych pojazdu, które pozwalają na: automatyczne przekazywanie informacji o trasie przejazdu środka transportowego (stały monitoring); odnalezienie pojazdu, który

¹⁴⁶ *Mały rocznik statystyczny Polski 2015*, Główny Urząd Statystyczny, Warszawa 2015, s. 323, K. Bentkowska-Senator, Z. Kordel, *Polski transport samochodowy w łańcuchach dostaw*, [w:] *Logistyka* 3/2012, s. 115.

np. został skradziony; zdalne unieruchomienie pojazdu, np. w przypadku kradzieży; przekazywanie informacji związanych z transportem materiałów niebezpiecznych odpowiednim służbom w celu ograniczenia prawdopodobieństwa katastrofy i zapobiegania jej skutkom; optymalizowanie kosztów przewozowych i eksploatacyjnych (dane w czasie rzeczywistym o prędkości, czasie pracy, postojach, a także planowanie tras przejazdu ze względów bezpieczeństwa, tj. natężenia ruchu, remontów, warunków atmosferycznych, stanu nawierzchni); zarządzanie przewozami w trybie on-line (eliminowanie pustych przebiegów i niewykorzystanej przestrzeni ładunkowej, szybka reakcja w przypadku nieprzewidzianych zdarzeń, takich jak wypadki czy kradzież); efektywne wykorzystanie środków transportu i potencjału ludzkiego (przygotowanie w odpowiednim czasie rozładunku, szybkie reagowanie na zaburzenia w planowaniu transportów).



Rys. 3.1. Schemat satelitarnego systemu śledzenia pojazdu

Źródło: W. Szulc, *Elektroniczne metody monitorowania ruchomych środków transportowych*, <http://www.zabezpieczenia.com.pl/>, 17.07.2014.

W praktyce do monitorowania ruchomych środków transportu wykorzystuje się systemy ogólnie dostępne na rynku, wykorzystujące satelitarny, globalny system pozycjonowania GPS (*Global Positioning System*), w połączeniu z pakietową transmisją danych GPRS (ang. *General Packed Radio System*) oraz

GSM (*Global System for Mobile Communication*) cyfrowej telefonii komórkowej działającej na częstotliwości 900 MHz.

Działanie obecnych satelitarnych systemów monitorowania pojazdów wykorzystujących GPS jest możliwe dzięki zastosowaniu kombinacji zaawansowanych technik satelitarnych, telekomunikacyjnych oraz informatycznych. Satelitarne systemy monitorowania pojazdów są zbudowane z czterech podstawowych podsystemów (rys. 3.1)¹⁴⁷:

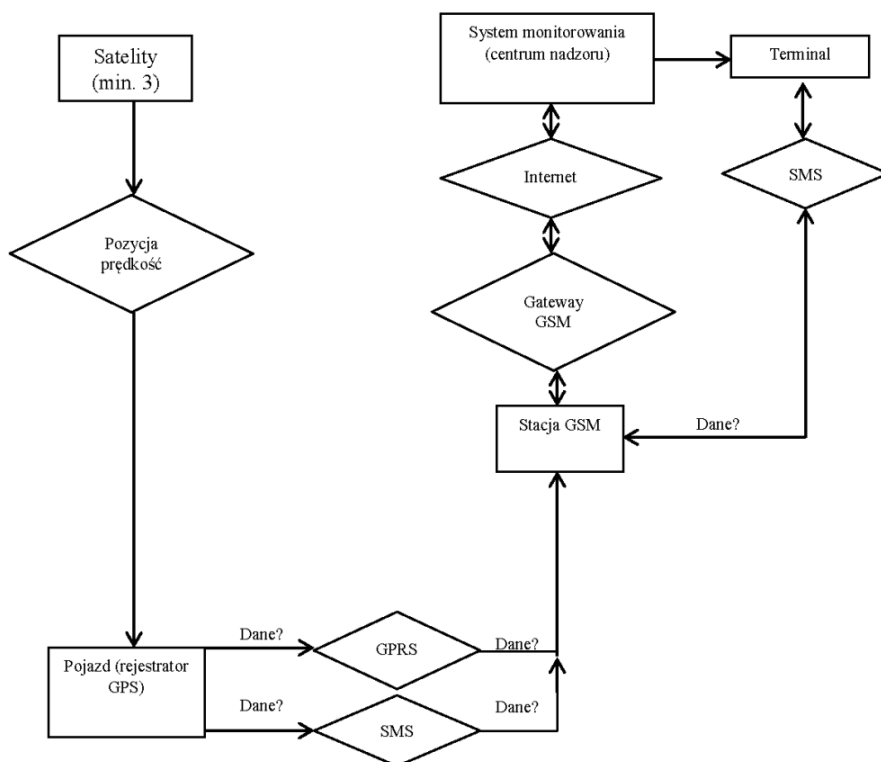
- lokalizacji – wykorzystuje 24 amerykańskie satelity wojskowe NAVSTAR systemu GPS, dokładność systemu wynosi około 25 m (90% pomiarów), a po zastosowaniu stacji referencyjnej średni błąd wynosi około 5 m;
- odbioru i przetwarzania danych – zainstalowany w obiekcie ruchomym, do jego zadań należy m.in. odbieranie sygnałów satelitarnych (sygnały te, po przetworzeniu ich przez mikroprocesor, są danymi w postaci współrzędnych geograficznych oraz parametru prędkości, informacje te wraz z raportami o stanie obiektu są przesyłane do stacji monitorowania);
- transmisji danych – wykorzystuje konwencjonalne oraz trunkingowe sieci radiowe (np. PMR – *Private Mobile Radio*, PAMR – *Public Access Mobile Radio*), telefonię komórkową (GSM – *Global System for Mobile Communications*, UMTS – *Universal Mobile Telecommunications System*), w tym pakietową transmisję danych, jak również łączność satelitarną (podsystem ten odpowiada za zagwarantowanie dwustronnej łączności pomiędzy monitorowanym obiektem a centrum monitoringu);
- zarządzania, odpowiedzialny za ciągle nadzorowanie obiektu oraz zarządzanie nim, zarówno w trakcie jego przemieszczania się, jak również w czasie postoju.

Przedstawiony system zapewnia, podobnie jak większość innych, opisanych w dalszym ciągu rozwiązań¹⁴⁸: lokalizowanie obiektów transportowych w czasie rzeczywistym z wykorzystaniem GPS; monitorowanie obiektów z wykorzystaniem szczegółowych, cyfrowych planów miast oraz map drogowych Polski i Europy; całodobowy dostęp do bieżących i archiwalnych informacji o lokalizacji obiektów; tanie i szybkie przesyłanie danych dzięki wykorzystaniu pakietowej transmisji danych GPRS; aktywację trybu alarmowego przez system czujników ruchu w przypadku nieprzewidzianego przechyłu lub przemieszczenia pojazdu; skuteczne, całodobowe zabezpieczenie przed kradzieżą pojazdu i ładunku; montaż dokonywany w sposób uniemożliwiający osobom niepowołanym dostęp do odbiornika GPS i zapewniający jego niewykrywalność; zarządzanie flotą pojazdów; wspomaganie rozliczeń kosztów eksploatacji

¹⁴⁷ Por. W. Drewek, *Monitorowanie ładunków niebezpiecznych w transporcie drogowym*, [w:] *Logistyce* 5/2011, s. 515.

¹⁴⁸ Por. W. Szulc, *Elektroniczne metody monitorowania ruchomych środków transportowych*, <http://www.zabezpieczenia.com.pl/>, 17.07.2014.

środków transportu przez zautomatyzowaną wymianę danych (ta cecha nie jest powszechna wśród innych opisywanych systemów).



Rys. 3.2. Algorytm komunikacji pomiędzy obiektem transportowym a systemem monitorowania (centrum nadzoru)

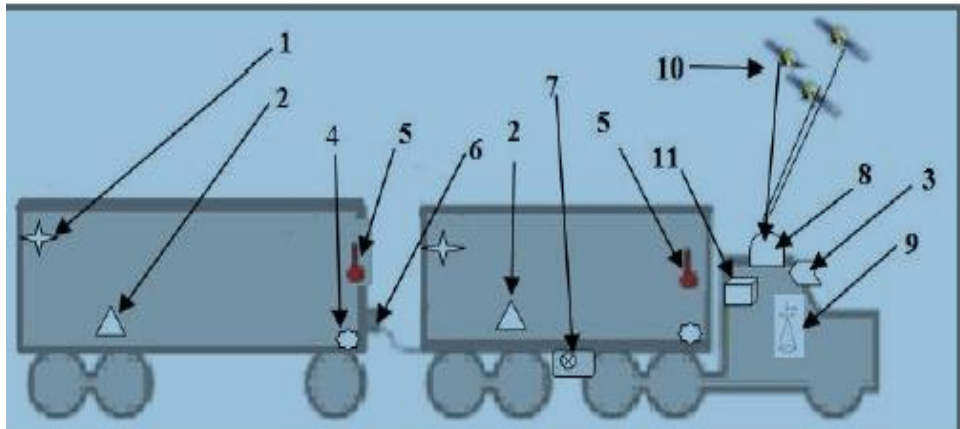
Źródło: W. Szulc, *Elektroniczne metody monitorowania ruchomych środków transportowych*, <http://www.zabezpieczenia.com.pl>, 17.07.2014.

Strukturę algorytmu komunikacji obiektu transportowego (ruchomego środka transportowego) z systemem monitorowania (centrum nadzoru) przedstawiono na rys. 3.2.

Algorytm obejmuje trzy główne bloki: system monitorowania (centrum nadzoru), stację GSM, pojazd (ruchomy obiekt transportowy).

System monitorowania, w celu nawiązania łączności z wybranym obiektem transportowym, łączy się drogą internetową lub poprzez SMS ze stacją GSM za pomocą specjalnego terminala. Następnie pojazd (wyposażony w sterownik lokalizacji i transmisji) wysyła potrzebne informacje do stacji GSM dwiema wariantowymi drogami, tj. przez GPRS albo przez SMS. Stacja GSM wysyła zebrane dane do stacji monitorowania (centrum monitorowania).

Wszystkie dane do komputera oznaczonego liczbą 11 spływają od czujników, które są rozmieszczone w różnych częściach środka transportu (rys. 3.3).



1 – czujnik wykrywania i identyfikacji kontenerów, 2 – czujnik stabilności ładunku, 3 – czytnik autoryzacji, 4 – czujnik wypadku, 5 – czujnik temperatury, 6 – identyfikator przyczepy, 7 – czujnik otwarcia zbiornika paliwa, 8 – moduł GSP, 9 – moduł GSM, 10 –satelity, 11 – komputer.

Rys. 3.3. Schemat satelitarnego systemu śledzenia pojazdu

Źródło: W. Drewek, *Monitorowanie ładunków niebezpiecznych w transporcie drogowym*, Logistyka 5/2011, s. 516.

Czujnik wykrywania i identyfikacji kontenerów – stwierdzenie obecności kontenera uaktywnia czytnik transponderowy RFID umieszczony z tyłu kabiny pojazdu. W zależności od sposobu ładowania, każdy kontener zostaje wyposażony w jeden lub dwa transpondery RFID. Czytnik identyfikuje unikalny kod przypisany każdemu z nich. Zebrane informacje o obecności (z czujnika obecności) oraz unikalnym kodzie (czytnik transponderów) kontenera są przekazywane do jednostki centralnej (komputera), skąd wraz z informacją o pozycji geograficznej pojazdu i czasie trafiają do dyspozytora (czy kierowcy)¹⁴⁹.

Czujnik stabilności ładunku (może być zamontowanych kilka) pozwala na stwierdzenie jego fizycznej obecności na pojeździe, czy ładunek znajduje się w takim położeniu, w jakim został ułożony podczas załadunku. Po załadunku pojemnik (opakowanie) zostaje „wykryty” – fale odbijające się od powierzchni opakowania potwierdzają jego obecność i odległość od krawędzi skrzyni ładunkowej lub ścian kontenera. Czujnik pełni funkcję kontrolną i aktywującą w stosunku do czytnika RFID. Czytnik identyfikuje kod przypisany każdemu czujnikowi¹⁵⁰.

¹⁴⁹ *Moduł identyfikacji kontenerów i pojemników typu dzwon*, <http://elte.systemygps.com.pl/>, 10.07.2014.

¹⁵⁰ Zob. W. Drewek, *Monitorowanie ładunków niebezpiecznych w transporcie drogowym...*, op. cit., s. 516.

Czujniki wypadku wysyłają do systemu GPS/GSM sygnał alarmowy o zdarzeniu, podając współrzędne. Przez wypadek należy rozumieć zderzenie lub przewrócenie się pojazdu w dowolnej osi. Natychmiast po jednym z wymienionych zdarzeń jest przesyłany sygnał alarmowy do jednostki centralnej, która wysyła komunikat na serwer dyspozytora i na nr tel. 112.

Czujnik otwarcia korka wlewu paliwa – zabezpieczenie korka wlewowego paliwa do samochodów ciężarowych i maszyn – jest urządzeniem montowanym na wlewach baków paliwa, w celu monitorowania i kontrolowania stanu otwarcia lub zamknięcia wlewu paliwa. Działanie urządzenia jest oparte na technologii radiowej kontroli dostępu (RFID), więc jakiegokolwiek próby ingerencji skutkują sygnalizacją naruszenia z powiadomieniem SMS lub email. Montaż polega na zastąpieniu dotychczasowego korka specjalnym odlewem przymocowanym na stałe do wlewu paliwa¹⁵¹.

Czujnik temperatury, np. chłodni samochodu – dane trafiają do systemu i w połączeniu z pozostałymi informacjami o monitorowanym pojeździe są cennym materiałem do analizy. Zamontowanie takiego czujnika do samochodu chłodni pozwala na ciągłą kontrolę temperatury przewożonych towarów. Z jednej strony, mamy niezależną i zdalną kontrolę pracy agregatu, z drugiej strony, pozwala na uchronienie się przed oskarżeniami kontrahentów o przewożenie towarów w nieodpowiednich warunkach. Zastosowanie cyfrowego czujnika zapewnia dużą dokładność pomiaru i nie wymaga żadnych dodatkowych kalibracji.

Czujnik przyczepy – identyfikator w postaci chipu, montowany w gnieździe złącza spiralnego, łączącego przyczepę (naczepę) z ciągnikiem. Stosowany w przypadkach, gdy możliwe jest wymienne używanie przyczep (naczep). Umożliwia tworzenie zestawień pracy przyczep.

Czujnik otwarcia, najczęściej transponderowy (chip o unikatowym numerze odczytywany drogą radiową), umożliwia kontrolę otwarcia klap, drzwi itp.

Identyfikacja systemów monitorowania i lokalizacji pojazdów

Współczesne systemy nawigacji satelitarnej z racji ich powszechności i użyteczności można podzielić na systemy o zasięgu: ogólnosiwiatowym (zapewniają możliwość lokalizacji dowolnego obiektu z dokładnością rzędu 100 m, z prawdopodobieństwem 98%) – GPS NAVSTAR (*Global Positioning System*), GLONASS (*Global Navigation Satellite System*); systemy o zasięgu regionalnym: EGNOS (*European Geostationary Navigation Overlay System*), będący rozszerzeniem regionalnym systemów globalnych w celu poprawienia dokładności pozycjonowania obiektów (zwiększenie dokładności do około 5-10 m), EUTELTRACS (*Eutelsat Transport Ranging and Communication Services*).

¹⁵¹ Por. A. Szymonik, *Ekonomika transportu dla potrzeb logistyka(i) Teoria i Praktyka*, Difin, Warszawa 2013, s. 189.

System GLONASS (*Global Navigation Satellite System* albo ГЛОНАСС, *Глобальная навигационная спутниковая система*) jest rosyjskim odpowiednikiem amerykańskiego systemu GPS NAVSTAR. Oba systemy działają na zasadzie biernego pomiaru.

EGNOS jest europejskim systemem satelitarnym, wspomagającym systemy GPS i GLONASS, a w przyszłości GALILEO¹⁵². Najważniejsze zadania to transmisja poprawek różnicowych i informowanie o awariach systemu GPS. System znacznie zwiększy dokładność i wiarygodność pozycji uzyskiwanej z GPS, co będzie miało szczególne znaczenie dla lotnictwa. Odpowiednikami EGNOS w Ameryce Północnej jest WASS (*Wide Area Augmentation System*), w Indiach – GAGAN (*GPS Aided Geosynchronous Augmented Navigation System*), a w Japonii – MSAS (*Multi-functional Satellite Augmentation System*)¹⁵³.

EGNOS – program budowy został zatwierdzony przez Radę Unii Europejskiej w 1994 roku. W ciągu czterech lat opracowano wymagania techniczne dla systemu. W tym czasie na orbicie umieszczono dwa satelity telekomunikacyjne, które później wykorzystano do emisji poprawek EGNOS. W 2003 roku ukończono prace nad pierwszym elementem segmentu naziemnego systemu – w niemieckim mieście Langen otwarto pierwszą stację kontrolną EGNOS, w wersji 1 ruszył w lipcu 2005 roku. Rok później udostępniono wersję 2.1, która dawała dostęp w czasie rzeczywistym do mierzonych poprawek. W 2008 r. system w wersji 2.2 objął swoim zasięgiem również część Afryki. Oficjalne ogłoszenie pełnej operacyjności usługi otwartej (*Open Service*) nastąpiło 1 października 2009 roku. Obecnie segment naziemny EGNOS składa się z 34 stacji pomiarowo-obszernych RIMS (jedna z nich od 27 września

¹⁵² System Galileo jest europejskim odpowiednikiem amerykańskiego systemu GPS NAVSTAR oraz rosyjskiego GLONASS). Jest on z założenia systemem cywilnym, nad którym kontrolę sprawować będzie międzynarodowe grono specjalistów, gwarantujące ciągłość jego pracy. Galileo będzie systemem radiolokacyjnym, pozwalającym na określanie położenia punktów i poruszających się obiektów wraz z parametrami ich ruchu w dowolnym miejscu na powierzchni Ziemi, niezależnie od pogody, pory dnia i nocy. Zasada jego działania będzie oparta na pomiarze drogi przebytej przez sygnał od satelity poruszającego się po ściśle zdefiniowanej orbicie do anteny odbiornika. Lokalizacja obiektów na powierzchni Ziemi będzie zatem polegała na określeniu czasu potrzebnego fali elektromagnetycznej na przebycie drogi między satelitą a użytkownikiem. System Galileo składać się będzie z trzech następujących segmentów: kosmicznego (30 satelitów), naziemnego (dwa komponenty kontroli satelitów i całości misji systemów), użytkownika (wszystkie gałęzie transportu, zarządzanie przesyłaniem energii elektrycznej, finanse, bankowość, ubezpieczenia, nawigacja osobista, poszukiwanie i ratownictwo, zarządzanie w sytuacjach kryzysowych, zarządzanie środowiskiem, rolnictwo i rybołówstwo).

¹⁵³ Por. J. Januszewski, *Stacje segmentu naziemnego nawigacyjnych systemów satelitarnych i systemów je wspomagających*, wn.am.gdynia.pl/, 18.07.2014.

2004 r. pracuje w Centrum Badań Kosmicznych PAN w Warszawie), 4 stacji kontrolnych (MCC), 6 stacji transmitujących (NLES) oraz 2 stacji kontrolno-testowych (w Tuluzie i Torrejon). Zgodnie z danymi publikowanymi przez administratorów systemu, EGNOS umożliwia wyznaczenie pozycji z dokładnością 3 m w poziomie i 4 m w pionie. Niezawodność rozwiązania wynosi zaś 99%.

System wspomaganie satelitarnego EGNOS, dzięki zwiększeniu efektywności pracy GPS NAVSTAR i GLONASS, przyczyni się do¹⁵⁴: polepszenia koordynacji ruchu i bezpieczeństwa w transporcie drogowym, kolejowym, czy żegludze śródlądowej; sprawniejszego funkcjonowania służb porządkowych, policji, służby zdrowia, komunikacji miejskiej, taksówek, firm przewozowych czy turystów, dla których znajomość pozycji i parametrów ruchu jest także bardzo ważną informacją; dokładnego określania czasu dostarczania przesyłek, co wpłynie na poprawę obsługi klienta, dzięki możliwości informowania go o ewentualnych opóźnieniach i ich powodach; latania bez uwzględniania tuneli powietrznych; redukcji czasu lotu, jak i zużycia paliwa, a tym samym zmniejszenia zanieczyszczeń powietrza; pewniejszego wykonywania manewrów lądowania niezależnie od warunków pogodowych, redukując występujące opóźnienia, odwołania lotów czy lądowania na lotniskach alternatywnych; zwiększenia przepustowości pasów startowych, a także bezpieczeństwa na lotniskach i lądowiskach; usprawnienia naziemnej kontroli lotów, obsługę zwiększającego się ciągle ruchu lotniczego, redukując jednocześnie infrastrukturę naziemną; usprawnienia w sektorze morskim nawigacji, zarządzania i administrowania ruchem statków, wykonywania manewrów portowych, analizowania wypadków i katastrof, eksploracji i eksploatacji dna morskiego, jak również prowadzenia połowów; usprawnienia w transporcie naziemnym optymalizacji szlaków drogowych i ich większej kontroli; dokładnego administrowania pojazdów, poprzez ich ciągłe śledzenie i precyzyjne rejestrowanie ich pozycji; szybkiej lokalizacji pojazdów skradzionych czy w przekazywaniu informacji turystycznych; oszczędności finansowych właścicieli linii kolejowych, poprzez eliminację konieczności zbędnego okablowywania torów; usprawnienia funkcjonowania przejazdów kolejowych; zapewnienia globalnej, stabilnej (na poziomie kilku nanosekund względem uniwersalnego czasu koordynowanego UTC¹⁵⁵) skali odniesienia czasu (przyczyni się to do lepszej synchronizacji, a wraz z serwisami GSM i UMTS do powstania wielu nowych usług).

¹⁵⁴ Tamże.

¹⁵⁵ UTC – Uniwersalny czas koordynowany, UTC (*Universal Time Clock* lub *Coordinated Universal Time*, fr. *Temps Universel Coordonné*) – wzorcowy czas ustalany na podstawie TAI (fr. *Temps Atomique International*), uwzględniający nieregularność ruchu obrotowego ziemi i koordynowany względem czasu słonecznego.

Inteligentne systemy transportu drogowego

Inteligentne Systemy Transportowe (ITS) obejmują szeroki zakres rozwiązań technologicznych mających na celu poprawę transportu poprzez zwiększenie mobilności i bezpieczeństwa w ruchu pasażerskim i towarowym. Oznacza to systemy, które stanowią szeroki zbiór różnych technologii (telekomunikacyjnych, informatycznych, automatycznych i pomiarowych), jak również technik zarządzania stosowanych w transporcie, w celu zwiększenia bezpieczeństwa uczestników ruchu, zwiększenia efektywności systemu transportowego oraz ochrony zasobów środowiska naturalnego.

Dyrektywa Parlamentu Europejskiego i Rady nr 2010/40/EU z dnia 7 lipca 2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu nakreśliła sześć priorytetowych działań: zapewnienie dostępnych na terenie całej UE usług w zakresie informacji o podróży z wykorzystaniem różnych rodzajów transportu; zapewnienie dostępnych na terenie całej UE usług informacyjnych dotyczących ruchu w czasie rzeczywistym; dane i procedury dotyczące bezpłatnego dostarczania użytkownikom – w miarę możliwości – minimalnego zakresu powszechnych informacji o ruchu, związanych z bezpieczeństwem drogowym; zharmonizowane zapewnienie interoperacyjnej usługi eCall¹⁵⁶ na terenie całej UE; zapewnienie usług informacyjnych o bezpiecznych i chronionych miejscach parkingowych dla samochodów ciężarowych i pojazdów użytkowych; zapewnienie usług w zakresie rezerwacji bezpiecznych i chronionych miejsc parkingowych dla samochodów ciężarowych i pojazdów użytkowych.

Korzyści płynące z zastosowania inteligentnych systemów transportowych są różnorakie. Z badań wynika, iż zastosowanie ITS powoduje¹⁵⁷: zwiększenie przepustowości sieci ulic średnio o 22,5%; poprawę bezpieczeństwa ruchu drogowego (zmniejszenie liczby wypadków średnio o 60%); zmniejszenie czasów podróży i zużycia energii (o blisko 60%); poprawę jakości środowiska naturalnego (redukcję emisji spalin o średnio 40%); poprawę komfortu podróżowania i warunków ruchu kierowców podróżujących transportem zbiorowym oraz pieszych; redukcję kosztów zarządzania taborom drogowym; redukcję kosztów związaną z utrzymaniem i renowacją nawierzchni; zwiększenie korzyści ekonomicznych w regionie, w którym są zastosowane rozwiązania ITS.

Dostęp do bieżących informacji jest możliwy dzięki wykorzystaniu nowoczesnych technologii, które są widoczne w pojeździe i na zewnętrznych

¹⁵⁶ eCall – ogólnoeuropejski system szybkiego powiadamiania o wypadkach drogowych. eCall jest związany z inicjatywą eSafety, która jest częścią kompleksowej strategii Komisji Europejskiej, zmierzającej do zachowania bezpieczeństwa na drogach i poprawy efektywności transportu w Europie.

¹⁵⁷ *Inteligentne Systemy Transportowe*, <https://neurosoft.pl/>, 11.11.2015.

tablicach czy monitorach. Do nich zaliczamy: GPS – jeden z systemów nawigacji satelitarnej; DSRC – (*Dedicated Short Range Communication* – dedykowana komunikacja krótkiego zasięgu), technika oparta na przesyłaniu danych w krótkim obszarze, wykorzystana w transporcie wysokotonazowym w celu pobierania opłat za przejazdy wyznaczonymi odcinkami dróg (rozwiązanie to znalazło zastosowanie we wprowadzonym od 1 lipca 2012 roku elektronicznym systemie poboru opłat – viaToll); sieci bezprzewodowe (GSM/EDGE¹⁵⁸, Wi-Fi), podobnie jak technologie wykorzystywane do tradycyjnego łączenia się z Internetem pozwalają na szybką komunikację; telefonia komórkowa – aplikacje ITS mogą przekazywać dane poprzez sieci 3G¹⁵⁹ lub 4G¹⁶⁰ (zaletą telefonii komórkowej jest obraz wideo dostępny na żywo); systemy łączności radiowej (DAB, RDS-TMC)¹⁶¹; urządzenia do monitorowania ruchu (sensory, detektory, sterowniki, wideodetektory); urządzenia nadzoru telewizyjnego (kamery nadzorujące); urządzenia i systemy monitorowania i pomiaru pogody; zmienne tablice świetlne; geograficzne bazy danych (GIS)¹⁶²; bazy danych drogowych; karty elektroniczne.

W wielu krajach usprawnienie systemu transportowego polega nie tylko na budowaniu dróg, usprawnianiu istniejących, ale również na zastosowaniu tego, co jest związane z nowymi technikami i technologiami (np. czujnik, chipy, technologie bezprzewodowe itp.).

¹⁵⁸ EDGE – (*Enhanced Data rates for GSM Evolution*) – technologia używana w sieciach GSM do przesyłania danych.

¹⁵⁹ System telefonii komórkowej 3G – umożliwia nieograniczony dostęp radiowy do globalnej infrastruktury telekomunikacyjnej za pośrednictwem segmentu naziemnego, zarówno dla użytkowników stacjonarnych, jak i ruchomych. Jest systemem integrującym w zamierzeniu wszystkie systemy telekomunikacyjne (teleinformatyczne, radiowe i telewizyjne).

¹⁶⁰ System telefonii komórkowej 4G – technologia oparta o sieć radiową o szybkim przesyłaniu i wielofunkcyjnych punktach nadawczo-odbiorczych. Główną cechą odróżniającą 4G od swojej poprzedniczki (3G) jest szybkość transferu pomiędzy urządzeniami.

¹⁶¹ DAB – system (*Digital Audio Broadcasting*) stworzony jest dla radiofonii naziemnej i satelitarnej – zarówno do odbiorników stacjonarnych, jak i ruchomych. Zadaniem DAB jest: odbieranie programów przez odbiorniki stacjonarne, przewoźne i przenośne (antena prętowa) w otoczeniu powodującym odbicia i zaniki sygnału; transmitowanie informacji dodatkowych (poza programami), w tym wykorzystanie dotychczasowych systemów RDS (*Radio Data System*), TMC (*Traffic Message Channel*) i EWS (*Emergency Warning System*); *Rozwój radiotelefonii i telewizji*, <http://itpedia.pl/>, 17.07.2014.

¹⁶² GIS (*Geographical Information System*) – pojęcie *geograficzny system informacyjny* jest używane dla określenia skomputeryzowanego systemu umożliwiającego zbieranie, przechowywanie, analizę i obrazowanie danych związanych z określoną lokalizacją w środowisku geograficznym.

Inteligentne systemy transportowe w transporcie kolejowym

W transporcie kolejowym ważnym instrumentem jest Europejski System Zarządzania Ruchem Kolejowym – ERTMS (*European Railway Traffic Management System*).

Stanowi on jedno z kluczowych przedsięwzięć, którego celem jest zapewnienie jak największej interoperacyjności¹⁶³ transportu, szczególnie kolei w Europie. System ERTMS umożliwia¹⁶⁴: podniesienie poziomu bezpieczeństwa ruchu pociągów; zwiększenie zdolności przepustowej linii kolejowej; zmniejszenie ryzyka wypadków, odnowę urządzeń łączności i dostosowanie do standardów międzynarodowych; podniesienie jakości przewozów w związku z możliwością uruchomienia dodatkowych usług przy jego wykorzystaniu.

ERTMS obejmuje między innymi zunifikowaną europejską radiołączność pociągową **GSM-R** (*Global System for Mobile Communications – Railway*) i zunifikowany europejski system bezpiecznej kontroli jazdy pociągu **ETCS** (*European Train Control System*). Obydwa systemy są istotnymi składnikami europejskiej polityki likwidacji barier w transporcie, zarówno w wymiarze barier technicznych na sieciach kolejowych wewnątrz granic UE, jak i w zakresie budowania wspólnego rynku produktów i usług na rzecz kolei.

ETCS – zapewnia realizację sygnalizacji kabinowej i ciągłą kontrolę pracy maszynisty. Zgodnie z polskimi przepisami prowadzenie pociągu z prędkością przekraczającą 160 km/h wymaga sygnalizacji kabinowej. System ETCS dostosowuje się do potrzeb linii kolejowej poprzez wdrożenie odpowiedniego poziomu ETCS. Poziomy pierwszy, drugi i trzeci są zgodne w dół, co oznacza, że pojazd wyposażony w wyższy poziom może jeździć nie tylko po liniach tego poziomu ETCS, ale także po liniach poziomów niższych¹⁶⁵.

GSM-R – jest kolejową wersją systemu GSM, pracującą w paśmie 900 MHz. GSM-R odpowiada funkcjonalnie wersji GSM 2+, udostępniającej użytkownikom, obok kanału „rozmownego”, cyfrowy kanał radiowy do przesyłania danych i realizacji funkcji, przewidzianych dla specjalistycznych zastosowań dla kolei. GSM-R, oprócz realizacji funkcji łączności techno-

¹⁶³ Interoperacyjność oznacza zdolność transeuropejskiego systemu kolei do bezpiecznego i niezakłóconego ruchu pociągów, przy zapewnieniu wymaganych wielkości osiągow. W praktyce oznacza to, że interoperacyjny tabor może poruszać się po interoperacyjnej infrastrukturze kolejowej i przemieszczać się pomiędzy sieciami kolejowymi poszczególnych państw bez konieczności zatrzymywania się na granicach, wymiany lokomotyw i maszynistów. Cechy te mają zapewnić wysoki poziom bezpieczeństwa oraz jakość usług, wg M. Kornaszewski, M. Chrzan, *Zaangażowanie Polski we wdrażanie systemu ERTMS na tle wybranych krajów europejskich*, Logistyka, 3/2012, s. 169.

¹⁶⁴ Por. A. Szymonik, *International logistics*, Lodz University of Technology Press, Lodz 2014, s. 93.

¹⁶⁵ Por. A. Szymonik, *International ...*, op. cit., s. 93.

logicznej dla kolei, stanowi również medium transmisyjne dla systemu ETCS poziom 2 i 3, którymi są przesyłane zezwolenia na jazdę wydawane przez Radiowe Centrum Sterowania (*Radio Block Centre – RBC*) poszczególnym pociągom znajdującym się w obszarze danego RBC. Drogą radiową z użyciem systemu GSM-R są również przesyłane informacje aktualizacyjne w systemie ETCS poziom 1 wykorzystującym funkcje radio infill. System GSM-R w perspektywie kilkunastu lat zastąpi obecnie eksploatowany, przestarzały system radiolączności analogowej 150 MHz¹⁶⁶.

Tabela 3.12

Długość linii kolejowych, na których uruchomiono łączność GSM-R w Europie

| Kraj | Długość w km |
|-------------|---------------------------------------|
| Niemcy | 25 000 |
| Włochy | 11 000 (100 km w tunelach) |
| Szwecja | 8000 |
| Norwegia | 4000 |
| Holandia | 3500 |
| Francja | 3000 |
| Hiszpania | 2000 |
| Szwajcaria | 1800 |
| Austria | 1000 |
| W. Brytania | 500 (jest zainstalowana na 12 500) |
| Czechy | 200 |
| Litwa | 100 |

Źródło. M. Rabsztyń, *Łączność GSM-R w ruchu międzynarodowym*, Biuletyn informacyjny, Ministerstwo Infrastruktury, Warszawa 2010, 4/2010, s. 17.

Według UIC Międzynarodowego Związku Kolei, łączność GSM-R jest w Europie zainstalowana na różnym poziomie. Przodują w tym zakresie koleje niemieckie i włoskie (tabela 3.12, kraje niewykazane dopiero pracują nad budowaniem tego typu sieci).

Towarowe przewozy kolejowe podlegają nieco innym przepisom, regulowanym przez PKP, ale coraz częściej wymagane jest monitorowanie całych składów pociągów i znajdujących się w nich towarów (nie chodzi tu o sterowanie ruchem kolejowym). Problem dotyczy również bezpieczeństwa obsługi oraz samych środków transportowych.

System monitorowania środków transportowych w ruchu kolejowych może mieć duże znaczenie w przypadku przewozu ładunków cennych bądź wyma-

¹⁶⁶ Tamże.

gających specjalnego nadzoru z innych względów (np. strategicznych). Ze względu na tego rodzaju przeznaczenie w klasie użytkowników mogą znaleźć się służby celne, policja, SOK (Straż Ochrony Kolei), Straż Graniczna oraz firmy ochroniarskie, specjalizujące się np. w przewozach pieniędzy, ładunków o charakterze specjalnym (np. materiały promieniotwórcze), węgla (np. ze Śląska w głąb kraju) itp. I tutaj cennymi są te narzędzia, które wykorzystuje się w telematyce w transporcie drogowym. Do nich zaliczmy systemy¹⁶⁷: komunikacji elektronicznej, łączące poszczególne elementy systemu telematycznego (sieci rozległe WAN, sieci lokalne LAN, sieci telekomunikacji ruchomej, systemy satelitarne); pozyskiwania informacji (czujniki pomiarowe, kamery wideo, radary); prezentacji informacji dla administratorów systemu telematycznego (systemy GIS, systemy kontroli dostępu); prezentacji informacji dla użytkowników systemu (sygnalizacja świetlna, radiofonia, technologie internetowe – WWW, SMS).

Najważniejszymi funkcjami systemów telematycznych są funkcje operowania informacją. Dotyczy to jej pozyskiwania, przetwarzania, dystrybucji wraz z transmisją i wykorzystania w różnorodnych procesach decyzyjnych. Systemy i aplikacje telematyczne są konstruowane do określonych procesów.

Narzędziem, które ma być szeroko wdrożone i zastosowane w transporcie kolejowym jest globalny system nawigacji satelitarnej – GNSS (*Global Navigation Satellite System*), który składa się z dwóch podstawowych elementów: segmentu kosmicznego oraz segmentu naziemnego. Ponadto funkcjonują szeroko rozumiane segmenty kontrolne, przez niektórych uważane za części segmentu naziemnego.

Według analiz przeprowadzonych przez CER (Wspólnota Kolei Europejskich) i UIC (Międzynarodowy Związek Kolei) można obecnie wskazać ponad 40 obszarów zastosowania systemu GNSS w transporcie kolejowym. W uproszczeniu można je podzielić na pięć podstawowych grup¹⁶⁸:

- GNSS w inżynierii kolejowej, budowie i modernizacji systemów kolejowych, przeglądach, diagnostyce i obsłudze serwisowej;
- aplikacje komercyjne, rynku masowego, kompleksowej informacji i zarządzania;
- podstawowe systemy bezpieczeństwa;
- aplikacje zwiększające bezpieczeństwo – wspomaganie kierowania, zabezpieczenia systemów podstawowych;
- automatyzacja procesów związanych z zarządzaniem taborem i ruchem kolejowym, precyzyjną koordynacją, wykorzystaniem GNSS jako źródła czasu dla innych systemów.

¹⁶⁷ Por. K.B. Wydro, *Telematyka – znaczenie terminu*, <https://www.itl.waw.pl/czasopisma/TiTI/2005/1-2/116.pdf>, 17.07.2014.

¹⁶⁸ Por. A. Szymonik, *Ekonomika...* op. cit., s. 150.

W praktyce zastosowane systemy GNSS:

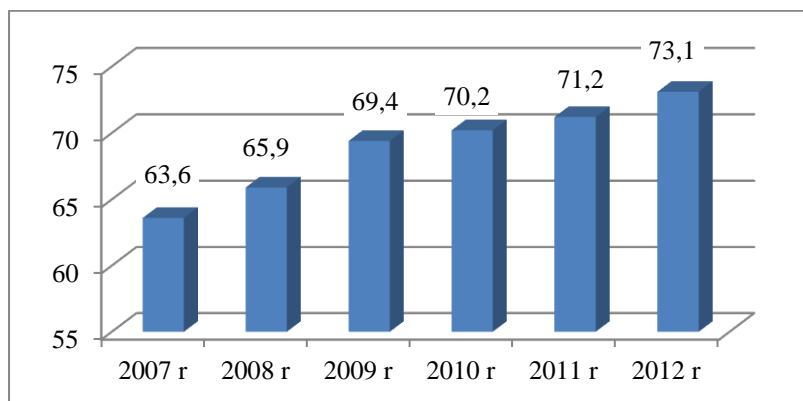
- usprawniają pomiary geodezyjne niezbędne do modernizacji i budowy szybkich kolei;
- dokonują oceny jakości wykonanych prac lub stanu technicznego torowiska;
- dokonują przeglądów dużych sieci kolejowych, wykonywanych za pomocą kamer cyfrowych sprzężonych z odbiornikami systemu GNSS zainstalowanymi na lokomotywach (umożliwia to proste, bezobsługowe dokumentowanie stanu sieci kolejowej oraz jej otoczenia);
- dokładnie określają położenie, szybkości poruszania się oraz czas, dzięki temu pasażerowie pociągu na swoich indywidualnych terminalach pasażerskich lub na ogólnych monitorach wagonowych będą mogli zobaczyć mapę pokonywanej trasy ze wskazaniem miejsca, w którym się aktualnie znajdują oraz dowiedzieć się, z jaką prędkością się poruszają i czy pociąg jedzie zgodnie z rozkładem jazdy (pasażerowie planujący przesiadki dowiedzą się, czy ich pociągi odjadą zgodnie z rozkładem jazdy i z którego peronu, a osoby oczekujące na pociąg będą dokładnie informowane o czasie, jaki pozostał do jego przyjazdu);
- umożliwiają śledzenie wagonów dzięki transponderom RFID i bramkom wzdłuż trasy pociągu, co pozwala właścicielom wagonów, nadawcom i odbiorcom ładunków wiedzieć, gdzie się one znajdują i kiedy dotrą do celu (jest to tzw. system automatycznej identyfikacji pojazdów w transporcie kolejowym AVI – *Automatic Vehicle Identification*);
- pozwalają zmniejszyć zagrożenie w czasie transportów środków toksycznych, materiałów wybuchowych i łatwopalnych, a także odpadów nuklearnych i materiałów rozszczepialnych poprzez: nadzorowanie ruchu ładunku na całej jego trasie, wybór bezpiecznej trasy i miejsc postojowych, ograniczenie czasu transportu, wykrywanie nieprawidłowości i zagrożeń, szybką lokalizację w przypadku wykrycia zagrożenia, skrócenie czasu reakcji na zdarzenie, użycie właściwych sił i środków do zwalczania zagrożenia.

3.4. Bezpieczeństwo gospodarki magazynowej

Bezpieczeństwo gospodarcze w systemie bezpieczeństwa narodowego jest ściśle związane z gospodarką magazynową, która to pozwala na realizację takich procesów, jak: przeładunek kompletacyjny, spedycje, obsługę celną, magazynowanie, sortowanie. To w magazynach przechowuje się zapasy o różnym przeznaczeniu i późniejszym wykorzystaniu. Bez magazynów trudno wyobrazić sobie funkcjonowanie gospodarki narodowej, dziedzin i sektorów bezpieczeństwa. O znaczeniu magazynów świadczą między innymi zestawienia liczbowe, opracowane przez Instytut Logistyki i Magazynowania w 2013 roku (wykresy 3.6 i 3.7), z których wynika, że w Polsce w 2012 r. całkowita powierzchnia magazynów zamkniętych wynosiła ok. 73,1 mln m², w tym nowoczesnych 9,7 mln m².

Wykres. 3.6

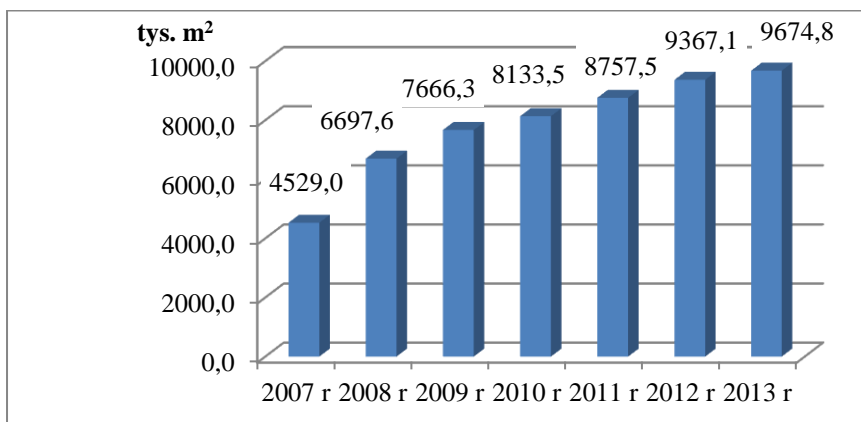
Wielkość ogółem powierzchni magazynów zamkniętych w Polsce
w latach 2007-2012 w mln m²



Źródło: opracowano na podstawie *Logistyka w Polsce Raport 2013*,
red. nauk. I. Fechner, G. Szyszka, ILiM, Poznań 2014, s. 118.

Wykres. 3.7

Nowoczesna powierzchnia magazynowa¹⁶⁹ w latach 2007-2013 w tys. m²



Źródło: opracowano na podstawie *Logistyka w Polsce Raport 2013*,
red. nauk. I. Fechner, G. Szyszka, ILiM, Poznań 2014, s. 118.

¹⁶⁹ Nowoczesna powierzchnia magazynowa – powierzchnia w obiekcie magazynowym o następujących parametrach: wysokość składowania min. 9 m, min. 1 brama na 1000 m² powierzchni, posadzka w magazynie bezpylna, o wytrzymałości min. 5 t/m², system ppoż. w postaci zraszaczy i kłap dymowych, 5-8% powierzchni biurowej, wg *Logistyka w Polsce Raport 2013*, red. nauk. I. Fechner, G. Szyszka, ILiM, Poznań 2014, s. 118.

Magazyny są ściśle związane nie tylko z produkcją i usługami, ale również z utrzymaniem różnych środków zaopatrzenia, w tym rezerw strategicznych, w celu zabezpieczenia potrzeb (resortom siłowym, służbom publicznym, ratowniczym, potrzebującym pomocy) w zakresie materiałowym w czasie pokoju, kryzysu i wojny.

Środki zaopatrzenia, przykładowo w SZ RP, zostały podzielone na 5 grup¹⁷⁰, które gromadzi się w magazynach w celu uzyskania ustalonych poziomów – normatywów.

Gromadzenie zapasów obejmuje trzy zasadnicze fazy przedsięwzięć: narastanie poziomów zapasów – okres pomiędzy wprowadzeniem danego rodzaju środka na uzbrojenie wojsk a osiągnięciem zapasu normatywnego; utrzymywanie zapasów – okres gospodarowania zapasami, w tym nadzorowanie właściwego rozmieszczenia zapasów, ich stanu jakościowego, itp.; wycofywanie środków zaopatrzenia – okres wycofywania środków materiałowych nieprzydatnych dla sił zbrojnych (np. zestarzenie techniczne lub moralne)¹⁷¹.

Racjonalny, sprawny i transparentny system rezerw strategicznych wspiera wykonywanie zadań w zakresie bezpieczeństwa i obrony państwa, odtworzenia infrastruktury krytycznej, złagodzenia zakłóceń w ciągłości dostaw służących funkcjonowaniu gospodarki i zaspokojeniu podstawowych potrzeb obywateli, ratowania życia i zdrowia obywateli, a także wypełnienia zobowiązań międzynarodowych Rzeczypospolitej Polskiej¹⁷².

Rezerwy strategiczne to między innymi: surowce, materiały, urządzenia, maszyny, konstrukcje składanych wiaduktów, mostów drogowych i kolejowych, elementy infrastruktury krytycznej, produkty naftowe, produkty rolne i rolno-spożywcze, środki spożywcze i ich składniki, wyroby medyczne, produkty

¹⁷⁰ Środki zaopatrzenia w SZ RP są podzielone na pięć klas (wg: *Doktryna Logistyczna Sił Zbrojnych Rzeczypospolitej Polskiej DD/4*, Sztab Generalny, Warszawa 2004, s. 25).

a) klasa I – środki zaopatrzenia przeznaczone do konsumpcji zarówno przez personel, jak i zwierzęta, występujące w jednolitych racjach niezależnie od lokalnych warunków bojowych lub terenowych;

b) klasa II – środki zaopatrzenia, na które zostały ustalone tabele należności lub wyposażenia;

c) klasa III – paliwa, oleje i smary do wszelkich zastosowań z wyłączeniem lotnictwa oraz bojowe środki specjalne wytwarzane na bazie produktów naftowych;

klasa IIIA – paliwa lotnicze, oleje i smary stosowane w lotnictwie;

d) klasa IV – środki zaopatrzenia, w tym materiały konstrukcyjne i fortyfikacyjne, dla których nie zostały ustalone tabele należności i wyposażenia;

e) klasa V – środki bojowe.

¹⁷¹ *Doktryna Logistyczna Sił Zbrojnych Rzeczypospolitej Polskiej DD/4*, Sztab Generalny, Warszawa 2004, s. 26.

¹⁷² Biała Księga Bezpieczeństwo Narodowe Rzeczypospolitej Polskiej, Biuro bezpieczeństwa Narodowego, Warszawa 2013, s. 101.

lecnicze, produkty lecznicze weterynaryjne¹⁷³. Rezerwy strategiczne są ściśle związane z takimi działaniami, jak tworzenie, udostępnianie, wymiana, zamiana – są to typowe procesy gospodarki magazynowej.

Realizacja gospodarki magazynowej jest uzależniona od tzw. węzłowych punktów modalnych¹⁷⁴ sieci logistycznej, które w praktyce, w zależności od czasu powstawania, klasyfikacji, przeznaczenia przybierały nazwę: budynku (obiektu) magazynowego, centrum magazynowego, logistycznego centrum usług, centrum dystrybucji, parku logistycznego, centrum logistycznego, hubu logistycznego¹⁷⁵.

Oprócz wymienionych, do węzłów sieci możemy zliczyć między innymi: porty morskie, lotnicze, śródlądowe, sortowanie paczek, intermodalne terminale przeładunkowe.

Do najczęściej używanych nazw w praktyce możemy zaliczyć: centrum logistyczne, centrum dystrybucji, centrum magazynowe, magazyn.

O tym, z jakim węzłem mamy do czynienia decyduje zakres usług przez niego realizowanych. I tak najczęściej, np.: magazyn – wykonuje przeładunek kompletacyjny, spedycje, obsługę celną, magazynowanie, sortowanie; centrum magazynowe – oprócz wymienionych – wykonuje usługi telekomunikacyjne; centrum logistyczne – realizuje czynności magazynu, centrum magazynowego i ponadto prowadzi usługi finansowe, ubezpieczeniowe, gospodarkę opakowaniami, serwis i naprawy samochodów oraz urządzeń transportowych, sprzedaż paliw, usługi socjalno-bytowe, pomoc medyczną.

Z zakresem czynności wykonywanych przez magazyn, centrum magazynowe, centrum logistyczne związana jest ilość budynków, budowli, powierzchnia, stopień mechanizacji, automatyzacji, liczba zatrudnionych i inwestorów (centra magazynowe – najczęściej jeden inwestor – developer, centra logistyczne – wielu inwestorów).

Podstawowym i głównym zadaniem realizowanym w centrach logistycznych jest przeładunek intermodalnych jednostek transportowych (kontenerów, nadwozi wymiennych i naczep samochodowych), a dodatkowo ma w nim miejsce świadczenie usług niezwiązanych bezpośrednio z logistyką.

W działalności centrów logistycznych można wyróżnić trzy rodzaje funkcji¹⁷⁶: **logistyczne** (transport, magazynowanie, zarządzanie zapasami,

¹⁷³ Ustawa z dnia 29 października 2010 r. o rezerwach strategicznych, s. 2.

¹⁷⁴ Mianem punktów modalnych sieci logistycznych określamy miejsca zatrzymania się produktów, tzn. magazyny, punkty i węzły transportowe oraz fabryki, sieci dystrybucji itd.

¹⁷⁵ hub – główny punkt (węzeł) przeładunkowy sieci opartej o terminale, połączone między sobą komunikacją drogową, kolejową, morską lub lotniczą; huby mogą być połączone z innymi hubami lub terminalami, podczas gdy terminale są połączone tylko z hubami, [w:] *Leksykon spedytora*, <https://www.google.pl/>, 22.07.2014.

¹⁷⁶ Por. A. Szymonik, *Eurologistyka, Teoria i Praktyka*, Difin, Warszawa 2013, s. 83.

zarządzanie zamówieniami, przeładunki na terminalu kontenerowym, pakowanie, kompletacja); **pomocnicze** (spedycja, obsługa celna, ubezpieczenia, systemowy obrót zbiorczymi opakowaniami transportowymi wielokrotnego użytku, wynajem kontenerów, palet i innych opakowań transportowych, usługi informacyjne i informatyczne, promocja i marketing); **dodatkowe** (techniczna obsługa pojazdów, sprzedaż paliw, olejów i akcesoriów, naprawa kontenerów i innych opakowań transportowych, usługi hotelarskie, usługi gastronomiczne, usługi bankowe, usługi księgowo-rachunkowe, usługi telekomunikacyjne, usługi parkingowe).

Z usług centrów logistycznych niejednokrotnie korzystają przedsiębiorstwa produkcyjne, gdzie dokonują się procesy związane z zaopatrzeniem, montażem i dystrybucją. W takim przypadku do funkcji realizowanych przez centra możemy zliczyć sferę¹⁷⁷: **zaopatrzenia** (przyjmowanie i magazynowanie towarów przeznaczonych dla celów produkcji, konsolidacja dostaw zaopatrzeniowych dla celów produkcji, kompletacja zestawów montażowych, dostarczanie towarów do przedsiębiorstw produkcyjnych, w tym sekwencyjne dostawy na linii produkcyjne); **produkcji – podmontaż** (np. zgrzewanie i spawanie blach karoseryjnych) i **montaż** zespołów z dala od podstawowej wytwórni; **specjalistycznej obsługi** wymagającej przestrzegania np. unijnych wymogów HACCP w zakresie transportu (chłodnie samochodowe), przechowywania (temperatura, wilgotność), dystrybucji żywności; koordynacji działań między sferą produkcji a sferą usług – konfekcjonowanie produktów, co-manufacturing¹⁷⁸; **dystrybucji** – montaż końcowy, pakowanie, dostarczanie.

Istotną sferą dla funkcjonowania magazynu jest jego bezpieczeństwo, które na gruncie analizy systemowej możemy traktować jako¹⁷⁹:

- własność magazynu charakteryzującą jego odporność na powstanie sytuacji niebezpiecznych (zagrożeń), przy czym uwaga koncentruje się na zawodności bezpieczeństwa magazynu, czyli jego podatności na powstanie sytuacji niebezpiecznych;
- zdolność do ochrony zapasów i infrastruktury magazynowej przed zewnętrznymi zagrożeniami.

Zagrożenia bezpieczeństwa magazynu możemy podzielić na: związane z postępowaniem człowieka (złe intencje – podpalenia, kradzieże zdeponowanych zapasów, niezadowoleni pracownicy, terroryści, konkurencja, kradzież informacji o dostawcach i odbiorcach oraz bez złych intencji – wypadki spowodowane ignorancją i nieodpowiedzialnością), niezwiązane z postępowaniem człowieka (katastrofa budowlana, awarie: klimatyzacji, transportu

¹⁷⁷ Tamże, s. 84.

¹⁷⁸ Co-manufacturing polega na montażu towarów z części przesyłanych od różnych producentów dokładnie na konkretne zamówienia klienta.

¹⁷⁹ Por. P. Sienkiewicz, *Teoria i inżynieria systemów*, [w:] Inżynieria systemów bezpieczeństwa, PWE, Warszawa 2015, s. 9.

wewnętrznego, regałów, zasilania, systemu informatycznego), katastrofy naturalne (powódzie, huragany, trzęsienia ziemi)¹⁸⁰.

Bezpieczeństwo w magazynie jest zależne od trzech grup czynników, tj. technicznych, prawnych oraz personalnych – tabela 3.13.

Tabela 3.13

Czynniki decydujące o bezpieczeństwie w magazynie

| Czynnik | Treść |
|------------------------|--|
| Techniczny | Wyposażenie i infrastruktura magazynu |
| Prawny (organizacyjny) | Dokumentacja i jej wdrożenie oraz procedury, minimalizują ryzyko dojścia do wypadku czy strat materialnych |
| Personel | Kompetencje, kwalifikacje oraz doświadczenie, doskonalenie zawodowe personelu |

Źródło: opracowanie własne.

Czynniki techniczne wpływające na bezpieczeństwo w magazynach są związane z odpowiednim wyposażeniem i infrastrukturą, która zapewnia właściwe magazynowanie, transport wewnętrzny, kompletację zamówień, sortowanie, ekspedycję oraz właściwą ochronę obiektu. To od infrastruktury również zależy bezpieczeństwo osób pracujących w magazynie oraz zasobów materialnych tam zdeponowanych.

Do infrastruktury zaliczamy: budynki administracyjne (np. biuro zarządzania i administracji); budynki i budowle magazynowe, umożliwiające składowanie i ochronę zapasów; wyposażenie magazynów (regały, środki służące do manipulacji wyrobami, urządzenia pomiarowo-kontrolne, urządzenia przeciwpożarowe i inne); środki transportu, służące przemieszczaniu produktów zarówno wewnątrz przedsiębiorstwa, jak i pomiędzy dostawcami i odbiorcami; urządzenia do załadunku i wyładunku; drogi wewnętrzne i drogi dojazdowe, głównie dla samochodów, ale także dla wagonów; opakowania, spełniające funkcje ochronne, magazynowe, transportowe, manipulacyjne, informacyjne i reklamowe; jednostki ładunkowe do wielokrotnego użytku, takie jak palety czy kontenery; budynki i biura związane z realizacją funkcji pomocniczych i dodatkowych (np. stacja obsługi, stacja paliw, pomieszczenia socjalno-bytowe, obsługa bankowa, ubezpieczenia); urządzenia i środki związane z bezpieczeństwem, takie jak np. instalacja tryskaczowa ESFR¹⁸¹, otwory wentylacyjne, wyjścia awaryjne, zasilanie awaryjne – akumulatornia, wykrywacze ognia i dymu, całodobowa ochrona – monitoring poprzez wykorzystanie systemów

¹⁸⁰ Tamże, s. 10.

¹⁸¹ Tryskacz ESFR (*Early Suppression Fast Response*) – szybkie reagowanie i wczesne gaszenie.

sygnalizacji włamań i napadu, systemu nadzoru wizyjnego, systemu sygnalizacji pożaru.

W dobie informatyki i elektroniki nie sposób pominąć w wyposażeniu tego, co wspomaga monitorowanie i kontrolowanie w trybie on-line zgromadzonych zapasów pod względem ilości, wartości, rodzajów, terminów ważności. Do pomocnych narzędzi i instrumentów w tym zakresie zaliczamy: **światłne sygnalizatory pobrań**; **RFID** (*Radio-frequency identification*) – technika, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu stanowiącego etykietę obiektu przez czytnik, w celu identyfikacji obiektu; **systemy głosowe** – użycie technologii głosowych zapewnia łatwy, dwukierunkowy sposób komunikacji między systemem informatycznym, np. WMS¹⁸² a jego użytkownikiem, np. pracownikiem magazynu; **czytniki kodów kreskowych**, popularnie nazywanych skanerami – urządzenia, które zamieniają światło odbite od kodu kreskowego na sygnał elektroniczny, zrozumiały dla kasy lub komputera; **terminale RF** – bezprzewodowa wymiana informacji drogą radiową on-line, terminale takie są często wyposażone w skaner kodów kreskowych; **komputery montowane w pojazdach** oraz **przenośne komputery** – mają przewagę nad urządzeniami podręcznymi (większy ekran, większa klawiatura), są wyposażone w przyjazny dla użytkownika interfejs GUI¹⁸³ (generalnie urządzenia montowane na pojazdach korzystają z zewnętrznego przewodowego lub bezprzewodowego czytnika kodów kreskowych w celu przetwarzania danych).

W całodobowej ochronie współcześnie najczęściej wykorzystuje się systemy telewizji dozorowej CCTV (*Closed Circuit TeleVision*). Jest to zespół środków technicznych i programowych przeznaczonych do obserwacji, wykrywania, rejestrowania oraz sygnalizowania warunków wskazujących na istnienie niebezpieczeństwa powstania szkód lub zagrożeń osób i mienia. Telewizja CCTV może stanowić wydzielony system dozorowy lub może też wchodzić przykładowo w skład większych systemów sygnalizacji włamania i napadu – SSWiN lub systemów kontroli dostępu – SKD.

Do czynników technicznych wpływających na bezpieczeństwo magazynu należą również zabezpieczenie mechaniczne, którymi są wszelkiego rodzaju stałe przegrody (konstrukcje, ściany, bramy, drzwi ppoż., antywłamaniowe), a ich zadaniem jest dodatkowo ochrona szczególnie ważnych (cennych lub niebezpiecznych) zapasów tam zgromadzonych.

¹⁸² WMS, *Warehouse Management System* – system informatyczny wspomagający zarządzanie procesami magazynowymi, nadzorujący racjonalne rozmieszczenie zapasów, wykorzystujący techniki automatycznej identyfikacji.

¹⁸³ GUI graficzny interfejs użytkownika (*Graphical User Interface*), często nazywany też *środowiskiem graficznym* – ogólne określenie sposobu prezentacji informacji przez komputer oraz interakcji z użytkownikiem, polegające na rysowaniu i obsłudze podstawowych elementów, np. okno, pole edycji, suwak, przycisk.

Do czynników **prawnych** (organizacyjnych) zaliczamy opracowanie dokumentacji i jej wdrożenie oraz opracowanie procedur, których bezwzględne przestrzeganie minimalizuje ryzyko dojścia do wypadku czy strat materialnych.

Niezwykle ważne w czasie opracowywania dokumentacji jest uwzględnienie, co będzie w magazynie (rodzaj środka zaopatrzenia, zapasu) i jakie są przepisy oraz unormowania prawne precyzujące warunki przechowywania zgromadzonych zasobów. Do dokumentacji zaliczamy: zakres obowiązków magazyniera; instrukcję przeciwpożarową dla magazynu; instrukcję bezpieczeństwa i higieny pracy; kartę informacyjną magazynu; instrukcję o utrzymaniu magazynu; instrukcję o obsłudze przyrządów do pomiaru wilgotności i temperatury; instrukcję o wietrzeniu magazynów; instrukcję o stosowaniu sygnałów alarmowych i ich rodzajach; plan ewakuacji mienia przechowywanego w magazynie; skład grupy awaryjno-ratunkowej (siły i środki do ewakuacji mienia); wykaz ilościowy wyposażenia magazynu (dotyczy wyposażenia trwałego); schemat rozmieszczenia sprzętu w magazynie (plan składowania); metrykę magazynu z aktualnymi danymi; instrukcję postępowania w przypadku rozlania substancji niebezpiecznej; regulamin pracy magazynu; imienny wykaz osób uprawnionych do zatwierdzania dokumentów obrotu materiałowego; zapis temperatury i wilgotności (również w formie elektronicznej); wzory plomb; książkę ewidencji osób wchodzących do obiektu magazynowego; książkę przeglądów kontrolnych magazynu; książkę ewidencji mienia przekazanego do naprawy (konserwacji); książkę depozytów; inne (wg potrzeb).

Nie bez znaczenia dla funkcjonowania magazynu mają odpowiednie procedury, które zapewniają funkcjonowanie magazynu poprzez skuteczne i sprawne zapobieganie powstawaniu zagrożeń oraz reagowanie na występujące zagrożenia, tzn. podejmowanie takich działań, które minimalizują ich niekorzystne efekty (skutki).

Do typowych procedur organizacyjnych związanych z funkcjonowaniem magazynu zalicza się¹⁸⁴: techniczne warunki eksploatacji magazynu i jego urządzeń, ochronę przeciwpożarową, ochronę przed włamaniami, bezpieczeństwo pracy personelu, przyjęcie i wydawanie dóbr materialnych, inwentaryzacja stanu zapasów, rozmieszczenie zapasów w magazynie, ewidencję magazynową, dokumenty przyjęć i wydań towarów, inne czynności informacyjne.

Procedury powinny minimalizować ryzyko dojścia do wypadku w magazynie, gdzie przyczynami mogą być: problemy z prawidłową obsługą podnośników w czasie pracy; brawura i nieodpowiedzialne zachowanie pracowników; pośpiech – presja czasu; zła organizacja pracy – nieprzestrzeganie regulaminu pracy; brak ostrożności – zdarzenia wywołane nieodpowiednim zachowaniem innych pracowników oraz użytkowników dróg komunikacyjnych,

¹⁸⁴ Por. Cz. Skowronek, Z. Sarjusz-Wolski, *Logistyka w przedsiębiorstwie*, PWE, Warszawa 2008, s. 141.

niewygodna pozycja operatora wózka widłowego lub nadmierny wysiłek – niewłaściwa ergonomia wpływająca na zmęczenie lub sterowanie.

Realizowane procedury, dotyczące procesów logistycznych w magazynach wielkopowierzchniowych, są wspierane informatycznie przez magazynowy system informatyczny WMS, który realizuje zadania¹⁸⁵: rejestracji przyjęć towarów z dostaw zewnętrznych i zwrotów własnych do magazynu oraz wydań towarów z magazynu; aktualizacji i zarządzania stanami magazynowymi wg założonych kryteriów; wskazywania miejsc składowania dostaw, lokalizacji zapasów i kompletacji wydań; generowania dokumentów dostawy i wydania; generowania zamówień; kontroli zgodności dostawy/wydania z dokumentami; kontroli załadunku środków transportu zewnętrznego; kontroli przebiegu obrotu magazynowego; identyfikacji i lokalizacji towarów; inwentaryzacji stanów magazynowych; doboru środków transportu dla realizacji wysyłek. Przykładem systemu obsługującego wszystkie aspekty logistyki magazynowej jest softwarowy pakiet firmy Swisslog – załącznik 3.2¹⁸⁶.

Nie bez znaczenia, dla bezpieczeństwa magazynu, są opracowane procedury regulujące odpowiedzialność materialną pracowników za powierzone mienie. Podstawy prawne dotyczące odpowiedzialności są zawarte w kodeksie pracy i trzech rozporządzeniach – załącznik 3.3.

W kodeksie pracy, zgodnie z art. 124:

- paragraf 1 – „pracownik, któremu powierzono z obowiązkiem zwrotu albo do wyliczenia się: 1) pieniądze, papiery wartościowe lub kosztowności, 2) narzędzia i instrumenty lub podobne przedmioty, a także środki ochrony indywidualnej oraz odzież i obuwie robocze, odpowiada w pełnej wysokości za szkodę powstałą w tym mieniu;
- paragraf 2 – „pracownik odpowiada w pełnej wysokości również za szkodę w mieniu innym niż wymienione w § 1, powierzonym mu z obowiązkiem zwrotu albo do wyliczenia się”.

Pracownik może uwolnić się od odpowiedzialności za szkody w powierzonym mieniu, jeżeli wykaże, że szkoda powstała z przyczyn niezależnych od niego.

W ramach odpowiedzialności majątkowej możemy wyodrębnić odpowiedzialność majątkową jednostkową i wspólną.

Poza przepisami prawnymi należy także zwracać uwagę, aby magazynierzy, którzy ponoszą odpowiedzialność majątkową za powierzone mienie posiadali odpowiednie wykształcenie, kwalifikacje zawodowe i moralne oraz określony staż pracy. Osoby powoływane na stanowisko magazyniera nie powinny mieć

¹⁸⁵ Instrukcja o zasadach i organizacji przechowywania oraz konserwacji uzbrojenia i sprzętu wojskowego DD/4.22.8, Inspektorat Wsparcia SZ RO, Bydgoszcz 2013, s. 30.

¹⁸⁶ A. Michalski, *Rola zautomatyzowanych centrów logistycznych w nowoczesnych procesach łańcucha dostaw*, <http://www.logistyka.net.pl>, 07.05.2014.

nałogów (pijaństwo, hazard) oraz nie powinny być sądownie karane za kradzieże, oszustwa i inne przestępstwa gospodarcze.

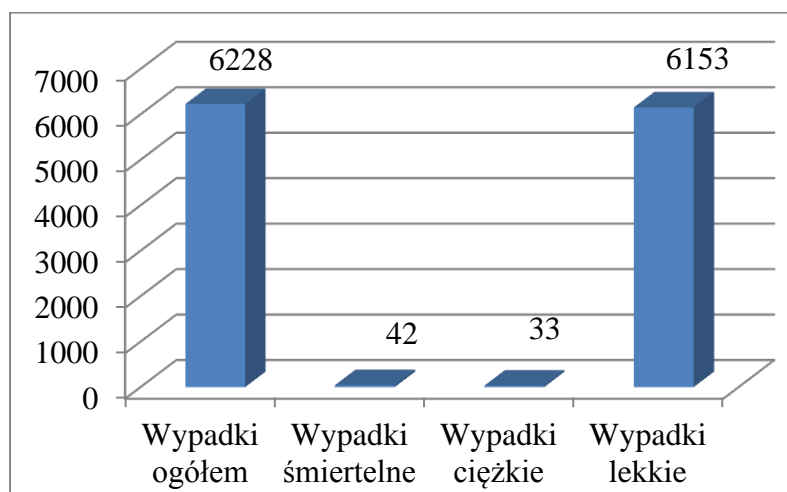
Dla bezpieczeństwa magazynów istotne są procedury zawarte w planach fizycznej ochrony magazynów. Optymalnym rozwiązaniem jest podpisanie umowy z profesjonalnymi firmami typu SUFO (Specjalistyczne Uzbrojone Formacje Ochrony) w zakresie ochrony osób i mienia, które mają obowiązek współpracy z Policją, Państwową Strażą Pożarną, Strażą Miejską. Pracownicy SUFO w ramach swej służby mają prawo do: legitymowania (w granicach chronionych obszarów) oraz ujęcia osób, stosowania siły fizycznej jako środka przymusu bezpośredniego, stosowania środków przymusu bezpośredniego, takich jak pałka, kajdanki, gaz obezwładniająco-paraliżujący, paralizator itp., użycia broni palnej.

Pracownicy tych firm prowadzą bieżącą kontrolę wejścia i wyjścia pracowników magazynu i osób postronnych oraz wjazdu i wyjazdu pojazdów samochodowych z terenu magazynu.

Niezwykle ważnym czynnikiem bezpieczeństwa w magazynie jest **personel** tam pracujący. Jest to zespół osób pracujących w magazynach i wykonujących czynności związane bezpośrednio z jego działalnością. Do stanowisk pracy w magazynach zgodnie z taryfikatorem kwalifikacyjnym należą: kierownik magazynu, starszy magazynier, magazynier, robotnik magazynowy. Ilość pracowników i ich kwalifikacje zależą od przeznaczenia i wielkości magazynu. Przy doborze pracowników należy mieć na uwadze: kompetencje, kwalifikacje oraz doświadczenie, a gdy są już zatrudnieni nie zapominać o doskonaleniu zawodowym personelu.

Wykres 3.8

Wypadki w 2014 r. w transporcie i gospodarce magazynowej
– zestawienie liczbowe

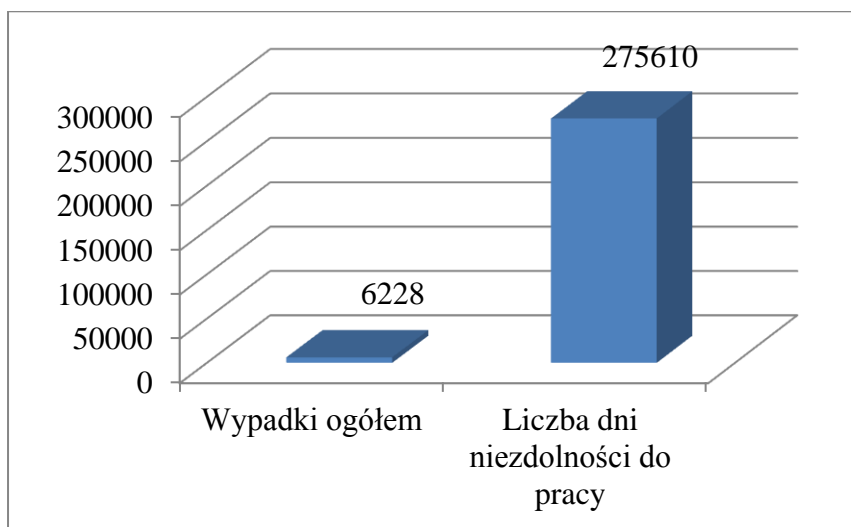


Źródło: *Wypadki przy pracy w 2014*, GUS, Warszawa 2015, s. 28.

Niezmiernie ważnym czynnikiem związanym z bezpieczeństwem jest przestrzeganie przepisów BHP przez personel magazynu i osób korzystających z niego (np. kierowcy, którzy dostarczają i zabierają ładunki logistyczne do i z magazynu). Dane liczbowe (wykresy 3.8 i 3.9), opracowane przez GUS w zakresie analizy wypadków, w transporcie i magazynowaniu, świadczą, że jest to istotny problem z punktu widzenia społecznego i gospodarczego.

Wykres 3.9

Wypadki w 2014 r. w transporcie i gospodarce magazynowej – liczba dni niezdolnych do pracy spowodowanych wypadkami ogółem



Źródło: *Wypadki przy pracy w 2014*, GUS, Warszawa 2015, s. 28.

Liczba wypadków w transporcie i gospodarce magazynowej wynosząca 6228 i liczba dni niezdolności do pracy 275610 świadczą o tym, że w BHP jest jeszcze dużo do zrobienia w obszarze organizacyjnym i proceduralnym.

Dla osób organizujących prace w magazynach i odpowiedzialnych za bezpieczeństwo pracowników magazynu (a nawet bezpieczeństwo osób trzecich) istotnym jest fakt, że nie ma oddzielnych przepisów dotyczących bezpośrednio bezpieczeństwa i higieny pracy przy magazynowaniu, składowaniu materiałów.

Sytuacja taka powoduje konieczność korzystania z wielu aktów prawnych jednocześnie, od ogólnych przepisów BHP poprzez przepisy branżowe do norm technicznych, a w wielu sytuacjach z zasad dobrej praktyki magazynowej. Wymagania ogólne dotyczące szeroko rozumianych prac transportowych i magazynowych określa rozdział 4 Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpie-

czeństwa i higieny pracy¹⁸⁷. Niezbędna jest także wiedza na temat identyfikacji zagrożeń i stosowania odpowiednich środków profilaktycznych i korygujących, ograniczających skutki zagrożeń. Wymagania prawne w zakresie budowy magazynowych, pomieszczeń, stosowanych urządzeń transportowych, zasad składowania i magazynowania różnego rodzaju materiałów określają liczne akty prawne oraz normy techniczne, w szczególności obejmujące zagadnienia bezpieczeństwa z obszarów¹⁸⁸: wymagania budowlane oraz BHP dla pomieszczeń magazynów, oświetlenie i ogrzewanie magazynów, wymagania dla dróg magazynowych, ogólne warunki bezpieczeństwa pożarowego, wyposażenie magazynu – zasady bezpiecznego składowania, zasady bezpieczeństwa dla magazynów otwartych i półotwartych, zasady BHP podczas transportu magazynowego, organizacja zmechanizowanych prac magazynowych, magazynowanie gazów technicznych, magazynowanie gazów płynnych w butlach, magazynowanie chemicznych materiałów niebezpiecznych.

Tabela 3.14

Požary magazynów w Polsce w latach 2000-2010

| Wyszczególnienie | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | Średnio |
|------------------|------|------|------|------|------|------|------|------|------|------|------|---------|
| Ogółem, w tym: | 1429 | 1116 | 1333 | 1461 | 1361 | 1258 | 1295 | 1286 | 1783 | 1197 | 1096 | 1329 |
| – małe | 1218 | 940 | 1141 | 1196 | 1142 | 1039 | 1097 | 1047 | 1127 | 978 | 904 | 1075 |
| – średnie | 167 | 142 | 159 | 213 | 170 | 178 | 169 | 165 | 196 | 176 | 149 | 171 |
| – duże | 37 | 29 | 22 | 38 | 35 | 28 | 29 | 38 | 42 | 29 | 34 | 33 |
| – b. duże | 7 | 5 | 11 | 14 | 14 | 13 | 8 | 16 | 18 | 14 | 9 | 12 |

Źródło: Biuletyny Informacyjne PSP z lat 2000-2010.

Ważnym czynnikiem wpływającym na bezpieczeństwo ludzi i zapasów zgromadzonych w magazynie jest właściwa organizacja przeciwpożarowa. To metodycznie, realistycznie opracowane instrukcje, zgromadzony, sprawny sprzęt poż., systematyczne szkolenia dają gwarancję poczucia bezpieczeństwa od następstw ewentualnych pożarów w magazynie.

¹⁸⁷ Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz. U. z 2003 r. Nr 169, poz. 1650, z późn. zm.).

¹⁸⁸ Zob. L. Zieliński, *BHP W MAGAZYNIE*, Wydawnictwo Wiedza i Praktyka Sp. z o.o., Warszawa 2015, s. 78.

Przyczynami pożarów mogą być: podpalenia przez niezadowolonego pracownika, konkurencję, nieprzestrzeganie podstawowych przepisów ppoż., niesprawna instalacja elektryczna, grzewcza, klimatyzacyjna, samozapłon, wylądowania atmosferyczne i inne. Liczbę pożarów i ich częstotliwość prezentują tabele 3.14 i 3.15.

Tabela 3.15

Częstość pożarów¹⁸⁹ dla magazynów handlowych (zamknięte i zadaszone) w Polsce w latach 2000-2009

| Częstość | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2009 | Średnio |
|----------------------------|-------|-------|--------|--------|--------|--------|--------|------|---------|
| Częstość pożarów magazynów | 0,043 | 0,033 | 0,0439 | 0,0465 | 0,0435 | 0,0389 | 0,0404 | 0,04 | 0,0295 |

Źródło: S. Wieteska, Pożary magazynów jako element zakłócenia funkcjonowania łańcuchów dostaw, [w:] Logistyka 2/2013, s. 166.

Zaprezentowany materiał dotyczący pożarów magazynów wskazuje na kilka istotnych aspektów: każdy pożar to niebezpieczeństwo dla ludzi i dóbr materialnych tam zgromadzonych, każdy pożar to straty i zakłócenie procesów realizowanych przez gospodarkę magazynową, w tym funkcjonowanie łańcuchów dostaw, średnio w Polsce mamy ok. 1300 pożarów magazynów w ciągu roku.

3.5. Zapewnienie bezpieczeństwa żywnościowego

Waga problemu związanego z bezpieczeństwem żywnościowym jest na tyle istotna, że zajmują się nim nie tylko przedsiębiorstwa związane z jej wytwarzaniem, dystrybucją, ale również najwyższe władze rządowe, a potwierdzeniem niech będzie zapis w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014: *Wzmacnianie bezpieczeństwa żywnościowego. Niezbędne jest wdrożenie polityki rolnej, która zwiększy odporność produkcji rolnej na niekorzystne zjawiska i utrzymanie kontroli nad ważnymi dla bezpieczeństwa państwa działami gospodarki żywnościowej oraz zagwarantuje właściwy poziom samowystarczalności żywnościowej*¹⁹⁰. Jest to argumentem, że bezpieczna żywność to zagadnienie wieloaspektowe i wielokryterialne.

¹⁸⁹ Przez częstość pożarów magazynów rozumiemy relację ilości pożarów magazynów do stanu ogółem zaewidencjonowanych magazynów w Polsce w danym roku.

¹⁹⁰ Zob. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2014*, pkt. 104 i 105.

Żywność wraz z opakowaniem, tak jak każdy produkt, powinna zaspokoić potrzeby producentów, logistyków oraz konsumentów poprzez spełnienie określonych cech: fizycznych (np. wymiary, ciężar ułatwiających transport i magazynowanie), chemicznych (np. skład surowców i ich wpływ na organizm, środowisko), technologicznych (np. łatwość w wytwarzaniu, przechowywaniu), organoleptycznych (np. przyjaznych w dotyku, w smaku, w węchu), funkcjonalnych (np. łatwość: otwarcia, przygotowania do spożycia, utylizacji, wygodnych w „śledzeniu”), ekonomicznych (cena, koszt przygotowania, utylizacji, transportu), estetycznych (np. kolor, kształty), bezpieczeństwa (np. szkodliwość, zdrowotność, łatwość monitorowania jakości produktu, ochronę przeciwko złodziejom, zniszczeniu).

Wszystkie zaprezentowane wymagania są ważne, ale na szczególną uwagę zasługują te, które mają wpływ na zdrowie i życie człowieka oraz dbałość o środowisko naturalne. Jak pokazuje rzeczywistość na rynku pojawiają się produkty, które nigdy nie powinny na nim się znaleźć. A oto przykłady.

Pierwszy. W 2012 roku w Czechach produkowano zatruty alkohol, który przez dystrybutorów został wprowadzony na ich rynek krajowy, słowacki i polski, w wyniku czego zmarło 38 osób, a wiele zostało zatrutych¹⁹¹.

Drugi. Pod Kaliszem podczas produkcji suszu jajecznego w dwóch firmach dochodziło do nieprawidłowości i zaniedbań. Przez wiele lat wytwarzany susz był wątpliwy pod względem jakości, jak i zawartych w nim zanieczyszczeń. Produkt zawierał między innymi metale ciężkie oraz bakterie z grupy Coli. Nieprawidłowości wykryto dopiero w 2012 roku, a susz był produkowany od 2008. Zabezpieczono około 26 ton suszu jajecznego, który był przeznaczony do sprzedaży ponad 100 producentów pasztetów, słodkości i makaronów w Polsce. W sprawie samego suszu pojawił się także wątek międzynarodowy. Prowadzi on do Czech i Holandii. Okazuje się, że jeden z podejrzanych w tej sprawie przedsiębiorców zaopatrywał się w towar u mieszkańca województwa łódzkiego, który z kolei sprowadzał mieszanki jajeczne z zagranicy¹⁹².

Trzeci. W Polsce, w roku 2012 wykryto nielegalny obrót solą spożywczą. Na rynek zamiast soli jadalnej była wprowadzana tzw. sól wypadowa, która swym wyglądem przypomina sól spożywczą. Skład chemiczny soli wypadowej może być bardzo niebezpieczny dla zdrowia człowieka, bowiem może zawierać potas lub azotan potasu, które mogą mieć wpływ na akcję serca, a nawet doprowadzić do jego zatrzymania. Jest ona odpadem technologicznym przy produkcji chlorku wapnia, który nadaje się do utrzymania dróg. Zamiast soli

¹⁹¹ Zob. *Biuletynu Wydziału Analiz Rządowego Centrum Bezpieczeństwa*, red. G. Świszcz, RCB, Warszawa 2013, s. 7, <http://rcb.gov.pl/>, 12.09.2014.

¹⁹² Por. A. Kurzyński, *Afera jajeczna: W suszu były bakterie. Zarzuty dla 11 osób*, <http://www.gloswielkopolski.pl/>, 24.07.2015.

spożywczej stosowano sól wypadową w 646 cukierniach, restauracjach, piekarniach, w tym także piekarniach w hipermarketach Tesco czy Auchan¹⁹³.

Zaprezentowane przykłady pozwalają stwierdzić, że *jeśli dokładnie będziemy znać skąd pochodzą surowce, kto je transportował, magazynował, gdzie były użyte do produkcji, kto dokonał dystrybucji, to zmniejszymy liczbę podrabianych, szkodliwych wyrobów dla zdrowia i życia, które będą docierały do klienta*. Warunkiem jest stworzenie odpowiedniego bezpiecznego systemu, na wszystkich etapach produkcji, przetwarzania i dystrybucji z możliwością szczegółowego identyfikowania dostawców oraz bezpośrednich klientów.

Bezpieczeństwo żywnościowe w wymogach prawnych i organizacyjnych

W Unii Europejskiej strategia bezpiecznej żywności opiera się na trzech filarach: prawo, doradztwo oparte o badania i praktyczne rozwiązania oraz kontrola i wdrażanie. Ustawodawstwo w zakresie bezpieczeństwa żywnościowego w UE ma charakter kompleksowy, dotyczy: higieny środków spożywczych, higieny w odniesieniu do żywności pochodzenia zwierzęcego, organizacji urzędowych kontroli w odniesieniu do produktów pochodzenia zwierzęcego przeznaczonych do spożycia przez ludzi, kontroli urzędowych przeprowadzanych w celu sprawdzenia zgodności z prawem paszowym i żywnościowym oraz regulami dotyczącymi zdrowia zwierząt i dobrostanu zwierząt. Wykaz ważniejszych aktów normatywno-prawnych przedstawia załącznik 3.4.

Zapewnienie bezpieczeństwa zdrowotnego żywności jest związane w wdrażaniem systemów zarządzania bezpieczeństwem zdrowotnym żywności, jakimi są m.in. zasady Dobrej Praktyki Higienicznej – GHP, Dobrej Praktyki Produkcyjnej – GMP oraz system HACCP. Jest to wymóg prawa określony m.in. w¹⁹⁴: Ustawie z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia, Rozporządzeniu Parlamentu Europejskiego i Rady Nr 178/2002 z dnia 28 stycznia 2002 r. ustalającego ogólne zasady i wymagania prawa żywnościowego, ustanawiające Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w sprawie bezpieczeństwa żywnościowego.

W świetle tego ostatniego rozporządzenia wszyscy operatorzy żywności bez względu na wielkość i profil prowadzonej działalności od dnia 1 stycznia 2006 r. mają obowiązek posiadać wdrożony i funkcjonujący system HACCP. Skrót HACCP (*Hazard Analysis and Critical Control Point System*) oznacza System Analizy Zagrożeń i Krytycznych Punktów Kontroli. HACCP jest narzędziem zarządzania bezpieczeństwem żywności i uniwersalną metodą systematycznej oceny możliwości wystąpienia zagrożeń oraz określenia metod ich eliminacji podczas produkcji żywności.

¹⁹³ Zob. Ł. Jachimowicz, *Fakty i szczegóły Głównego Inspektora Sanitarnego dotyczące działań Inspekcji Sanitarnej w sprawie fałszowania żywności solą przemysłową*, <http://gistest.pis.gov.pl/>, 25.07.2015.

¹⁹⁴ Por. HACCAP, <http://www.izz.waw.pl/>, 12.06.2015.

W praktyce funkcjonują dodatkowe standardy bezpieczeństwa żywnościowego między innymi takie jak: IFS (*International Food Standard*) – międzynarodowy standard bezpieczeństwa żywnościowego opracowany w 2002 roku przez przedstawicieli niemieckiego handlu detalicznego. W 2012 roku została wydana zaktualizowana wersja „IFS Food version 6”, która zaczęła obowiązywać od 1 lipca 2012 r. System IFS jest specyficznym standardem uznanym i opracowanym dla wszystkich producentów żywności, w głównej mierze na potrzeby sieci handlowych i ich marek własnych. Głównym celem tego systemu jest potwierdzenie bezpieczeństwa i jakości produktu oraz jego zgodności z obowiązującymi prawami i normami. IFS ujednolica wymagania i wprowadza przejrzystość w łańcuchu dostaw, od surowca po produkt końcowy¹⁹⁵.

BRC to międzynarodowy standard (*Global Standard*) opracowany przez Brytyjskie Konsorcjum Detalistów (*British Retail Consortium*) wymagany przez coraz większą grupę hiper- i supermarketów na terenie całej Europy. Standard opracowano, aby zapewnić jak najwyższą jakość dostarczanych produktów. Główne korzyści z wprowadzenia BRC to¹⁹⁶: zmniejszenie ilości produktów o niewłaściwej jakości; kontrola zarówno dostawcy jak i odbiorcy; zmniejszenie ilości audytów przeprowadzanych przez odbiorców; ujednolicenie wymagań z zakresu bezpieczeństwa żywności; dokumentacja potwierdzająca powtarzalność produktu o oczekiwanej jakości. W styczniu 2015 roku została opublikowana wersja 7 Standardu, która obowiązuje od 1 lipca 2015 roku.

Nie bez znaczenia dla zarządzania bezpieczeństwem i higieną żywności ma norma PN-EN ISO 22000: 2006, która wprowadza ujednoczony i globalnie zharmonizowany standard w zakresie bezpieczeństwa i higieny żywności, ułatwiając jednocześnie wdrożenie systemu HACCP oraz integrację z normą ISO 9001: 2008.

Norma 22000: 2006 jest możliwa do zastosowania przez wszystkie organizacje bezpośrednio lub pośrednio uczestniczące w łańcuchu żywnościowym, tj. producentów żywności, pasz, zbóż, dodatków do żywności, rolników, firmy świadczących usługi żywieniowe i cateringowe, sprzedawców detalicznych i hurtowych, firmy świadczące usługi porządkowe, transportowe i dystrybucyjne, dostawców wyposażenia, środków do mycia i higieny, materiałów opakowaniowych oraz innych materiałów kontaktujących się z żywnością.

¹⁹⁵ Por. IFS, <http://www.suedzucker.pl/pl/>, 12.06.2015, IFS – Lista wymagań audytowych, Hamilton Poland LTD, Rzeczoznawstwo i badania Laboratoryjne, materiały szkoleniowe, Toruń 2012.

¹⁹⁶ Zob. *Globalna norma bezpieczeństwa żywności*, BRC Global Standard, British Retail Consortium, London, 2015.

Zarządzanie bezpieczeństwem i jakością żywności, wg systemu zgodnie z normą ISO 22000, zawiera specyficzne wymagania dla zapewnienia bezpieczeństwa żywności, a dotyczące¹⁹⁷: *komunikacji w łańcuchu dostaw* – wewnętrznej oraz z dostawcami i klientami, aby zapewnić identyfikację i nadzorowanie zagrożeń bezpieczeństwa; *zarządzania systemem jakości* – stosowany i aktualizowany system powinien być włączony do ogółu działań związanych z zarządzaniem firmą; *monitorowania operacyjnych programów wstępnych* – planów zarządzania materiałami (np. surowcami, środkami chemicznymi), środków zapobiegających zakażeniom krzyżowym, kontroli szkodników, higieny personelu, dostawy mediów, usuwania odpadów; *weryfikacji zasad HACCP* – z naciskiem na analizę i monitorowanie środków nadzoru zagrożeń, jako klucza do skuteczności funkcjonowania systemu.

Dodatkowo dla potrzeb logistyki zostały opracowane standardy¹⁹⁸:

IFS Logistics – standardem dla firm, które mają kontakt fizyczny z produktami żywnościowymi w opakowaniach (transport, konfekcjonowanie produktów żywnościowych opakowanych, załadunek, wyładunek, przechowywanie, dystrybucja, składowanie palet). Standard ten dotyczy transportu drogowego, kolejowego, morskiego oraz procesów mrożenia, chłodzenia.

BRC Global Standard Storage and Distribution jest standardem w obszarze magazynowania i dystrybucji. Dotyczy on procesów logistycznych realizowanych w łańcuchach dostaw, do których zaliczamy: magazynowanie, dystrybucje, transport, usługi kontraktowe, pakowanie, chłodzenie, zamrażanie, odmrażanie.

*BRC/IoP*¹⁹⁹ *Packaging and Packaging Materials* – zawiera wymagania dotyczące higieny, otoczenia produkcji oraz badań opakowań. W standardzie zawarte są wymagania nie tylko dla materiałów do opakowań żywności, ale także dla wszystkich producentów opakowań (m.in. w sektorach: szkła, plastiku, drewna, papieru, aluminium, stali). Standard określa dwa poziomy ryzyka higieny, które są uzależnione od końcowego przeznaczenia materiału opakowaniowego. Opakowania przeznaczone dla przechowywania żywności będą miały najwyższy poziom ryzyka, a te „nieżywnościowe” – najniższy.

IFS Broker – zapewnia standard dotyczący jakości i bezpieczeństwa produktów na etapie ich skupu, przechowywania i odsprzedaży przez importerów, brokerów oraz agencji handlowych. Zatem jest stosowany przez agencje handlowe, importerów, brokerów lub inne podmioty, które zajmują się pośrednictwem w sprzedaży produktów żywnościowych.

¹⁹⁷ Zob. A. Kielesinska, *Aspekty prawne bezpieczeństwa żywności w logistyce*, [w:] *Logistyka* 6/2014, s. 13454.

¹⁹⁸ Zob. *Systemy zarządzania – Bezpieczeństwem żywności*, Dekra, <http://www.dekra-certification.com.pl/>, 11.11.2015.

¹⁹⁹ IoP (*Institute of Packaging*) – Instytut Opakowań.

Korzyści z certyfikacji systemu zarządzania bezpieczeństwem żywności to²⁰⁰: potwierdzenie przestrzegania wymagań prawnych oraz stosowania standardów higienicznych i bezpieczeństwa żywności, w tym zasad HACCP, zwiększony poziom bezpieczeństwa wprowadzanych do obrotu produktów żywnościowych, wzrost zaufania konsumentów do organizacji, ułatwienie współpracy z partnerami w łańcuchu dostaw.

Realizacja zawarta w aktach normatywno-prawnych i innych standardach oraz normach nie byłaby możliwa bez: system wczesnego ostrzegania dla powiadamiania o bezpośrednim lub pośrednim niebezpieczeństwie grożącym zdrowiu ludzkiemu, pochodzącym z żywności lub pokarmu; ocena ryzyka (oznacza proces wsparty naukowo, składający się z czterech etapów: identyfikacji zagrożenia, charakterystyki niebezpieczeństwa, oceny oraz charakterystyki ryzyka) i zarządzania nim; zarządzania kryzysem wywołanym zagrożeniami, które definiuje się jako czynnik biologiczny, chemiczny lub fizyczny w żywności lub paszy, bądź stan żywności lub paszy, mogący powodować negatywne skutki dla zdrowia.

Bezpieczeństwo żywnościowe w praktyce

Przeprowadzone wywiady z ekspertami odpowiedzialnymi za produkcję żywności nasuwają niepodważalną maksymę, że dzisiaj produkt do spożycia bezpośredniego lub pośredniego ma być smaczny, odpowiednio zbilansowany, najwyższej jakości i świeżości. Osiągnięcie zaprezentowanych parametrów jest niezwykle trudne, jak stwierdzili eksperci, ze względu na²⁰¹: ciągle zmiany w zapatrywaniu, produkcji, dystrybucji wywołane nowymi technikami, technologiami, rolnictwem intensywnym (duże zyski, zastosowanie wydajnych maszyn, wykorzystywanie środków chemicznych, nawozów, środków owadobójczych itd.); funkcjonowanie, z tendencją rosnącą super i hipermarketów, firm zbiorowego żywienia oraz punktów ulicznych sprzedających żywność (posiłki); zmiany środowiskowe – jego funkcjonowanie jest narażone na skażenie (celowe lub nie), wywołane najczęściej czynnikami cywilizacyjnymi; wydłużone łańcuchy dostaw, wynikające z pozyskiwania tanich surowców u globalnych dostawców oraz poszukiwania odległych rynków zbytu; działania konkurencji i to czasami w sposób nietyczny.

Wszystko to sprzyja zwiększającemu prawdopodobieństwu rozprzestrzeniania się żywności o złej jakości, czasami skażonej, niejednokrotnie zagrażającej zdrowiu i życiu człowieka, a także negatywnie wpływającej na środowisko naturalne.

W celu zapewnienia najwyższego poziomu bezpieczeństwa żywnościowego, w badanych firmach był wdrożony system HACCP oraz system IFS.

²⁰⁰ Zob. PN-EN ISO 22000 – System zarządzania bezpieczeństwem żywności (HACCP), Urząd Dozoru Technicznego, <http://www.udt.gov.pl/>, 08.11.2015.

²⁰¹ Por. A. Szymonik, *Bezpieczeństwo żywnościowe*, [w:] Logistyce 2015/5, s. 1543.

To one pozwoliły opracować szereg instrukcji i procedur, które zapewniają, że produkowana żywność jest bezpieczna i przyjazna dla człowieka oraz środowiska. Główny cel spełniania wymagań wymienionych norm to: zaangażować wyższe kierownictwo w odpowiedzialność za bezpieczeństwo i jakość żywności; podniesienie świadomości i umiejętności pracowników, w zakresie wymagań jakie powinien spełniać produkt; uporządkowanie kompetencji i obowiązków osób odpowiedzialnych za produkcję żywności lub realizację żywienia.

W obszarze procesów logistycznych istotnych jest kilka zagadnień, które należy brać pod uwagę, zdaniem ekspertów, by przemieszczany strumień rzeczowy, począwszy od surowców, poprzez produkcje i dystrybucję żywności, był monitorowany i zarządzany właściwie, a tym samym bezpieczny. A oto niektóre z nich.

Pierwszy. Procedury wyboru dostawców powinny być opracowane, zatwierdzone. Zakupione materiały i usługi, które mają wpływ na bezpieczeństwo i jakość żywności powinny być monitorowane, sprawdzane, a użyte do tego mierniki powinny posiadać jasne kryteria oceny. Oceny dostawców powinny być systematycznie analizowane w kontekście zagrożeń i rodzajów ryzyka.

W czasie realizacji procesów magazynowych szczególną uwagę należy zwrócić na: zgodność przyjmowanych towarów, w tym opakowań i etykiet, ze specyfikacją, warunki przechowywania surowców, półproduktów, produktów gotowych, które powinny odpowiadać odpowiednim wymaganiom i nie doprowadzić do zanieczyszczenia krzyżowego; aktualność oznakowań, ułatwiających właściwą gospodarkę (pierwsze weszło, pierwsze wyszło – FIFO lub pierwsze traci ważność, pierwsze wychodzi FEFO).

Drugi. Na podstawie analizy zagrożeń i rodzajów ryzyka oraz przeznaczenia wyrobów, firma musi posiadać specyfikację na materiały opakowaniowe. Muszą one być: zgodne z wymogami, ustawionymi w normach i ustawodawstwie; przydatne dla każdego produktu (np. organoleptyczne, przechowalnicze, bezpieczne dla produktu, człowieka i środowiska); sprzyjać procesowi *traceability*²⁰²; dobrze, czytelnie, zgodnie z wymogami, nieusuwalnie oznakowane; podlegać systematycznej, udokumentowanej kontroli.

Trzeci. Niezmiernie ważnymi ogniwami w zapewnieniu bezpieczeństwa żywności są: odpowiednio realizowane konserwacje i naprawy, które nie mogą wpłynąć negatywnie na produkt; odpowiednio zaprojektowane, przygotowane, eksploatowane zaplecze socjalne; specjalne szatnie dla personelu, kontrahentów, osób odwiedzających; umywalnie, ubikacje w pełni zabezpieczające higienę (np. bezdotykowe elementy wyposażenia, dezynfekcja rąk, odpowiednie

²⁰² Szerzej w podrozdziale 5.5.

wyposażenie do utrzymania higieny, oznakowanie wyjaśniające wymagania dotyczące mycia rąk, pojemnik otwierany bez użycia rąk).

Czwarty. Wiele uwagi w firmach produkujących żywność przywiązuje się do obrony żywności i kontroli zewnętrznych. Do czynności realizowanych w ramach tego przedsięwzięcia należy: wyznaczenie osób, które są odpowiedzialne za obronę żywności²⁰³; systematycznie analizować zagrożenia i rodzaje ryzyka z nimi związane; posiadać opracowane procedury, które są systematycznie sprawdzane i testowane w praktyce (np. podczas szkoleń czy dodatkowych treningów); zabezpieczenie całej firmy przed nieautoryzowanym dostępem.

Zostały zaprezentowane tylko niektóre obszary, które mają wpływ na bezpieczeństwo żywności. Zdaniem ekspertów, najlepsze procedury, instrukcje, nowoczesne techniki i technologie zdadzą się na nic, gdy zawiedzie człowiek.

²⁰³ Obrona żywności koncentruje się na ochronie zasobów żywności przed umyślnym skażeniem różnymi substancjami chemicznymi, biologicznymi lub innymi substancjami szkodliwymi przez ludzi, którzy chcą zaszkodzić zakładowi lub populacji. Środki celowo zanieczyszczające produkt mogą zawierać związki, które naturalnie nie występują w żywności lub nie są badane z przeznaczeniem do kontaktu z żywnością. Celem atakującego może być zaszkodzenie producentowi żywności, niszczenie gospodarki danego kraju lub zabijanie ludzi. Zamierzone działania nie są zazwyczaj racjonalne i są trudne do przewidzenia, [w:] K. Godlewska, *Forum Mleczarskie Biznes* 2/2014 (18), <http://www.forummleczarskie.pl/>, 20.07.2015.

4. EKOLOGISTYKA W SYSTEMIE BEZPIECZEŃSTWA ŚRODOWISKA NATURALNEGO

Środowisko naturalne, wraz z takimi sektorami jak finansowy, energetyczny, transportowy, infrastruktury (w tym krytycznej), ma wpływ na bezpieczeństwo gospodarcze. O randze i wadze problemu mogą świadczyć zapisy w ustawach i ważnych dokumentach krajowych i UE. Z nich wynika, że środowisko naturalne systematycznie i w sposób nieprzerwalny jest zanieczyszczane i niszczone przez przemysł, transport, rolnictwo, gospodarkę komunalną. Zapobiec temu może stworzony zintegrowany system bezpieczeństwa środowiska naturalnego, którego celem jest zabezpieczenie środowiska naturalnego przed oddziaływaniem zjawisk (procesów, zdarzeń) i ich negatywnych konsekwencji (skutków, szkód). Pomocna w tych działaniach jest ekologistyka, która występuje pod różnymi nazwami (logistyka zwrotna, logistyka odwrotna, logistyka odpadów, logistyka powtórnego zagospodarowania).

4.1. System bezpieczeństwa środowiska naturalnego

Każdej działalności ludzkiej towarzyszy powstawanie odpadów. Początkowo ludzie w sposób naturalny wyczuwali, i sami podejmowali decyzje, jak postępować z odpadami. Jednak z upływem czasu, kiedy odpadów przybywało, nie można już było tego problemu zostawić pojedynczemu człowiekowi, o czym świadczy np. fakt, że w 1900 r. w Nowym Jorku 100 tys. koni potrzebnych do obsługi miasta produkowało 2,5 mln funtów odchodów dziennie, zalegających w hałdach sięgających okien pierwszego piętra. Pierwsza światowa konferencja na temat planowania miejskiego zakończyła się przed czasem, bo zgromadzeni mędrcy nie potrafili rozwiązać końskiego problemu, a wszelkie prognozy wieszczyły ponurą przyszłość: Londyn w połowie XX w. miała pokrywać ponad dwumetrowa warstwa łajna²⁰⁴.

Pomimo że od wspomnianych zdarzeń minęło ponad 100 lat, to społeczeństwo nie uwolniło się od podobnych problemów. Przykładem mogą być opakowania i odpady. I tak np. średnio w krajach Europy Zachodniej, USA oraz Japonii zużycie opakowań na 1 mieszkańca waha się w granicach 300-340 EUR, w Polsce ok. 200 EUR²⁰⁵. Przeciętny Polak w ciągu roku

²⁰⁴ Por. E. Bendyk, *Moloch miejski*, [w:] Cywilizacja 2.0 Świat po rewolucji informacyjnej, wydanie specjalne, 8.2011, s. 48.

²⁰⁵ Por. W. Wasiak, *Przemysł i rynek opakowań*, [w:] Kierunki rozwoju opakowań, red. nauk. W. Wasiak, Polska Izba Opakowań, Warszawa 2014, s. 33.

produkuje 250-300 kg śmieci. Francuzi i Włosi wytwarzają ich 300-330 kg na głowę, Amerykanie – 864 kg, a Japończycy – aż 1000 kg. Są to liczby, które pokazują skalę problemu związanego z ochroną środowiska²⁰⁶.

Aktualnie degradacja środowiska w głównej mierze jest powodowana poprzez²⁰⁷: wzrost i koncentrację liczby ludności, mające wpływ na globalną masę produktów i usług niezbędnych do zaspokojenia ich potrzeb; wzrost poziomu konsumpcji będący następstwem zróżnicowania i wzrostu wymagań życiowych, determinujący różnorodność produktów i powstających odpadów; rozwój technologiczny mający wpływ na: wielkość zużycia energii, masę produktów, ich różnorodność i termin ich ważności; wzrost zagrożeń związanych (niezwiązanych) z postępowaniem człowieka oraz katastrof naturalnych. Należy pamiętać, że cywilizacja z jednej strony łagodzi skutki zagrożeń naturalnych i powodowanych przez dotychczasowe rozwiązania zwiększające wygodę życia, lecz z drugiej strony – generuje nowe rodzaje zagrożeń.

Środowisko naturalne, wraz z takimi sektorami, jak finansowy, energetyczny, transportowy, infrastruktury (w tym krytycznej), decyduje i ma wpływ na bezpieczeństwo gospodarcze, które jest jedną z czterech podstawowych dziedzin bezpieczeństwa narodowego. O randze i wadze problemu mogą świadczyć zapisy:

– w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. – art. 74:

1. *Władze publiczne prowadzą politykę zapewniającą bezpieczeństwo ekologiczne²⁰⁸ współczesnemu i przyszłym pokoleniom.*

2. *Ochrona środowiska²⁰⁹ jest obowiązkiem władz publicznych.*

3. *Każdy ma prawo do informacji o stanie i ochronie środowiska.*

4. *Władze publiczne wspierają działania obywateli na rzecz ochrony i poprawy stanu środowiska.*

– w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014 roku – pkt. 105:

Ochrona środowiska naturalnego. Działania zwiększające bezpieczeństwo ekologiczne będą się koncentrowały na poprawie stanu środowiska, zachowaniu

²⁰⁶ Zob. K. Nadolski, *Globalne wysypisko*, <http://technowinki.onet.pl/>, 15.11.2015.

²⁰⁷ Por. R. Zarzycki, M. Imbierowicz, M. Stelmachowski, *Wprowadzenie do inżynierii ochrony środowiska. Ochrona środowiska naturalnego*, WNT, Warszawa 2007, s. 375.

²⁰⁸ Bezpieczeństwo ekologiczne to zdolność do ochrony wewnętrznych wartości przed zagrożeniami lub stan przeciwdziałania społecznego skutkom przekształceń otaczającego środowiska.

²⁰⁹ Ochrona środowiska – rozumie się przez to podjęcie lub zaniechanie działań, umożliwiające zachowanie lub przywracanie równowagi przyrodniczej; ochrona ta polega w szczególności na: a) racjonalnym kształtowaniu środowiska i gospodarowaniu zasobami środowiska zgodnie z zasadą zrównoważonego rozwoju, b) przeciwdziałaniu zanieczyszczeniom, c) przywracaniu elementów przyrodniczych do stanu właściwego, wg Ustawy Prawo Ochrony Środowiska z dnia 27 kwietnia 2001 r., art. 3.

różnorodności biologicznej oraz adaptacji do zmian klimatu, w szczególności poprzez uwzględnienie konieczności zapewnienia odpowiedniego poziomu inwestycji w źródła niskoemisyjne. W ramach ochrony środowiska kontynuowane będą działania na rzecz poprawy czystości powietrza, wód, gleb oraz właściwej gospodarki odpadami. Adaptacja do zmieniających się uwarunkowań klimatycznych i hydrologicznych wymaga wdrożenia nowych rozwiązań systemowych, ukierunkowanych między innymi na minimalizowanie skutków klęsk żywiołowych i ekstremalnych zjawisk pogodowych. Szczególne znaczenie w tym kontekście ma realizacja działań przeciwpowodziowych oraz usprawnienie systemu zarządzania kryzysowego. Istotne jest też prowadzenie kampanii edukacyjnych upowszechniających ochronę środowiska, zachowanie różnorodności biologicznej oraz adaptację do zmian klimatu. Gospodarka wodna musi stać się priorytetem w skali całej gospodarki kraju.

– w Białej Księdze Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, s. 189: *Ochrona środowiska naturalnego (bezpieczeństwo ekologiczne). Polityka państwa w zakresie bezpieczeństwa ekologicznego powinna skupiać się na dwóch obszarach: poprawie jakości środowiska oraz na działaniach prewencyjnych.*

Analiza zaprezentowanych treści wskazuje na kilka istotnych aspektów.

Pierwszy. O środowisko należy dbać, ponieważ to ono pozwala nam żyć na planecie zwanej Ziemią. Należy pamiętać, że wycinanie lasów to mniej tlenu, zmiany klimatyczne mogą oznaczać koniec życia na naszej planecie, powiększająca się dziura ozonowa to brak ochrony przed szkodliwym promieniowaniem słonecznym, zatrute środowisko zagraża wyginięciu flory i fauny, powoduje alergie i inne choroby. Zadbane i czyste środowisko przyciąga turystów i pozwala żyć zdrowo oraz wygodnie.

Drugi. Środowisko naturalne systematycznie i w sposób nieprzerwalny jest zanieczyszczane i niszczone przez przemysł, transport, rolnictwo, gospodarkę komunalną. W działaniach na rzecz poprawy jakości środowiska istotne znaczenie mają²¹⁰: postępująca redukcja emisji dwutlenków węgla, siarki i azotu oraz pyłu drobnego przy wytwarzaniu energii w celu wypełnienia zobowiązań traktatu akcesyjnego oraz dyrektyw unijnych; przyjęcie rozwiązań sprzyjających oszczędności energii oraz rozwojowi uzyskiwania jej z odnawialnych źródeł w nowej polityce energetycznej Polski do 2030 r.; podjęcie działań służących przygotowaniu do wdrożenia technologii wychwytywania i przechowywania dwutlenku węgla; utrzymanie lub osiągnięcie satysfakcjonującego stanu wód poprzez dokończenie programu budowy i rozbudowy oczyszczalni ścieków i sieci kanalizacyjnych dla aglomeracji w ramach unijnego Programu Operacyjnego Infrastruktura i Środowisko; opracowanie dla każdego dorzecza

²¹⁰ Por. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 189.

planu gospodarowania wodami; przygotowanie programu wodno-środowiskowego kraju; ograniczenie zanieczyszczenia powodowanego przez substancje niebezpieczne pochodzące ze źródeł przemysłowych; zwiększenie odzysku energii z odpadów komunalnych; zwiększenie do ponad 50 proc. ilości odzyskiwanych odpadów wytworzonych w gospodarstwach domowych; stworzenie skutecznego systemu nadzoru nad substancjami chemicznymi dopuszczonymi na rynek; usuwanie polichlorków bifenyli z transformatorów i innych urządzeń oraz usuwanie azbestu.

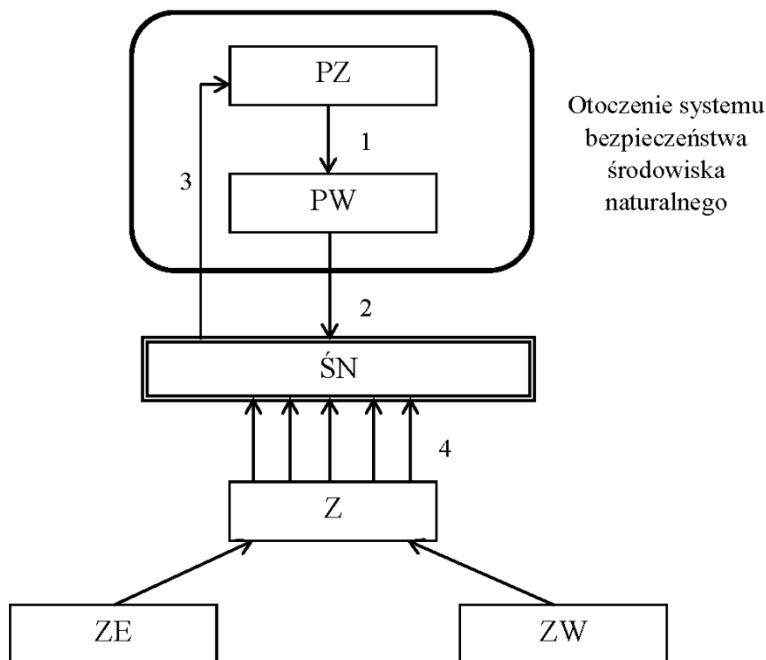
Trzeci. Ochrona środowiska naturalnego jest jednym z najważniejszych zadań, którego zrealizowania podjął się człowiek na progu XXI wieku. Odpowiedzialność za ochronę środowiska spoczywa na władzach publicznych, które są zobowiązane zapewnić bezpieczeństwo ekologiczne współczesnemu i przyszłym pokoleniom. Działania na rzecz ochrony środowiska mają charakter zasięgu krajowego i międzynarodowego.

Czwarty. Bezpieczeństwo środowiska naturalnego wymusza zidentyfikowanie niebezpieczeństw (zagrożeń), które mogą spowodować zakłócenia (egzystencji, rozwoju) lub utratę wartości przez ogół elementów przyrodniczych, w tym także przekształconych w wyniku działalności człowieka, a w szczególności powierzchnię ziemi, kopaliny, wody, powietrze, krajobraz, klimat oraz pozostałe elementy różnorodności biologicznej, a także wzajemne oddziaływania pomiędzy tymi elementami. Po identyfikacji zagrożeń, można stworzyć system bezpieczeństwa środowiska naturalnego (SBŚN), wyposażając go w określony potencjał zabezpieczeń. Można to zrealizować przez skuteczne zapobieganie (przeciwdziałanie), ochronę oraz reagowanie (zapobieganie) na występujące zagrożenia (tzn. podejmowanie takich działań, które minimalizują ich niekorzystne skutki)²¹¹. A zatem SBŚN można zdefiniować *jako taki system działania, którego celem jest zabezpieczenie (ochrona, obrona) środowiska naturalnego przed oddziaływaniem zjawisk (procesów, zdarzeń) i ich negatywnych konsekwencji (skutków, szkód)*.

Piąty. W systemie bezpieczeństwa środowiska naturalnego (SBŚN) wyróżniamy podsystemy: *wykonawczy* (siły i środki realizujące procesy wykonawcze, wydzielone np. ze straży pożarnej, ratownictwa medycznego, policji, wojska), *zarządzania* (realizuje wszystkie funkcje zarządzania, tj. planowanie, organizowanie, motywowanie, kontrolowanie, podejmowanie decyzji i koordynowanie stanowiące o sposobie zapewnienia bezpieczeństwa środowisku naturalnemu przez podsystem wykonawczy), *środowisko naturalne*, które jest obiektem oddziaływania, *zagrożenia* (każde zjawisko niepożądane z punktu widzenia niezakłóconego działania SBŚN).

²¹¹ Zob. E. Kołodziński, *Modelowanie systemów bezpieczeństwa*, [w:] Inżynieria systemów bezpieczeństwa, red. nauk. P. Sienkiewicz, PWE, Warszawa 2015, s. 18.

Koncepcję analizy systemowej bezpieczeństwa środowiska naturalnego przedstawia rys. 4.1.



- gdzie:
 1 → informacje sterujące
 2 → działania sprawcze
 3 → informacje z monitoringu środowiska naturalnego
 4 → negatywne oddziaływanie zagrożeń
- PZ – podsystem zarządzający, PW – podsystem wykonawczy,
 ŚN – środowisko naturalne, Z – zagrożenia,
 ZE – zagrożenia zewnętrzne, ZW – zagrożenia wewnętrzne.

Rys. 4.1. Koncepcja analizy systemowej bezpieczeństwa środowiska naturalnego

Źródło: opracowanie własne.

W podsystemie zarządzania SBS_{ŚN} istotną rolę odgrywa podsystem informacyjny, który odpowiada za: pozyskiwanie na bieżąco danych koniecznych do aktualnej oceny bezpieczeństwa (systematyczne zbieranie danych, dogłębna i wielokryterialna ich analiza); ocenę stanu ilościowego i jakościowego wydzielonych sił będących w dyspozycji podsystemu wykonawczego; trafną

prognozę zagrożeń i uwarunkowań niezbędnych do podejmowania decyzji dotyczących ochrony środowiska przed zagrożeniami.

Istotne dla ochrony środowiska są działania prewencyjne, które obejmują²¹²: monitoring skażeń powietrza, wód i gleby oraz prowadzenie doraźnych badań kontrolnych i pomiarowych; informowanie ośrodków decyzyjnych i ludności o skażeniach, a także alarmowanie w razie szczególnego zagrożenia; likwidację skutków zagrożeń w ramach akcji ratowniczych; działalność profilaktyczną i edukacyjną z zakresu zagrożeń związanych z niebezpiecznymi substancjami oraz przedsięwzięcia przywracające środowisko do stanu naturalnego.

Niezmiernie ważnym czynnikiem w zarządzaniu SBSN są oceny kryterium prawdopodobieństwa zaistnienia stanu zagrożenia oraz kryterium konsekwencji stanu zagrożenia, które są potrzebne do szacowania między innymi nakładów finansowych na ochronę środowiska.

Szósty. Bezpieczeństwa środowiska naturalnego nie wolno rozpatrywać z pozycji gminy, regionu czy kraju. Wymaga ono koordynacji nie tylko w skali narodowej, ale i międzynarodowej. Należy pamiętać, że bezpieczeństwo ekologiczne (środowiskowe) to składowa bezpieczeństwa narodowego i międzynarodowego. Takie myślenie i działanie zostało wymuszone np. przez zaistniałe przemysłowe katastrofy w Sevaso²¹³, Bhopalu²¹⁴, Czernobylu.

Możemy zatem przyjąć, że bezpieczeństwo ekologiczne to system organizacji rządowych, samorządowych, instytucji w wymiarze krajowym i międzynarodowym, zarządzających oraz wykonawczych, przeciwdziałających społecznym skutkom przekształceń otaczającego środowiska, których funkcjonowanie powinno przynieść pożądane efekty w wypadku zagrożeń, bez względu na ich rodzaj i pochodzenie.

²¹² Zob. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 190.

²¹³ W zakładzie ICMESA (Włochy), gdzie produkowano m.in. Trichlorofenol, nastąpiła utrata kontroli nad jednym z procesów technologicznych. Skażeniu uległo około 1500 ha gęsto zaludnionego obszaru, ewakuowano 730 osób, około 700 mieszkańców zostało poszkodowanych w wyniku zatrucia. Zginęło wiele zwierząt, wielkie tereny zostały skażone i wykluczone na wiele lat z działalności gospodarczej.

²¹⁴ Z fabryki pestycydów i środków owadobójczych amerykańskiego koncernu *Union Carbide* (Indie) uwolniło się ponad 30 ton par śmiertelnie trującego izocyjanianu metylu. Gaz uformował trującą chmurę, przemieszczającą się nad miastem. Uwolnienie do atmosfery dużych ilości niebezpiecznych, toksycznych substancji chemicznych nie spowodowało dramatycznych zniszczeń fizycznych w zakładzie i w środowisku. Natomiast liczba ofiar śmiertelnych i ciężko poszkodowanych była ogromna – pod tym względem była to największa katastrofa na świecie. Przemieszczająca się chmura izocyjanianu metylu i jego pochodnych spowodowała śmierć 6300 mieszkańców, a 250 tys. osób zostało zatrutych. Wielu z nich zostało sparaliżowanych, inni stracili wzrok i słuch oraz mieli uszkodzone płuca i nerki. Skutek skażenia to ponad 6 tysięcy ofiar śmiertelnych. Z miejsca zdarzenia ewakuowano 200 000 ludzi.

4.2. Zagrożenia ekologiczne

Degradacja środowiska na wielką skalę rozpoczęła się od rewolucji przemysłowej, zapoczątkowanej w XVIII wieku w Anglii i Szkocji, kiedy to nastąpiło przejście od pracy ręcznej na maszynową. Jest to okres, kiedy pojawiły się nowe rozwiązania technologiczne (maszyna parowa, telegraf, parowóz, silnik spalinowy, telefon, żarówka), które spowodowały rozwój przemysłu, zwiększenie wydobycia surowców, powstanie i rozwój kolei, zastosowanie maszyn parowych w fabrykach, statkach, kolei, transporcie samochodowym, rozwój miast związany z masową migracją ludzi ze wsi do miasta, skoncentrowanie ludności w obrębie dużych miast.

Przeobrażenia społeczne, kulturowe, gospodarcze zapoczątkowane rewolucją przemysłową rozpoczęły na wielką skalę degradację i zanieczyszczanie litosfery, hydrosfery oraz atmosfery. Z perspektywy czasu można stwierdzić, że negatywne zmiany w środowisku się nasilają, a dowodem tego jest: zanikanie całych ekosystemów, zanieczyszczanie powietrza, wody, gleby, zmiany klimatyczne, szybkie wymieranie gatunków fauny i flory, katastrofy ekologiczne. Zagrożenie środowiska przez powszechnie występującą technikę, a głównie przez motoryzację zalicza się do najbardziej współcześnie odczuwalnych uciążliwości rozwoju cywilizacji.

Odbudowa zagrożonego środowiska jest bardzo trudna. Odtworzenie wyciętego lasu wymaga ok. 100 lat, zbiorników wodnych – wielu dziesiątków lat, a na odbudowę gleb skażonych metalami ciężkimi trzeba tysięcy lat²¹⁵.

Źródła zagrożeń

W literaturze źródła zagrożeń są ujmowane w kontekście przedmiotowym i podmiotowym²¹⁶.

Przedmiotowe – źródłami zagrożeń są zdarzenia powodowane siłami przyrody i działalnością gospodarczą, postrzegane, jako²¹⁷: naturalne – skutki klęsk i katastrof żywiołowych oraz cywilizacyjne – materialne zanieczyszczenia różnego rodzaju i typu wprowadzane do otoczenia w toku działalności człowieka.

²¹⁵ Por. S. Wiąckowski, *Ekologia ogólna*. Oficyna Wydawnicza Branta, Bydgoszcz 2008, s. 340.

²¹⁶ Por. S. Śladkowski, *Bezpieczeństwo ekologiczne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa 2004, s. 28.

²¹⁷ Por. M. Żuber, *Bezpieczeństwo ekologiczne*, Dolnośląska Szkoła Wyższa Wydział Nauk Społecznych i Dziennikarstwa, s. 14, [w:] <https://www.wsiz.rzeszow.pl/>, 11.12.2015.

W tym ujęciu można wyróżnić również następujące grupy rodzajowe²¹⁸:

- biologiczne: awarie lub akty sabotażu w laboratoriach i instytucjach naukowo-badawczych zajmujących się badaniami bakterii i wirusów, a w związku z tym i przechowujących substancje biologicznie niebezpieczne (wirusy chorób itp.);
- chemiczne: awarie w zakładach przemysłowych, laboratoriach, magazynach, składowiskach substancji chemicznych, transporcie: kolejowym, drogowym, morskim, lotniczym, rurociągowym;
- radiacyjne: wypadki i awarie naturalnych źródeł promieniowania, w elektrowniach jądrowych, w zakładach posiadających substancje radioaktywne;
- pożarowe: budynków mieszkalnych, wielkoobszarowe lasów, zakładów lub obiektów przemysłowych, obiektów użyteczności publicznej, magazynów itp.;
- hydrologiczno-meteorologiczne: powódzie, silne wiatry i huragany, długotrwałe występowanie ekstremalnych temperatur, wyładowania atmosferyczne, susze, intensywne opady atmosferyczne (śniegu lub deszczu), zjawiska lodowe na rzekach, jeziorach i zbiornikach wodnych itp.;
- uszkodzenia, awarie i katastrofy infrastruktury technicznej – katastrofy budowlane, katastrofy górnicze, awarie i uszkodzenia infrastruktury technicznej, gazowej, wodno-kanalizacyjnej, oczyszczania miast, elektroenergetycznej, paliwowej, sieci telekomunikacyjnej i informacyjnej;
- katastrofy komunikacyjne: drogowe, kolejowe, lotnicze, wodne.

Podmiotowe – są skutkiem działań, które przez zmianę naturalnego stosunku człowieka do biocenozy i biotopów²¹⁹ mogą doprowadzić populację do unicestwienia. Ich źródłami są głównie: załamanie równowagi przyrodniczej jako następstwo nadmiernej eksploatacji zasobów środowiska; zanieczyszczenie sfer ziemi i otoczenia przez substancje pochodzenia przemysłowego, transportowego i komunalnego; postępująca degradacja ekosystemów wskutek zanieczyszczeń odpadami toksycznymi oraz katastrof ekologicznych.

Najczęściej występujące zagrożenia naturalne w Polsce

W Polsce występują różne zagrożenia naturalne. Ich częstotliwość, nasilenie, czas trwania, prawdopodobieństwo wystąpienia są zależne od pory roku. Zestawienie zagrożeń wraz z okresem wystąpienia przedstawia tabela 4.1.

²¹⁸ Tamże, s. 14.

²¹⁹ Biocenoza – zespół istot żywych, zamieszkujących jednolity wycinek biosfery, w którym liczba gatunków i osobników odpowiada przeciętnej możliwości życiowej. W każdej biocenozy wyróżnia się jej dwie podstawowe składowe: roślinną i zwierzęcą. Biotyp – zespół osobników o tych samych właściwościach dziedzicznych, czyli o takim samym genotypie. Przykładem może być flora bakteryjna, zasiedlająca organizmy ludzkie. Każdy człowiek ma wiele biotypów bakteryjnych właściwych wyłącznie dla niego, wykształconych w ciągu jego życia.

Bywają okresy, kiedy istnieje ryzyko równoczesnego wystąpienia wielu zagrożeń; tym, które powoduje największe straty jest powódź. Kolejnym pod tym względem zagrożeniem są wichury i trąby powietrzne, a także silne mrozy.

Powódzie – czasowe pokrycie przez wodę terenu, który w normalnych warunkach nie jest pokryty wodą, powstałe na skutek wezbrania wody w ciekach naturalnych, zbiornikach wodnych, kanałach oraz od strony morza, powodujące zagrożenie dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej²²⁰.

Ze względu na przyczynę wyróżniamy powódzie²²¹:

- opadowe – przyczyną są silne opady nawalne, czyli o dużym natężeniu lub rozlewne, występujące na dużym obszarze; jednym z groźniejszych, coraz częściej występujących w Polsce rodzajów powodzi opadowej, jest tak zwana powódź błyskawiczna (*Flash Flood*), określana także jako nagła powódź lokalna, która powoduje szybkie zalanie lub podtopienie terenu w wyniku wystąpienia intensywnego, krótkotrwałego opadu deszczu, najczęściej burzowego; są to powódzie, które najczęściej występują w Polsce;
- roztopowe – przyczyną jest gwałtowne topnienie śniegu;
- sztormowe – przyczyną są silne wiatry (najczęściej północno-zachodnie) powodujące wezbrania sztormowe wód morskich, wlewających się do wód śródlądowych i utrudniających odpływ wody z rzek;
- zatorowe – przyczyną jest powstanie zatorów lodowych powodujących częściowe lub całkowite zmniejszenie przepustowości koryta rzeki;
- roztopowo-opadowe – przyczyną jest topnienie śniegu spotęgowane opadami deszczu;
- wywołane awariami budowli hydrotechnicznych lub niewłaściwym gospodarowaniem wodą na zbiornikach wodnych.

Tabela 4.1

Tabela zagrożeń wraz z okresem wystąpienia

| Zagrożenie/miesiąc | I | II | III | IV | V | VI | VII | VIII | IX | X | XI | XII |
|----------------------------|---|----|-----|----|---|----|-----|------|----|---|----|-----|
| powódzie roztopowe | 1 | 1 | 1 | 1 | | | | | | | | |
| Powódzie roztopowo-opadowe | 1 | 1 | 1 | 1 | | | | | | | | |
| powódzie zatorowe | 1 | 1 | 1 | 1 | | | | | | | | 1 |
| powódzie opadowe | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | |

²²⁰ Ustawa z dnia 18 lipca 2001 r. *Prawo wodne*, art. 9.

²²¹ *Powódź w obliczu zagrożenia*, Wydział analiz RCB, marzec 2013, s. 3.

| | | | | | | | | | | | | |
|--|---|---|---|---|---|---|---|---|---|---|---|---|
| powodzie szturmowe | 1 | | | | | | | | | | | 1 |
| osuwiska | | | | | 2 | 2 | 2 | 2 | | | | |
| wichury, huragany, halny | 2 | 2 | 2 | | | | | | | | 2 | 2 |
| trąby powietrzne | | | | | 2 | 2 | 2 | 1 | | | | |
| silne mrozy, zamiecie, zawieje śnieżne | 2 | 2 | | | | | | | | | | 2 |
| pożary lasów | | | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | | |
| grypa | 2 | 2 | 2 | 2 | | | | | 2 | 2 | 2 | 2 |
| susza | | | 3 | | | 3 | 3 | 3 | 3 | | | |
| halny | 3 | 3 | | | | | | | | 3 | 3 | 3 |
| lawiny śnieżne | 4 | 4 | 4 | | | | | | | | | 4 |
| upał | | | | | | | 4 | 4 | | | | |

Legenda:

1. zagrożenie przynoszące bardzo duże straty finansowe
2. zagrożenie przynoszące duże straty finansowe
3. zagrożenie przynoszące średnie straty finansowe
4. zagrożenie przynoszące małe straty finansowe

Uwaga: Określając hierarchię zagrożeń, wzięto pod uwagę potencjalne skutki dla życia i zdrowia ludzkiego oraz szacowaną wielkość strat finansowych. Okresy występowania zagrożeń zostały wskazane na podstawie danych historycznych. Obserwowane w ostatnich latach ekstremalne zjawiska pogodowe świadczą o istnieniu potencjalnego ryzyka pojawienia się tych zagrożeń również w innych, niewymienionych miesiącach.

Źródło: *Zagrożenia okresowe występujące w Polsce*, aktualizacja, Wydział analiz RCB, styczeń 2013, s. 3.

Najczęściej występującymi powodziami są powodzie opadowe. Jako najbardziej zagrożone jej wystąpieniem są tereny pięciu województw południowych: małopolskiego, podkarpackiego, śląskiego, opolskiego i dolnośląskiego.

W ramach wdrożenia Dyrektywy 2007/60/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (tzw. Dyrektywy powodziowej), w roku 2013 opracowano *Wstępną ocenę ryzyka powodziowego*. Jej celem było wyznaczenie obszarów narażonych na niebezpieczeństwo powodzi, czyli obszarów, na których istnieje znaczące ryzyko powodziowe lub na których wystąpienie dużego ryzyka jest prawdopodobne. W Polsce do obszarów narażonych na niebezpieczeństwo powodzi zakwalifikowano 839 rzek o łącznej długości 27 161 km²²².

W wyniku powodzi występują liczne zagrożenia dla ludzi i ich dobytku oraz zwierząt. Zniszczona zostaje infrastruktura transportowa (drogi, mosty,

²²² Tamże, s. 4.

wiadukty, tory kolejowe). Uszkodzeniu ulegają linie telekomunikacyjne, wodociągowe, gazowe, linie energetyczne. W rezultacie tych strat (które trudno wszystkie wymienić ze względu na ich ilość i wieloaspektowości) powstają skutki wtórne, do których możemy zaliczyć: możliwą degradację środowiska naturalnego; możliwość miejscowego skażenia środowiska w wyniku uszkodzeń instalacji i urządzeń technicznych i uwolnienia szkodliwych substancji, możliwy brak wody pitnej, możliwy wzrost przestępczości o charakterze kryminalnym oraz zwiększoną liczbę przestępstw i wykroczeń pospolitych (kradzieże z włamaniem, rozboje, niszczenie mienia); możliwe wystąpienie epidemii, zamknięcie szkół, szpitali i urzędów administracji publicznej. Należy liczyć się ze znacznymi stratami finansowymi wynikłymi z poniesionych strat w czasie powodzi.

Wichury i trąby powietrzne – po powodzi, pod względem zagrożeń, są kolejnymi, które powodują największe straty. O tym, z jakim charakterem wiatru mamy do czynienia i z jakim stopniem zagrożenia decyduje jego prędkość na wysokości 10 m (załącznik 4.1 i 4.2).

Wichury – wiatr wiejący z prędkością powyżej 75 km/h. Najczęściej pojawiają się od listopada do marca. Mogą powodować uszkodzenia budynków, łamać i wyrwać drzewa.

Trąba powietrzna – wirowy ruch powietrza, powstający w chmurze burzowej, rozwija się do postaci wielkiego rękawa lub ogona. Podstawa trąby przy powierzchni ziemi może liczyć do 30 metrów. Trąba powietrzna osiąga wysokość 800-1500 metrów i może przemieścić się na odległość około 50-60 km, z prędkością 30-40 km/godz. Siła trąby jest tak duża, że może ona porwać człowieka, zwierzęta, elementy budynku, samochody²²³.

Według analiz prowadzonych w Instytucie Meteorologii i Gospodarki Wodnej do rejonów kraju o największym prawdopodobieństwie wystąpienia maksymalnych prędkości wiatru w porywach, związanych z ogólną cyrkulacją atmosfery, należy wschodnia część Pobrzeża Słowińskiego od Koszalina po Rozewie i Hel oraz północno-wschodnia część Pojezierza Mazurskiego, szczególnie Suwalszczyzna, a także Beskid Śląski, Beskid Żywiecki, Pogórze Śląskie, Beskid Mały, Gorce oraz Bieszczady. Wysokim prawdopodobieństwem charakteryzuje się także obszar Mazowsza.

Trąby powietrzne najczęściej pojawiają się w rejonie Opola i wędrują poprzez Wyżynę Małopolską i Lubelską, obejmując szerokim pasem o kierunku południowo/zachodnim – północno/wschodnim Wyżynę Kutnowską, Mazowsze, rejon Podlasia i Pojezierza Mazurskiego aż po Suwalszczyznę. Wiatr halny występuje w rejonie Tatr, natomiast fen w rejonie Karkonoszy²²⁴.

²²³ *Zagrożenia okresowe występujące w Polsce*, aktualizacja, Wydział analiz RCB, styczeń 2013, s. 8.

²²⁴ Tamże.

Skutki silnych wiatrów mogą obejmować obszary o różnej powierzchni zależnie od charakteru i stopnia zagrożenia. Mogą one spowodować ofiary w ludziach, naruszyć ich zdrowie. Huragany mogą spowodować zniszczenia budynków, infrastruktury telekomunikacyjnej i energetycznej, zakłócenia we wszystkich gałęziach transportu, straty w środowisku naturalnym, awarie w zakładach przemysłowych, połączone z uwolnieniem niebezpiecznych substancji, zamknięcia szkół, szpitali, urzędów administracji publicznej.

Silne mrozy, zawieje i zamiecie śnieżne, intensywne opady śniegu, marznące opady stanowią kolejne trzecie największe zagrożenie dla ludzi, środowiska naturalnego, infrastruktury (energetycznej i transportowej) oraz gospodarki w Polsce. Stopień zagrożenia zależy od ich intensywności i stopnia zagrożenia (załącznik 4.3, 4.4, 4.5 i 4.6).

Skutkiem zjawisk, które towarzyszą zimie są: zwiększone ryzyko wychłodzenia organizmów, odmrożenia, zamarznienia, zamarzanie instalacji i urządzeń hydrotechnicznych, utrudnienia komunikacyjne, nieprzejezdność dróg lokalnych, uszkodzenia drzewostanu, uszkodzenia dachów, zagrożenie życia, awarie magistrali ciepłowniczych, wodociągów, sieci kanalizacyjnej i linii przesyłowych wysokiego napięcia, co może sparaliżować normalne funkcjonowanie obywateli i gospodarki na zagrożonych obszarach.

Najniższe średnie wartości temperatur w Polsce mają obszary górskie. W nizinnej części kraju najchłodniejszy jest rejon północno-wschodni, obejmujący województwa suwalskie. W rejonie tym zimy są ostrzejsze i dłuższe, a lata stosunkowo krótkie i niezbyt ciepłe.

Oprócz wymienionych zagrożeń naturalnych, występują inne, takie jak: osuwiska, upały, pożary lasów, lawiny śnieżne, susze. Każde z nich występuje z różnym natężeniem, a straty są zależne od natężenia i stopnia zagrożenia, jakie ze sobą noszą.

Najczęściej występujące zagrożenia cywilizacyjne w Polsce

We współczesnych czasach najgroźniejsze są zagrożenia cywilizacyjne, które poprzez różnego rodzaju i typu materialne zanieczyszczenia są wprowadzane do otoczenia w toku działalności człowieka. Źródłami zagrożeń dla Polski, towarzyszących rozwojowi cywilizacyjnemu, są: katastrofy (drogowe, kolejowe, morskie, w kopalniach), awarie (w przedsiębiorstwach produkcyjnych, usługowych i handlowych, linii energetycznych, zapór i urządzeń zbiorników wonnych, sieci gospodarki komunalnej), skażenia przemysłowe (chemiczne i radiologiczne dokonujące skażeń organizmów oraz żywności, atmosfery, gleby, fauny i flory), transport, dziura ozonowa (efekt cieplarniany, zanik warstwy ozonowej), inne (hałas, wstrząsy – drgania, kwaśne deszcze, dymy, pyły, ropa naftowa i jej pochodne).

Katastrofa ekologiczna to nowy termin, rozumiany jako trwałe, nieodwracalne uszkodzenia lub zniszczenia środowiska, mające negatywny wpływ na życie i zdrowie człowieka. Katastrofy ekologiczne wiążą się ze zmianą

struktury i funkcji całych ekosystemów. Ze względu na pochodzenie można je podzielić na dwie grupy²²⁵: katastrofy naturalne (określane także jako klęski żywiołowe) oraz katastrofy antropogeniczne.

Katastrofy naturalne są powodowane przez siły przyrody wymienione w tabeli 4.1, np.: powódzie, osuwiska ziemi, ekstremalne temperatury, susze, pożary dużych kompleksów leśnych.

Drugą grupę stanowią katastrofy antropogeniczne, a więc te, które są związane z celową działalnością człowieka lub mają charakter niezamierzony przez niego, lecz pozostają w związku z jego działalnością. Najczęściej pojawiają się w wyniku awarii różnego rodzaju obiektów budowlanych, maszyn, czego skutkiem jest emisja trujących gazów lub cieczy do środowiska. Katastrofy tego rodzaju mogą dotyczyć wody, powietrza i ziemi.

Od lat 90. eksperci wyróżniają cztery główne rodzaje zagrożenia ekologicznego o globalnym charakterze. Są to²²⁶: rozprzestrzenianie się substancji toksycznych niedających się biologicznie rozłożyć – chemicznych lub radioaktywnych (wybuchy jądrowe, awarie przemysłowe), dewastacja flory i fauny, zanieczyszczenia górnych warstw atmosfery, które powodują uszkodzenie warstwy ozonu (dziura ozonowa) i na skutek tego wzrost przenikania szkodliwych promieni ultrafioletowych, efekt cieplarniany.

Rozprzestrzenianie się substancji toksycznych – może odbywać się w wodzie, powietrzu, jak i glebie, a ich źródła w głównej mierze są: energetyczne (spalanie paliw), przemysłowe (procesy technologiczne w zakładach chemicznych, rafineriach, hutach, kopalniach i cementowniach), komunikacyjne (głównie transport samochodowy, ale także kolejowy, wodny i lotniczy), komunalne (funkcjonowanie gospodarstw domowych oraz gromadzenie i utylizacja odpadów i ścieków, np. wysypiska, oczyszczalnie ścieków).

Transport samochodowy jest jednym z głównych źródeł antropogenicznego zanieczyszczenia powietrza, degradacji środowiska naturalnego i negatywnego oddziaływania na człowieka. Wskutek spalania paliw w silnikach pojazdów do powietrza są emitowane substancje toksyczne, takie jak: tlenek węgla (CO), węglowodory (HC), tlenki azotu (NOx), aldehydy (RCHO), dwutlenek siarki (SO₂), związki ołowiu, cząstki stałe.

Najgroźniejsze dla człowieka w atmosferze są gazy i aerozole o cząstkach mniejszych niż mikrometr, które łatwo przenikają do płuc. Głównymi składnikami zanieczyszczeń powietrza są²²⁷: tlenki siarki pochodzące z węgla i olejów opałowych używanych w przemyśle, pyły i sadza z przemysłu, na bazie których dochodzi do powstania smogu w miastach, trujące związki z pojazdów mechanicznych powodujące bóle głowy, niedyspozycje, a w dużych

²²⁵ Por. Z. Polcikiewicz, *Teoria bezpieczeństwa*. WSOWL, Wrocław 2012, s. 58.

²²⁶ Tamże, ss. 59-60.

²²⁷ Por. N. Wolański, *Ekologia człowieka. Ewolucja i dostosowanie biokulturowe*. PWN, Warszawa 2008, s. 300.

stężeniach nawet śmierć, utleniacze, stanowiące wynik działania promieni słonecznych na niespalone węglowodory i tlenki azotu, a powodujące smog, który podrażnia oczy i ogranicza widzialność, tlenki azotu ze spalin samochodowych oraz powstające w czasie produkcji przemysłowej, ołów, dodawany do benzyny i wydzielany z samochodów wraz ze spalinami, akumulowany w ciele – działa toksycznie.

Dewastacja flory i fauny – to zjawisko, które przybiera na sile. Jednym z czynników są tzw. kwaśne deszcze. Szczególnie zagrożone tym rodzajem zanieczyszczeń są obszary przemysłowe i duże miasta. Źródłem kwaśnych deszczów zagrażających zarówno lasom, jak i zabytkom jest zanieczyszczenie atmosfery. Źrące opady są rezultatem reakcji z udziałem lotnych węglowodorów, dwutlenku siarki, tlenków azotu emitowanych przez przemysł, elektrownie ciepłownicze, transport i rolnictwo. Woda zawarta w chmurach znajdujących się nad fabrykami nasycana jest emitowanymi do atmosfery związkami chemicznymi. W tych okolicznościach zachodzą reakcje, które powodują powstawanie kwasów: z dwutlenku siarki (SO_2) tworzy się ostatecznie kwas siarkowy (H_2SO_4), z tlenków azotu – kwas azotowy (HNO_3). Szkodliwe substancje przemieszczają się z wiatrem w postaci zawiesiny i opadając z cząsteczkami wody na ziemię, uszkadzają wiele ekosystemów. Perspektywy poprawy tego procesu są wątpliwe. Pozytyw wynikający ze zmniejszenia emisji dwutlenku siarki jest niwelowany faktem, że zanieczyszczenie tlenkami azotu stale wzrasta ze względu na nasilający się ruch samochodowy.

Kwaśne deszcze mają destrukcyjny wpływ na roślinność. Powodują obumieranie drzew, a także niszczenie runa leśnego. Liście drzew ulegają uszkodzeniu, co powoduje nadmierne parowanie wody i zakłócenia w procesie fotosyntezy, skutkiem czego jest mała odporność tych roślin na warunki klimatyczne. Poza tym kwaśne deszcze zakwaszają glebę, co przyczynia się do uaktywnienia glinu i kadmu, a także nagromadzenia azotanów i siarczanów. Korzenie roślin mają zmniejszoną możliwość pobierania wapnia, magnezu i potasu, ponieważ wymywają je kwaśne deszcze. Skutkiem tego jest niedobór niezbędnych składników odżywczych. Korzenie zamierają, a roślina ginie.

Kwaśne deszcze i inne opady przedostają się także do jezior, rzek itp., zakwaszają je i powodują, że niemożliwe staje się ich wykorzystywanie. Szkodliwe substancje mogą dostawać się do wód w dwojaki sposób. Trafiają tam wraz z wodą ściekającą z okolicznych pól, łąk i innych terenów, a także bezpośrednio wraz z opadami atmosferycznymi²²⁸.

Dziura ozonowa – to kolejny problem XXI wieku w obszarze ochrony środowiska. Zjawisku temu towarzyszy zmniejszenie koncentracji ozonu w ozonosferze, która rozciąga się na wysokości 10-50 km. Przypuszcza się,

²²⁸ Zob. B. Żółtowski, K. Kwiatkowski, *Zagrożone środowisko*, Wydawnictwa Uczelniane Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy, Bydgoszcz 2012, ss. 9-10.

że przyczyną powstawania dziury ozonowej są substancje przedostające się do atmosfery w wyniku gospodarczej działalności człowieka, zwłaszcza freony i halony, a także tlenki azotu (produkt m.in. spalania paliw w silnikach samolotów i raket).

Problem z dziurą ozonową pojawił się, gdy freonu oraz innych fluoropochodnych metanu i etanu zaczęto używać do produkcji aerozoli.

Ozonosfera pochłania bardzo szkodliwe dla wszystkich żywych organizmów promieniowanie ultrafioletowe (UV). Niszczenie warstwy ozonowej prowadzi do zmniejszenia się efektywności pochłaniania promieni UV. W wyniku tego organizmy są narażone na zwiększone promieniowanie ultrafioletowe.

Nadmiar promieni UV może doprowadzić do zakłócenia równowagi całych ekosystemów. Promieniowanie ultrafioletowe przenika wodę do kilku metrów włąb (w przypadku wód czystych nawet do kilkunastu metrów). Powoduje to zamieranie szczególnie wrażliwych organizmów roślinnych i zwierzęcych tworzących plankton. Zmniejszy się więc występowanie ryb żywiących się planktonem oraz ryb drapieżnych.

Promieniowanie ultrafioletowe wpływa również niekorzystnie na rośliny. Wśród roślin, które wykazują reakcję na promienie UV, ponad dwie trzecie gatunków jest na nie wrażliwe. Należy przy tym zaznaczyć, że są to głównie gatunki roślin uprawnych i przemysłowych. Zwiększenie się natężenia promieniowania ultrafioletowego na Ziemi odbije się z pewnością na gospodarce człowieka. Zmniejszenie liczebności populacji ryb na skutek zaniku planktonu doprowadzi do znacznie mniejszych połowów na określonym terenie. Ucierpi więc rybactwo i rybołówstwo.

Promieniowanie ultrafioletowe może również negatywnie wpływać bezpośrednio na ludzi. Poprzez wytwarzanie pigmentów w skórze, człowiek tylko w niewielkim stopniu jest zdolny do obrony. Nadmierne promieniowanie UV może osłabiać u ludzi system immunologiczny i tym samym zmniejszać odporność na infekcje i choroby, wśród których najgroźniejsze są z pewnością choroby nowotworowe, a szczególnie nowotwory skóry (np. czerniak). Ponadto promieniowanie ultrafioletowe powoduje podrażnienie spojówek, a przez to występowanie licznych chorób oczu, głównie zaćmy. Promienie UV powodują także przyspieszenie procesów starzenia się skóry²²⁹.

Efekt cieplarniany to zjawisko ocieplenia atmosfery (klimatu) wywołane wzrostem zanieczyszczeń związkami chemicznymi, głównie dwutlenkiem węgla.

Promieniowanie słoneczne docierające do Ziemi odbija się od atmosfery, chmur i od powierzchni planety. Pozostała jego część przenika przez atmosferę

²²⁹ Zob. B. Żółtowski, K. Kwiatkowski, *Zagrożone środowisko*, Wydawnictwa Uczelniane Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy, Bydgoszcz 2012, ss. 9-10; *Dziura ozonowa*, <http://ekoproblemy.2ap.pl/>, 28.11.2015.

i dociera do powierzchni Ziemi, gdzie zostaje pochłonięta. Ziemia natomiast wysyła energię w postaci promieniowania cieplnego (promieniowanie podczerwone o dłuższej długości fali niż promieniowanie świetlne), które jest pochłaniane przez atmosferę, a dokładniej przez obecne w niej gazy zwane gazami cieplarnianymi. Część tego promieniowania jest wyemitowana w przestrzeń kosmiczną, pozostała zaś ulega odbiciu i wraca w kierunku Ziemi. Ciepło to ogrzewa atmosferę, powierzchnię lądów i oceanów, dzięki czemu warunkuje istnienie odpowiednich warunków temperaturowych do rozwoju życia.

Otóż w trakcie wymiany Słońce-Ziemia-przestrzeń kosmiczna niektóre gazy reagują jak szyba: umożliwiają przejście światłu słonecznemu, zatrzymują jednak podczerwień. W cieplarni promienie Słońca, padając przez szyby, ogrzewają rośliny, które z kolei wypromieniowują ciepło pozostające w znacznej części we wnętrzu szklarni. Gdyby proces ten nie zachodził, temperatura powierzchni Ziemi wynosiłaby 18°C. Zaburzeniem jest więc nie samo zjawisko, lecz jego nasilenie się w wyniku działalności człowieka.

Światło słoneczne (światło widzialne) swobodnie przechodzi przez atmosferę. Pewna jego część jest natychmiast odbita przez chmury, cząstki stałe w atmosferze i jasne powierzchnie. Reszta jest pochłaniana przez podłoże i ogrzewa Ziemię. Gazy cieplarniane w atmosferze spowalniają emisję ciepła do przestrzeni kosmicznej.

Promieniowanie słoneczne docierające do powierzchni Ziemi jest pochłaniane przez roślinność, glebę i wodę oraz odbijane i kierowane do górnych warstw atmosfery. Gazy, takie jak dwutlenek węgla, tlenki azotu, metan i związki fluoropochodne zatrzymują odbite promienie i powodują ich wtórną emisję w kierunku Ziemi. Pozostała część promieni opuszcza atmosferę. Zjawisko wtórnej emisji pozwala na zachowanie równowagi energetycznej Ziemi i ustalenie średniej temperatury, która wynosi 15°C. Wzrastające w atmosferze stężenie gazów odpowiedzialnych za powstawanie efektu cieplarnianego, przede wszystkim CO₂, przyczynia się do nasilenia zjawiska wtórnej emisji i podwyższenia średniej temperatury na Ziemi.

Źródłami gazów, wywołujących efekt cieplarniany, są spalane kopalne surowce energetyczne (węgiel, ropa naftowa). Efekt cieplarniany jest wzmacniany ubytkiem lasów tropikalnych i pożarami sawanny. Szacuje się, że corocznie ok. 6 mld ton CO₂ uwalnia się do atmosfery. Część z niego jest pochłaniana przez ekosystemy leśne, np. lasy europejskie wychwytyją od 70 do 105 mln ton rocznie. Zatem zalesienie światowych zasobów terenów może znacznie ograniczyć postępujący efekt cieplarniany. Polska również ma udział w emisji CO₂, co obrazuje tabela 4.2.

Tabela 4.2

Całkowita emisja dwutlenku węgla w Polsce (w milionach ton)

| Wyszczególnienie | 2011 r. | 2012 r. | 2013 r. | 2014 r. |
|------------------|---------|---------|---------|---------|
| Dwutlenek węgla | 339,98 | 326,0 | 331,1 | 316,8 |

Źródło: *Environment, Ochrona środowiska 2014*, GUS, Warszawa 2014, s. 231.

Nadzieją na zatrzymanie efektu cieplarnianego było podpisanie porozumienia klimatycznego przez 195 delegacji różnych krajów z 12 na 13 grudnia 2015 roku w Paryżu.

Główny cel zawarty w porozumieniu klimatycznym to ograniczenie wzrostu temperatury na świecie do poniżej 2°C i dążenie do nawet 1,5°C. Z naukowych analiz opublikowanych przez BBC wynika, że jeśli kraje nie podjęłyby żadnych działań, do 2100 r. temperatura wzrosłaby aż o 4,5°C. Naukowcy przewidują jednak, że postanowienia z Paryża doprowadzą do zmniejszenia globalnego ocieplenia tylko do 2,7°C. Obrany cel, jakim są 2°C, oznacza więc, że kraje muszą wyjątkowo się zmobilizować. Kwestią wiążącą prawnie wszystkie kraje (i budzącą wcześniej największą emocje) będzie redukcja emisji dwutlenku węgla i innych gazów cieplarnianych do atmosfery. W Paryżu ustalono także, że do 2020 r. kraje rozwinięte mają łącznie przeznaczać na walkę ze zmianami klimatycznymi 100 mld dolarów rocznie. Zobowiązały się także do udzielania pomocy finansowej biedniejszym państwom rozwijającym się. Kraje świata ustaliły także w umowie, że będą spotykać się, co pięć lat, aby kontrolować wypełnianie postanowień, oszacować osiągnięty postęp i wypunktować to, co jeszcze należy zrobić²³⁰.

Hałas – pojęcie subiektywne, określające niekorzystne oddziaływanie dźwięków złożonych o różnej częstotliwości. Według Polskiej Normy hałasem jest dźwięk o dowolnym charakterze akustycznym, niepożądany w danych warunkach i przez daną osobę²³¹. Powodowany jest przede wszystkim przez środki transportu: ruch drogowy, ruch kolejowy, ruch samolotowy oraz pochodzący z obszarów działalności przemysłowej.

Ochrona przed hałasem polega na zapewnieniu jak najlepszego klimatu akustycznego środowiska, tj. zespołu zjawisk akustycznych na danym obszarze, w szczególności poprzez utrzymanie poziomu hałasu poniżej wartości dopuszczalnej lub na tym poziomie oraz na zmniejszeniu poziomu hałasu do co najmniej dopuszczalnego, jeśli nie jest on dotrzymany.

²³⁰ Por. A. Gersz, *Szczyt klimatyczny w Paryżu: Państwa przyjęły historyczne porozumienie*, <http://www.polskatimes.pl/>, 13.12.2015.

²³¹ Por. B. Rączkowski, *BHP w praktyce*, ODiDK, Gdańsk 2010, s. 257.

Trendy hałasu środowiskowego w Polsce wskazują z jednej strony na wzrost zagrożenia hałasem komunikacyjnym, z drugiej – na ograniczenie wzrostu i wystąpienie tendencji malejących w zakresie hałasu przemysłowego.

Przeprowadzone w 2013 r. pomiary monitoringowe hałasu przemysłowego objęły kontrolą 1137 obiektów emitujących hałas, z czego 37% przebadanych zakładów przekroczyło dopuszczalne wartości. Do najbardziej uciążliwych branż w porze dziennej zalicza się: przemysł rozrywkowy, tartacznictwo, obróbkę drewna oraz lotnictwo; w porze nocnej: górnictwo, produkcję alkoholu, suszarnie, obróbkę plastyczną oraz przemysł rozrywkowy.

Tendencje wzrostowe hałasu komunikacyjnego odnoszą się przede wszystkim do hałasu drogowego i hałasu lotniczego. Wzrost zagrożenia hałasem drogowym w ostatnich latach związany jest głównie z powstającymi nowymi drogami, mostami, obwodnicami i autostradami oraz szybkim wzrostem liczby pojazdów w Polsce.

Hałas drogowy stanowi zagrożenie przede wszystkim na terenach zurbanizowanych i jest odczuwany przez coraz większą liczbę mieszkańców, zwłaszcza w środowisku miejskim. Spośród 338 km dróg skontrolowanych w 2013 r., zaledwie dla 15 km dróg emisja hałasu drogowego mieści się w przedziale do 60 dB (tj. emisji niepowodującej przekroczeń dopuszczalnych poziomów dźwięku w porze dziennej na terenach mieszkalnych przyległych do dróg). Na 98% skontrolowanych dróg poziom hałasu został przekroczony.

W przypadku hałasu lotniczego obserwuje się trendy wzrostu poziomu hałasu wskutek rozwoju ruchu lotniczego. Hałas ten charakteryzuje się oddziaływaniem na duże powierzchnie terenu oraz wysokimi poziomami emisji, a także brakiem efektywnych zabezpieczeń środowiska²³².

Zarządzanie zagrożeniami ekologicznymi

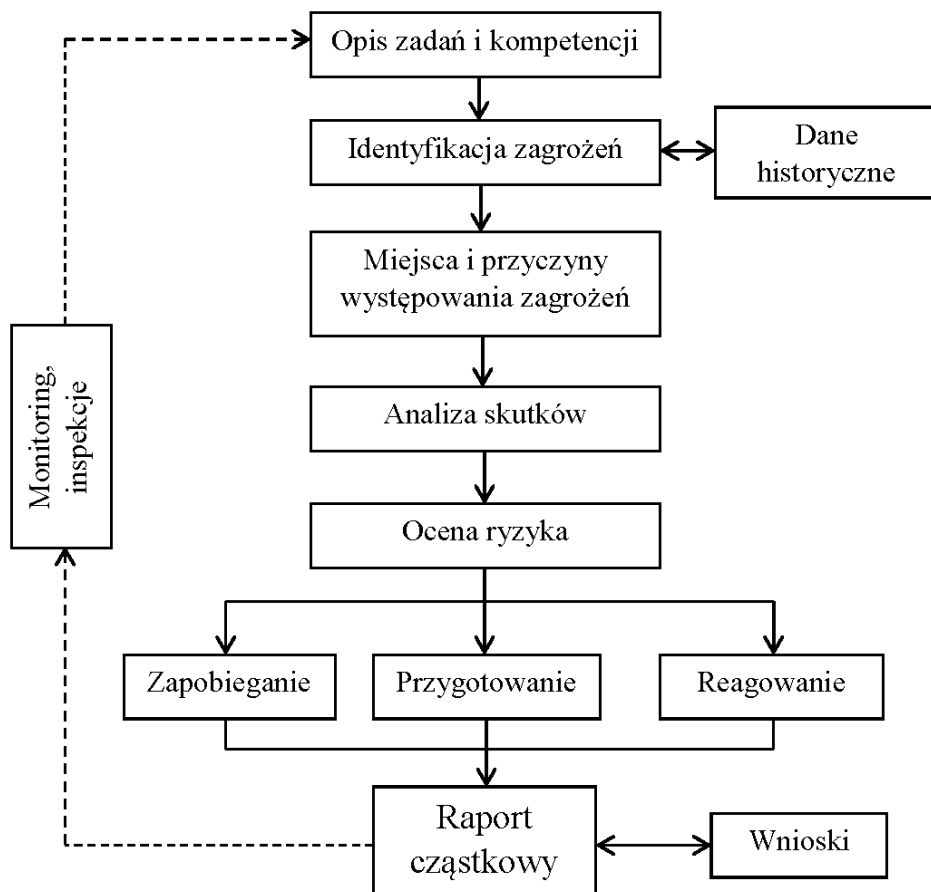
Zagrożenie, które godzi w życie lub zdrowie dużej liczby osób, mienie w znacznych rozmiarach albo środowisko na znacznych obszarach winno być zidentyfikowane oraz opisane na mapie ryzyka²³³ i mapie zagrożeń²³⁴. Każda taka analiza powinna udzielić odpowiedzi na pytanie: co złego i gdzie może się stać?

W celu sporządzenia raportu cząstkowego dla określonego zagrożenia mogącego mieć negatywny wpływ między innymi na środowisko, opracowano algorytm (rys. 4.2), który wymaga ujednoczonych informacji w obszarach: zagrożenia, zapobieganie, przygotowanie, reagowanie, dane historyczne, wykazy i wnioski.

²³² *Environment, Ochrona środowiska 2014*, GUS, Warszawa 2014, s. 45.

²³³ Mapa ryzyka – należy przez to rozumieć mapę lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę, wg Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3.

²³⁴ Mapa zagrożeń – należy przez to rozumieć mapę przedstawiającą obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń wg Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3.



Rys. 4.2. Algorytm opracowania raportu cząstkowego dla zagrożeń naturalnych i cywilizacyjnych środowiska naturalnego

Źródło: por. *Procedura opracowania raportu cząstkowego do Raportu o zagrożeniach bezpieczeństwa narodowego*, RCB Rządowe Centrum Bezpieczeństwa, Warszawa 2010, s. 6.

Zagrożenia

Identyfikacji podlegają wszystkie rodzaje zagrożeń, które mogą oddziaływać negatywnie na środowisko. Zagrożenia mogą być także identyfikowane poprzez analizę danych historycznych i/lub statystycznych z wykorzystaniem szacowań eksperckich, badań terenowych, modeli matematycznych, analizy „case study”, wyników danych z systemów monitoringu, oceny sytuacji międzynarodowej. Ważnym elementem w czasie identyfikacji zagrożeń jest ustalenie kryteriów oceny ryzyka, a w szczególności prawdopodobieństwa wystąpienia zagrożenia oraz skutków (konsekwencje) takiego zagrożenia. Dla prawdopodobieństwa wybrano skalę jakościową (opisową) od 1 – bardzo rzadkie do 6 – wielce prawdopodobne. Dla skutków proponuje się podobne rozwiązanie

z tym jednak, że należy dla sześciu skali (od A – nieistotne do E – katastrofalne) dopasować parametr najbliższy rzeczywistości w kategoriach (Z – życie, M – mienie, **S – środowisko**).

Na bazie dwóch zestawień prawdopodobieństwa wystąpienia zagrożenia i jego skutków opracowuje się matryce ryzyka. Dla każdego zagrożenia dla środowiska w matrycy ryzyka określa się wartość ryzyka²³⁵: minimalne (kolor niebieski), małe (kolor zielony), średnie (kolor żółty), duże (kolor czerwony), ekstremalne (kolor brunatny). Na tej bazie wprowadzono 4 kategorie akceptacji ryzyka: akceptowane (A) – niewymagane są żadne dodatkowe środki bezpieczeństwa, akceptowane są aktualne rozwiązania i przypisane im siły i środki, działania monitorujące; dopuszczalne (T) – należy dokonać oceny alternatyw czy wprowadzenie niewielkich zmian organizacyjnych, prawnych bądź funkcjonalnych nie przyczyni się do poprawy bezpieczeństwa lub jego poczucia; warunkowo tolerowane (WT) – należy wprowadzić dodatkowe środki bezpieczeństwa w terminie 6 miesięcy, należy ulepszyć stosowane rozwiązania; nieakceptowane (N) – należy podjąć natychmiastowe działania w celu zwiększenia bezpieczeństwa, wprowadzić dodatkowe/nowe rozwiązania.

Zapobieganie – szereg przedsięwzięć, których realizacja eliminuje bądź zmniejsza prawdopodobieństwo wystąpienia zagrożenia i skutki jego oddziaływania na środowisko. Etap ten obejmuje między innymi czynności: prawne (ustawy, rozporządzenia, wytyczne), organizacyjne (wydzielenie zasobów ludzkich, finansowych, sprzętowych, prowadzenie prac badawczych i transferu technologii, stworzenie klimatu ogólnie społecznego przeciwdziałającego zagrożeniom), proceduralne (oddalenie zagrożenia od tego, co ma być chronione, zapobieganie uwolnieniu zagrożenia, które już istnieje, współdziałanie w szerokim pojęciu).

Przygotowanie – polega na podejmowaniu działań planistycznych, dotyczących sposobów reagowania na czas wystąpienia różnego rodzaju zagrożenia środowiska, umożliwiających wpływ na ich przebieg w celu zmniejszenia negatywnych skutków tych zdarzeń. Faza ta obejmuje również działania mające na celu powiększenie zasobów sił i środków niezbędnych do efektywnego reagowania, zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu reagowania na potencjalne zagrożenia środowiska²³⁶. Przygotowanie obejmuje: opracowanie planów, algorytmów (scenariuszy) i procedur działań, organizację systemów łączności i komunikacji, organizację systemów monitorowania, organizację i utrzymanie systemów

²³⁵ Procedura opracowania raportu cząstkowego (integralna część z arkuszem kalkulacyjnym) *do Raportu o zagrożeniach bezpieczeństwa narodowego* – Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. Z 2010, Nr 83, poz. 540).

²³⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

ostrzegania i alarmowania, szkolenia specjalistyczne i doskonalenie umiejętności, informowanie ludności cywilnej.

Reagowanie – działania po wystąpieniu zagrożeń naturalnych i cywilizacyjnych dla środowiska. Etap ten wymaga wcześniejszego określenia zasad reagowania i hierarchizacji działań w przypadku wystąpienia zagrożenia. Celem jest niesienie pomocy i ograniczenie wtórnych zniszczeń. Reagowanie wymaga właściwej i profesjonalnej znajomości problemu, a także nowoczesnych, niezawodnych środków łączności oraz dokładnych danych z monitoringu obszarów zagrożonych.

4.3. Ekologistyka w ochronie środowiska

W Polsce w 2013 roku wytworzono 142 mln ton odpadów, z czego 8% stanowiły odpady komunalne (11 mln ton). Głównym źródłem odpadów w 2013 r. były, podobnie jak w latach poprzednich: górnictwo i wydobywanie (ok. 52% ilości wytworzonych odpadów ogółem), przetwórstwo przemysłowe (20%) oraz wytwarzanie i zaopatrywanie w energię elektryczną (17%). W ostatnim dziesięcioleciu największy udział w ilości odpadów wytworzonych stanowiły odpady powstające przy poszukiwaniu, wydobywaniu, fizycznej i chemicznej przeróbce rud i innych kopalin (57% w 2013 r.) oraz odpady z procesów termicznych (23%). Z ogólnej ilości odpadów wytworzonych w 2013 r. 69% odpadów poddano odzyskowi, 25% unieszkodliwiono przez składowanie, 3% unieszkodliwiono w sposób inny niż składowanie oraz ok. 2% odpadów poddano czasowemu magazynowaniu.

Ogólna ilość odpadów dotychczas składowanych (nagromadzonych) na składowiskach własnych zakładów i obiektach unieszkodliwiania odpadów (hałdach, stawach osadowych) do 2012 r. systematycznie zmniejszała się, w roku 2013 nastąpił nieznaczny wzrost (o ok. 1%) do poziomu 1,7 mld ton. Ilość odpadów komunalnych wytworzonych w 2013 r. zmniejszyła się w stosunku do 2012 r. o 7% i wyniosła 11,3 mln ton. Oznacza to zmniejszenie z 314 kg w 2012 roku do 293 kg w 2013 r. odpadów wytworzonych na jednego mieszkańca Polski. Jest to jeden z najniższych wskaźników wśród krajów europejskich. Średnia ilość odpadów komunalnych na jednego mieszkańca UE w 2012 r. wyniosła 492 kg. Najwięcej odpadów komunalnych w przeliczeniu na 1 mieszkańca wytworzyły: Dania 668 kg, Cypr 663 kg, Luksemburg 662 kg oraz Niemcy 611 kg. Z ogólnej ilości wytworzonych odpadów komunalnych w UE, 34% unieszkodliwiono poprzez składowanie, 27% poddano recyklingowi, 24% unieszkodliwiono termicznie oraz 15% poddano kompostowaniu²³⁷.

²³⁷ *Environment, Ochrona ...*, op. cit., s. 42.

Problemy gospodarowania odpadami coraz częściej znajdują się w kompetencjach osób zajmujących się w przedsiębiorstwach logistyką. Należy zaznaczyć, że odpady to nie tylko coś co jest gorszej jakości, co jest odpadem działalności człowieka lub systemów gospodarczych, bądź mało lub całkowicie nieprzydatne do dalszego użytku. Nie wolno zapominać, że dla jednych coś jest odpadem, a dla drugich stanowi zasób do wykorzystania.

Odpady zachowują specyficzne cechy, są dobrem będącym w obrocie towarowym, o czym świadczą między innymi ogólnopolskie giełdy odpadów. Zdaniem ekspertów w najbliższych latach rynek obrotu odpadami może się podwoić. Uzyskiwanie energii ze spalania śmieci staje się coraz częstszą praktyką np. w Szwecji i w Danii. W Holandii, która jest największym importerem śmieci w Unii Europejskiej, odpady stały się ważnym źródłem energii i oszczędności.

W rozwiniętych krajach UE, a także w Szwajcarii i Norwegii pracuje obecnie ponad 400 instalacji odzyskujących energię z odpadów komunalnych. Spalają one obecnie na terenie UE 70 mln ton/rok odpadów komunalnych, dostarczają energię elektryczną dla około 13 mln mieszkańców, a ciepło dla 12 mln mieszkańców miast²³⁸.

Jest to zapewne argument, aby nasze społeczeństwo wyzbyło się niechęci do spalarni odpadów, które mają być budowane w okolicach, gdzie mieszkają ludzie²³⁹.

Zagospodarowanie odpadów jest ściśle związane ze zrównoważonym rozwojem, który *zaspokaja podstawowe potrzeby wszystkich ludzi oraz zachowuje, chroni i przywraca zdrowie i integralność ekosystemu Ziemi, bez zagrożenia możliwości zaspokojenia potrzeb przyszłych pokoleń i bez przekraczania długookresowych granic pojemności ekosystemu Ziemi*²⁴⁰.

Narzędziem pomocnym w zagospodarowaniu odpadów okazała się logistyka, która do niedawna była postrzegana jako koncepcja, która miała usprawniać wyłącznie przepływ strumienia rzeczowego od źródła pozyskania (np. surowców) poprzez produkcję wyrobów i dostarczenie ich finalnemu odbiorcy.

To nowe zastosowanie logistyki w zarządzaniu przepływami odpadów w uniwersalnej istocie nosi nazwę ekologii. W literaturze przedmiotu jest również określana jako logistyka: zwrotna, odwrotna, utylizacji, odpadów, odwrócona, pozostałości oraz logistyki powtórnego zagospodarowania.

²³⁸ Por. K. Blumenthal, *Generation and treatment of municipal waste*, [w:] Eurostat: Statistics in Focus, 31/2011. Eurostat, 2011.

²³⁹ Do końca 2015 roku przy znacznym poziomie wsparcia finansowego z Unii Europejskiej, powstanie 26 dużych zakładów zagospodarowania odpadów. W tym gronie znajdzie się sześć spalarni a 13 funkcjonujących już zakładów zostanie zmodernizowanych, *Akademia odpadowa*, <http://www.akademiaopadowa>, 11.12.2015.

²⁴⁰ Por. R.K. Stappen, *A Sustainable World is Possible. Der Wise Consensus: Problemlösungen für das 21 Jahrhundert. Impuls – dokument Manuskript 1.2/2006*, ss. 27-28.

Czasami ekologistyka jest utożsamiana z logistyką zieloną (*green logistics*), co jest błędem, jako że ta druga jest ściśle związana z wykorzystaniem przyjaznych środowisku zasobów włącznie z ich transformacją sprzyjającą człowiekowi, a nieszkodzącą istniejącemu środowisku.

Ekologistyka obejmuje ogół procesów zarządzania przepływami odpadów (w tym również produktów pełnowartościowych i uszkodzonych, ale uznanych przez ich dysponentów za odpady), a także informacji (związanych z tymi przepływami), od miejsc ich powstawania (pojawiania się w systemie logistycznym) do miejsca ich przeznaczenia w celu ich ponownego użycia, odzyskania wartości (poprzez naprawę, recykling lub przetworzenie) lub właściwego ich unieszkodliwienia i długoterminowego składowania w taki sposób, by przepływy te były efektywne ekonomicznie i minimalizowały negatywny wpływ na środowisko naturalne człowieka²⁴¹. W nawiązaniu do powyższych ustaleń ekologistykę można określić jako zintegrowany system, który²⁴²:

- opiera się na koncepcji zarządzania recyrkulacyjnymi przepływami strumieni materiałów odpadowych w gospodarce oraz przepływami sprzężonych z nimi informacji;
- zapewnia gotowość i zdolność efektywnego gromadzenia, segregacji, przetwarzania oraz ponownego wykorzystania odpadów wg przyjętych zasad technicznych i procesowych, spełniających wymagania normowe i prawne ochrony środowiska;
- umożliwia podejmowanie technicznych i organizacyjnych decyzji w kierunku zmniejszenia (minimalizacji) tych negatywnych skutków oddziaływania na środowisko, które towarzyszą realizacji procesów zaopatrzeniowych, przetwórczych, produkcyjnych, dystrybucyjnych i serwisowych w logistycznych łańcuchach dostaw.

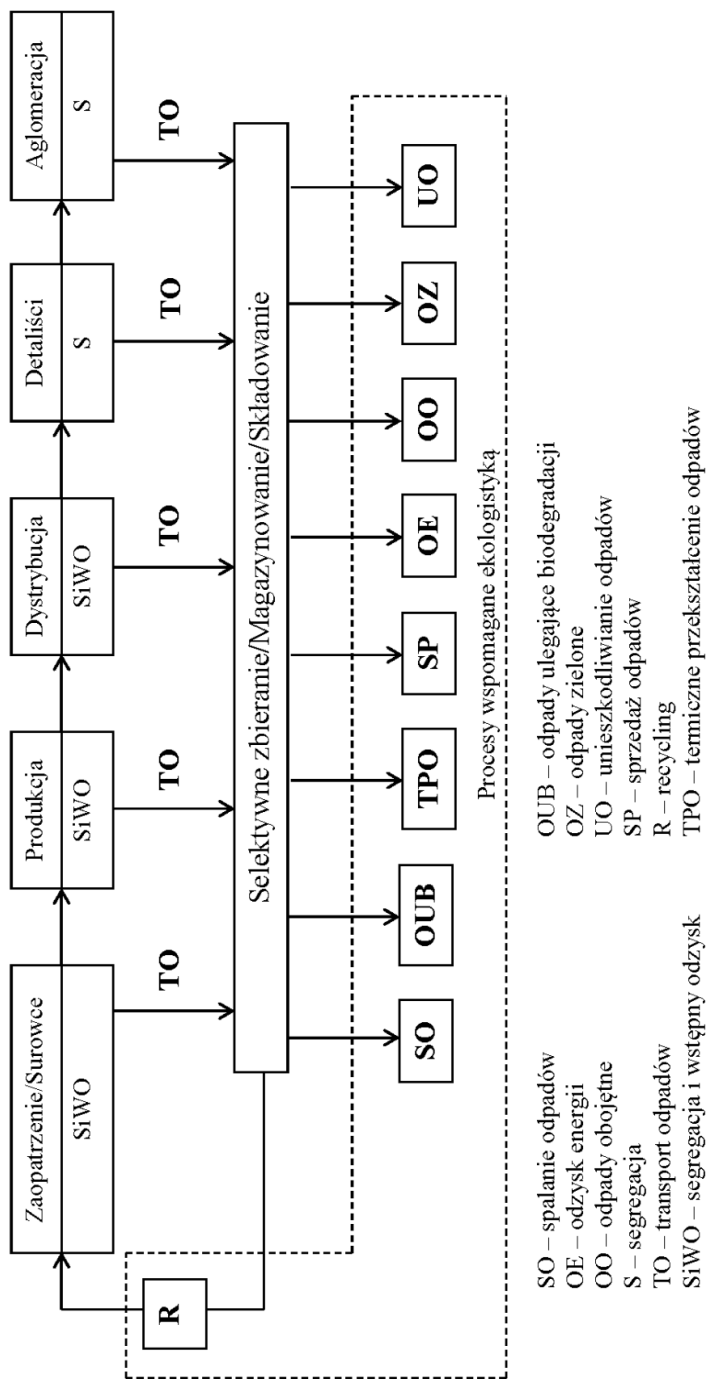
Ważnymi procesami w gospodarce odpadami, które wspomaga ekologistyka są²⁴³:

- selektywne zbieranie, w ramach którego dany strumień odpadów, w celu ułatwienia specyficznego przetwarzania, obejmuje jedynie odpady charakteryzujące się takimi samymi właściwościami i takimi samymi cechami;
- magazynowanie (wstępne przez ich wytwórcę, tymczasowe przez prowadzącego zbieranie, magazynowanie zasadnicze przez prowadzącego przetwarzanie odpadów);
- odzysk, którego głównym wynikiem jest to, aby odpady służyły użytecznemu zastosowaniu przez zastąpienie innych materiałów – w przeciwnym przypadku zostałyby one użyte do spełnienia danej funkcji, lub w wyniku którego odpady są przygotowywane do spełnienia takiej funkcji w danym zakładzie lub ogólnie w gospodarce;

²⁴¹ Por. D. Kiperska-Moroń, S. Krzyżaniak, *Logistyka*. Biblioteka Logistyka, Poznań 2009, s. 435.

²⁴² Por. Z. Korzeń, *Ekologistyka*, Biblioteka Logistyka, Poznań 2001, ss. 18-19.

²⁴³ Ustawy z dnia 14 grudnia 2012 r. o odpadach, art. 3.



Rys. 4.3. Model sieci ekologicznej

Źródło: opracowanie własne.

- odzysk energii, termiczne przekształcanie odpadów w celu odzyskania energii;
- recykling, odzysk, który polega na powtórnym przetwarzaniu substancji lub materiałów zawartych w odpadach w procesie produkcyjnym w celu uzyskania substancji lub materiału o przeznaczeniu pierwotnym lub o innym przeznaczeniu, w tym też recykling organiczny, z wyjątkiem odzysku energii;
- przetwarzanie, tj. odzysk lub unieszkodliwianie, w tym przygotowanie poprzedzające odzysk lub unieszkodliwianie;
- spalanie odpadów przez ich utlenianie w specjalnie wybudowanych spalarniach;
- unieszkodliwianie odpadów – rozumie się przez to proces niebędący odzyskiem, nawet jeżeli wtórnym skutkiem takiego procesu jest odzysk substancji lub energii.

Należy zaznaczyć, że ekologia przede wszystkim wspiera działania zapobiegające powstawaniu odpadów, a później dopiero przygotowania do ponownego użycia, recykling, inne procesy odzysku oraz unieszkodliwianie.

Zatem możemy podsumować, że ekologia przede wszystkim selektywne zbieranie, transport, magazynowanie, składowanie, recykling, unieszkodliwianie, sprzedaż i spalanie odpadów.

Ekologia w połączeniu z procesami logistycznymi tworzy sieć ekologii (rys. 4.3), w której możemy wyróżnić trzy poziomy:

- pierwszy: zaopatrzenie, produkcję, dystrybucję (podsystemy w przedsiębiorstwach produkcyjno-usługowych), detalistów oraz aglomeracje wytwarzające odpady komunalne – ogólnie są to wytwórcy odpadów²⁴⁴;
- drugi: selektywne zbieranie, magazynowanie, składowanie – wspierane środkami transportu;
- trzeci: procesy odzysku²⁴⁵ – (np. spalanie odpadów, odzysk energii, odpady zielone, unieszkodliwianie odpadów, segregacja, sprzedaż odpadów, recykling, termiczne przekształcenie odpadów).

²⁴⁴ Wytwórcy odpadów – rozumie się przez to każdego, którego działalność lub bytowanie powoduje powstawanie odpadów (pierwotny wytwórca odpadów) oraz każdego, kto przeprowadza wstępną obróbkę, mieszanie lub inne działania powodujące zmianę charakteru lub składu tych odpadów; wytwórcę odpadów powstających w wyniku świadczenia usług w zakresie budowy, rozbioru, remontu obiektów, czyszczenia zbiorników lub urządzeń oraz sprzątnięcia, konserwacji i napraw jest podmiot, który świadczy usługę, chyba że umowa o świadczenie usługi stanowi inaczej, wg Ustawy z dnia 14 grudnia 2012 r. o odpadach, art. 3.

²⁴⁵ Odzysk – rozumie się przez to jakikolwiek proces, którego głównym wynikiem jest to, aby odpady służyły użytecznemu zastosowaniu przez zastąpienie innych materiałów, które w przeciwnym przypadku zostałyby użyte do spełnienia danej funkcji, lub w wyniku, którego odpady są przygotowywane do spełnienia takiej funkcji w danym zakładzie lub ogólnie w gospodarce, wg Ustawy z dnia 14 grudnia 2012 r. o odpadach, art. 3.

5. TECHNOLOGIE WSPOMAGANIA ZARZĄDZANIA BEZPIECZEŃSTWEM SYSTEMÓW LOGISTYCZNYCH

Zarządzanie bezpieczeństwem logistyki na potrzeby bezpieczeństwa gospodarczego to nie tylko teoria, ale i praktyka, która sprowadza się między innymi do wdrożenia nowoczesnych rozwiązań ułatwiających zapobieganie, przygotowanie, reagowanie na zagrożenia procesów logistycznych realizowanych na rzecz podmiotów (instytucji) bezpieczeństwa. Tymi narzędziami są systemy informatyczne oparte o technologie internetowe. Pozwalają one prognozować i określać miejsce składowania zapasów, planować potrzeby materiałowe, dobierać transport, trasę przejazdu, obniżyć koszty, zarządzać infrastrukturą (w tym magazynową) i środkami trwałymi, co usprawnia realizację przedsięwzięć na rzecz podmiotów bezpieczeństwa. Niezwykle pomocnym narzędziem w optymalizacji i skuteczności procesów logistycznych realizowanych na rzecz bezpieczeństwa gospodarczego jest automatyczna identyfikacja, która pozwala w trybie on-line śledzić wyroby (części, komponenty) – co, ile, i gdzie mamy składowane, zabezpieczać krytyczną infrastrukturę, w tym dostęp do budynków oraz systemów, w tworzeniu nowych poziomów bezpieczeństwa dla konsumentów w sektorze bankowym i zróżnicowanych usług opartych na szybkim oraz skutecznym uwierzytelnianiu klienta w miejscu użytkowania. Nie bez znaczenia w dzisiejszych czasach dla bezpieczeństwa gospodarczego są: jakość, odporność na zakłócenia, użyteczność i terminowość informacji.

5.1. Informatyczne wspomaganie

Do zbioru determinantów bezpieczeństwa gospodarczego zliczamy szeroko rozumiany *postęp cywilizacyjny*²⁴⁶. Wiodącymi czynnikami tego postępu są technika i technologia, które to przyczyniają się do powstawania coraz to lepszych rozwiązań i nowych produktów. Niektóre z nich mogą być pomocne w zarządzaniu bezpieczeństwem systemów logistycznych działających na korzyść podmiotów bezpieczeństwa. Do nich możemy zaliczyć programy informatyczne.

Programy te, wykorzystywane w systemach logistycznych, można podzielić na trzy kategorie: uniwersalne (moduł obsługujący konkretny proces logistyczny lub systemy wielomodułowe dla określonych ogniw w relacji dostawca – odbiorca), specjalizowane (przeznaczone np. dla procesów integrujących łańcuch), pomocnicze (wspomagające pracę różnych działów firmy, a także

²⁴⁶ Szerzej w podrozdziale 1.3 – *Determinanty i funkcje zarządzania bezpieczeństwem gospodarczym*.

zarządzające dokumentami, kontaktami z klientami, ułatwiające obliczanie kosztów logistycznych²⁴⁷).

Programy informatyczne w logistyce nie tylko ułatwiają planowanie procesów, ale także dostarczają niezbędnych danych w trybie on-line, do podejmowania decyzji, w przypadku wystąpienia zakłóceń w przepływie strumienia rzeczowego.

W praktyce można spotkać typowe systemy informatyczne wspomagające procesy logistyczne. Do nich możemy zaliczyć systemy: efektywnej obsługi konsumenta (ECR – *Efficient Consumer Response*), zarządzania relacjami z klientem (CRM – *Consumer Relationship Management*), zarządzania łańcuchem dostaw (SCM – *Supply Chain Management*), planowania zasobów dystrybucji (DRP – *Distribution Resources Planning*), łączący funkcje kalendarzowe i bazy danych (CM – *Contact Management*), zarządzania magazynem (WMS – *Warehousing Management System*), zarządzania transportem (TMS – *Transport Management System*), planowania potrzeb logistycznych (LRP – *Logistics Requirements Planing*), zarządzania środkami trwałymi (EAM – *Enterprise Asset Management*).

Do systemów wspomagających również zarządzania logistyczne należą systemy i niektóre moduły takich rozwiązań, jak: planowania potrzeb materiałowych (MRP – *Materials Requirement Planning*), planowania zasobów produkcyjnych (MRP II – *Manufacturing Resources Planning*), zarządzania zasobami przedsiębiorstwa (ERP – *Enterprise Resource Planning*), pozwalające wykonywać złożone operacje planistyczne i symulacyjne wraz z optymalizacją (APS – *Advanced Planning System*).

Identyfikacja systemów informatycznych wykorzystywanych w systemach logistycznych wskazuje, że producenci systemów coraz większą wagę przywiązują do budowy skalowalnych aplikacji, czyli takich, które będą „rosły” wraz z długością i pojemnością łańcucha dostaw. Zazwyczaj proponują swoim klientom nową aplikację, zewnętrznie bardzo podobną do oferowanej dotychczas, ale znacznie rozbudowaną funkcjonalnie, wykorzystującą nowoczesną, wydajną bazę danych. Dzięki temu uczestnicy łańcucha dostaw decydujący się na zakup i wdrożenie programu odpowiedniego do aktualnej sytuacji, mogą w przyszłości łatwo wymienić oprogramowanie, gdy tylko jego potrzeby wzrosną²⁴⁸.

Nowy program jest zbliżony w obsłudze, korzystający z niego pracownicy nie muszą się więc uczyć go od nowa. Ponadto znacznie skraca się czas i obniżają koszty wdrożenia systemu. Ważną tendencją w systemach wspoma-

²⁴⁷ Por. J. Szoltysek, *Typologia obszarów stosowania logistyki – propozycja rozwiązania*, [w:] *Gospodarka Materiałowa i Logistyka*, 2010/8, ss. 2-6.

²⁴⁸ Zob. Harry K.H. Chow, K.L. Choy, W.B. Lee, Felix T.S. Chan, *Design of a knowledge-based logistics strategy system, Expert Systems with Applications*, Volume 29, Issue 2, August 2005, pp. 272-290.

gających zarządzanie przedsiębiorstwem jest systematycznie wzrastająca ich elastyczność. Nowoczesne oprogramowanie można coraz łatwiej modyfikować.

Wyniki prowadzonych badań wskazały, że warunkami koniecznymi informatycznej integracji w obrębie wielonarodowych i kooperatywnych łańcuchów dostaw są²⁴⁹: technologie informatyczne istniejące w przedsiębiorstwach i łańcuchach dostaw, jednolity standard identyfikacyjny, automatyczna identyfikacja, elektroniczna komunikacja, w tym elektroniczna wymiana danych, zintegrowany system informatyczny, zabezpieczenie przepływających informacji przed ingerencją osób nieupoważnionych oraz zagwarantowanie ich wiarygodności²⁵⁰.

Warunkiem zbudowania sieci powiązań zewnętrznych firm w ramach łańcucha dostaw, na co wskazują także wyniki badań własnych, jest posiadanie przez nie odpowiedniej klasy systemów informatycznych. Powinny to być systemy klasy ERP, dające możliwość rozszerzenia prowadzenia działalności o e-biznes, a więc rozwiązania ERP II, które uwzględniają także zewnętrzne elementy środowiska biznesowego. 70% firm zachodnich i większość członków NATO (Niemcy, Turcja, USA, Kanada, Wielka Brytania, Hiszpania, Portugalia, Francja, Włochy, Holandia i inne) stosuje systemy informatyczne klasy ERP, co utwierdza, że w firmach polskich powinny być wdrażane systemy informatyczne tej klasy²⁵¹.

Kompleksowa integracja systemów informatycznych może być realizowana według różnych strategii zależnych od rodzaju prowadzonego biznesu. Celem takiej integracji jest optymalizacja całego łańcucha dostaw, a następnie poszczególnych uczestników. Spełnienie tego warunku wymaga, aby system informacyjny zapewniał: możliwość pozyskiwania informacji w każdym żądanym miejscu przepływu wzdłuż łańcucha logistycznego, dostępność informacji dla wszystkich współpracujących partnerów, dokładność informacji, zadowalającą szybkość przepływu informacji i jej aktualność, możliwość przetwarzania informacji dla wspierania procesu decyzyjnego, możliwość automatyzowania czynności związanych z wytwarzaniem, pozyskiwaniem i przetwarzaniem informacji oraz podejmowaniem decyzji²⁵².

²⁴⁹ Por. A. Szymonik, *Technologie informatyczne w logistyce*, Difin, Warszawa 2010, s. 102.

²⁵⁰ Zob. P. Edwards, M. Peters, G. Sharman, *The effectiveness of information systems in supporting the extended supply chain*, Journal of Business Logistics Volume 22, 2001, Issue 1, pp. 1-27.

²⁵¹ Tamże, s. 103.

²⁵² Por. X. Zhu, X. Li, Q. Yao, Y. Chen, *Challenges and models in supporting logistics system design for dedicated-biomass-based bioenergy industry*, Bioresource Technology, Volume 102, Issue 2, 2011, pp. 1344-1351; M. Jedynak, *Efektywność systemów logistycznych*, [w:] Zeszyty Naukowe Uniwersytetu Szczecińskiego, Finanse. Rynki finansowe. Ubezpieczenia 2008/14, ss. 51-56.

System efektywnej obsługi odbiorcy (klienta) ECR

ECR – (*Efficient Consumer Response*), łańcuch dostaw zorientowany na klienta, odbiorcę. ECR to nowoczesna strategia obsługi łańcucha dostaw na bazie partnerstwa jego uczestników, polegająca na zsynchronizowanym zarządzaniu popytą i popytem przy zaangażowaniu technologii wspomagających przepływ produktów, informacji i środków finansowych, w celu podnoszenia konkurencyjności całego łańcucha dostaw oraz maksymalizacji korzyści wszystkich uczestników łańcucha przy wzroście zadowolenia ostatecznego odbiorcy²⁵³.

Wspólne dążenie do maksymalizowania wydajności całego łańcucha, zamiast tradycyjnego koncentrowania się na wydajności poszczególnych jego ogniw, prowadzi do zmniejszenia kosztów całkowitych systemu, poziomu zapasów i zaangażowanego kapitału, przy jednoczesnym podniesieniu wartości dla ostatecznego klienta.

Ich działania skupiają się na stosowaniu nowoczesnych metod zarządzania i środków technicznych w celu skrócenia czasu wędrowki produktu od linii produkcyjnej (magazynu, dystrybutora) do odbiorcy oraz obniżenia kosztów. W wyniku tych działań klient otrzymuje propozycję, którą jest skłonny zaakceptować przy zadowalającym go poziomie obsługi.

W praktyce koncepcja ECR stanowi podstawę budowania nowoczesnej strategii zarządzania łańcuchem dostaw, według której producenci, dystrybutorzy, detaliści i dostawcy usług (logistycznych, informatycznych, badawczych) współpracują ze sobą w celu lepszego, szybszego i bardziej efektywnego zaspokojenia potrzeb odbiorcy.

Wspólne dążenie do maksymalizowania wydajności całego łańcucha wartości, zamiast tradycyjnego koncentrowania się na wydajności poszczególnych jego ogniw, prowadzi do zmniejszenia kosztów całkowitych systemu, poziomu zapasów i zaangażowanego kapitału, przy jednoczesnym podniesieniu wartości dla ostatecznego odbiorcy.

Realizacja strategii ECR zakłada wykorzystanie nowoczesnych metod zarządzania i nowych technologii w celu skrócenia czasu wędrowki produktu od linii produkcyjnej (magazynu, dystrybutora) do odbiorcy.

Koncepcja ECR wspiera się na trzech filarach²⁵⁴: zapewnienie wymaganego poziomu obsługi, eliminacja kosztów, które nie dodają wartości, maksymalizacja efektów i eliminacja barier w całym łańcuchu dostaw.

²⁵³ Por. A. Baraniecka, *ECR Efficient Consumer Response, Łańcuch dostaw zorientowany na klienta*, IliM, Poznań 2004, s. 22; A. Rushton, P. Croucher, P. Baker, *Handbook of Logistics and Distribution Management (4th Edition)*, Kogan Page Publishers, 2010, s. 203.

²⁵⁴ Por. *ECR w praktyce*, ecr.pl, 17.01.2015.

System zarządzania relacjami z klientem CRM

Jednym z systemów wspomagających działalność firmy (dystrybutora, magazynu itp.) jest system zarządzania relacjami z klientami (*Customer Relationship Management* – CRM). Do funkcji systemów CRM zaliczamy²⁵⁵: gromadzenie i przetwarzanie danych archiwalnych dotyczących współpracy z odbiorcą, kontaktów, zleceń, zamówień, działalności przedstawicieli handlowych i pracowników będących w bezpośrednim kontakcie z odbiorcą; automatyzację organizacji i kierowania dostawą; konfigurowanie zleceń (produktów) na indywidualne życzenie klienta – systemy CRM wspomagają pośredników w miejscu sprzedaży i umożliwiają zestawienie wybranych elementów produktów i usług; przygotowanie ofert; wyszukiwanie odpowiednich danych; sporządzanie analiz i prognoz dotyczących sprzedaży i rynku; zarządzanie działami wsparcia technicznego i telefonicznymi punktami obsługi klienta (*call center*); dbanie o klienta, odbiorcę obsługiwanego (obsługa serwisu i ewentualnych reklamacji, wsparcie techniczne); komunikacja z rynkiem – poszukiwanie kontaktów z partnerami handlowymi; administracja – dzienna organizacja zadań (terminy, kontakty, raportowanie, prezentacje).

Oprogramowanie CRM składa się z 3 elementów (rys. 5.1)²⁵⁶: operacyjnego CRM (służy do konsolidacji danych o kliencie, odbiorcy – jego potrzebach, zachowaniach czy historii współpracy); komunikacyjnego CRM (obejmuje wyłącznie rozwiązania wspomagające kontakt z klientem, odbiorcą), analitycznego CRM (pomaga zrozumieć działania klienta, odbiorcy, podejmowane podczas kontaktu z organizacją, realizuje wszystkie procesy kontaktu z klientem, odbiorcą oraz wszystkie inne zachodzące w organizacji, mające jakiegokolwiek znaczenie z punktu widzenia klienta, odbiorcy).

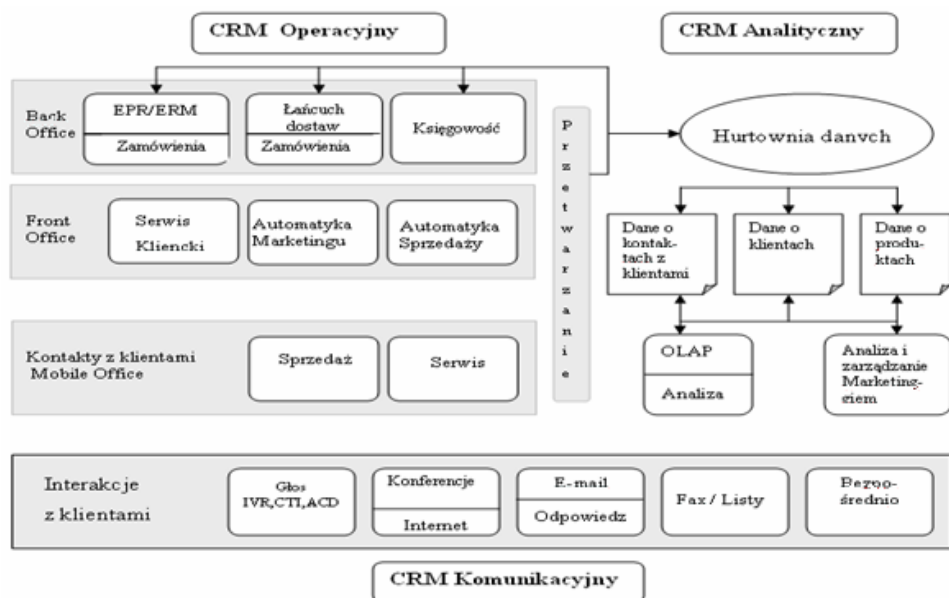
CRM rozwinięty o nowe technologie internetowe, tzw. e-CRM, pozwolił na rozszerzenie zakresu zarządzania relacjami z klientem, odbiorcą o sieć Internet oraz ograniczanie kosztów z tym związanych²⁵⁷.

Nie tylko w tradycyjnej gospodarce klient jest w centrum zainteresowania. Sieciowy CRM, tak jak tradycyjny, jest zorientowany na klienta, pełni te same funkcje, chociaż wymaga odrębnych zasad postępowania, innej technologii. Zmienił się całkowicie sposób obsługi klienta.

²⁵⁵ Zob. *Wstęp do informatyki...*, op. cit., s. 444; K. Halicka, *Wykorzystanie systemów CRM w logistyce obsługi klienta*, [w:] *Ekonomia i Zarządzanie*, nr 4, 2010, ss. 49-59.

²⁵⁶ Por. A. Lotko, *Zarządzanie relacjami z klientem*, Politechnika Radomska, Radom 2003, s. 67.

²⁵⁷ Zob. A. Szymonik, *Informatyka dla potrzeb logistyka (i)*, Difin, Warszawa 2015, s. 76.



IVR (*Interactive Voice Response*) – nazwa systemu, umożliwiającego interaktywną obsługę osoby dzwoniącej,
 CTI (*Computer Telephony Integration*) – system integrujący telefon sieci publicznej z komputerem,
 ACD – automatyczna dystrybucja połączeń, rozdziela dane automatycznie połączenia przychodzące pomiędzy dostępnymi w danym momencie agentami, przypisanymi i wyszkolonymi do obsługi np. infolinii,
 OLAP (*On-Line Analytical Processing*) – efektywna technologia przetwarzania danych analitycznych.

Rys. 5.1. Architektura CRM

Źródło: J. Stasieńko, *Sytem informatyczny wspomagający zarządzanie relacjami z klientami*, s. 228, <http://kis.pwszchelm.pl/publikacje/V/Stasienko.pdf>, 24.08.2014.

System zarządzania łańcuchem dostaw SCM

Zarządzanie łańcuchem dostaw SCM (*Supply Chain Management*) – rozwiązania informatyczne, które służą przedsiębiorstwu, podmiotowi bezpieczeństwa do zarządzania sieciowym łańcuchem dostaw. Wewnętrzne SCM obejmuje zagadnienia związane z zaopatrzeniem, produkcją i dystrybucją. Zewnętrzne SCM integruje przedsiębiorstwo, podmiot bezpieczeństwa z jego dostawcami i klientami²⁵⁸.

²⁵⁸ Zob. S.L., David, X. Chen, J. Bramel, *The Logic of Logistics: Theory, Algorithms, and Applications for Logistics and Supply Chain Management*, 2nd ed. New York, NY: Springer, 2004.

Rozwiązania SCM wykorzystuje się przede wszystkim w fazie projektowania produktu, wyboru źródeł zaopatrzenia, przewidywania popytu na wyroby oraz sterowania ich dystrybucją. Zawierają bowiem specjalistyczne narzędzia, które umożliwiają nadzór nad poszczególnymi działaniami logistycznymi firmy.

Podsumowując, należy stwierdzić, że model zarządzania łańcuchem dostaw opiera się na ośmiu wzajemnie uzupełniających się procesach biznesowych, które są wspierane narzędziami informatycznymi²⁵⁹: zarządzanie relacjami z klientem, zarządzanie obsługą klienta, zarządzanie popytem, realizacja zamówień, zarządzanie przepływami produkcyjnymi, zarządzanie relacjami z dostawcami, rozwój i sprzedaż produktu, zarządzanie reklamacjami.

System zarządzania łańcuchem dostaw pozwala na opracowanie przejrzystych zasad kooperacji między organizmami (instytucjami), podmiotami bezpieczeństwa uczestniczącymi w procesie produkcji i dystrybucji towarów²⁶⁰.

Wydajność całości przedsiębiorstwa, podmiotu bezpieczeństwa nie jest rozpatrywana jedynie z punktu widzenia globalnej różnicy przychodów i kosztów, ale również zaspokojenia potrzeb potrzebujących. Optymalizowana jest również efektywność wytwarzania i dystrybucji każdego produktu, ewentualnie kanału dystrybucji produktu lub zaopatrzenia w materiały.

Należy już na wstępie zaznaczyć, że nie można wdrożyć SCM bez opanowania produkcji, gospodarki magazynowej i własnej gospodarki materiałowej, jednym słowem, bez wdrożenia systemu zarządzania zasobami przedsiębiorstwa (ERP). Tak więc, dzięki metodzie SCM, firmy, podmioty bezpieczeństwa uzyskały narzędzie do zarządzania nie tylko tym, co dzieje się wewnątrz ich organizmu, lecz także na zewnątrz. Dzięki SCM można zarządzać nie tylko procesami w samej instytucji, podmiocie bezpieczeństwa, lecz także poza nią w łańcuchu dostaw.

Podczas implementacji SCM w bardziej szczegółowy sposób traktowane są funkcje planowania i realizacji łańcucha dostaw. SCM umożliwia opracowanie modelu całej sieci dostaw oraz wszystkich jej ograniczeń. Następnie za pomocą tego modelu można zsynchronizować działania i zaplanować przepływ materiałów w całym łańcuchu dostaw. Na tej podstawie dostosowuje się podaż do popytu oraz tworzy możliwe do realizacji plany związane z zaopatrzeniem, produkcją, zapasami i transportem.

W planowaniu SCM uwzględnia się wiele lokalizacji, ich wzajemne zależności, globalny łańcuch logistyczny i partnerów danej firmy, podmiotu bezpieczeństwa. Proces współpracy na skalę globalną jest nowością dla większych firm, podmiotów bezpieczeństwa i wymaga wprowadzenia zmian organizacyjnych.

²⁵⁹ Por. *Strategie łańcuchów dostaw*, red. nauk. M. Ciesielski, J. Długosz, PWE, Warszawa 2010, s. 25.

²⁶⁰ Zob. J. Majewski, *Informatyka dla logistyki*, ILiM, Poznań 2002, s. 60.

Obejmuje nie tylko realizację, ale i planowanie strategiczne, taktyczne oraz operacyjne. W rezultacie SCM ma wpływ na procesy biznesowe nawet na najniższym poziomie.

Planowanie w czasie rzeczywistym, zaawansowane metody symulacji i możliwości optymalizacji za pomocą SCM gwarantują całkowicie nowy przepływ procesów, inny niż w przypadku systemu ERP. Użytkownicy SCM muszą więc gruntownie zapoznać się z funkcjonowaniem całego łańcucha dostaw.

System planowania zasobów dystrybucji DRP

Metoda DRP (*DRP – Distribution²⁶¹ Resources Planning*) jest definiowana jako system określający popyt na zapasy w poszczególnych centrach dystrybucji przedsiębiorstwa, podmiotu bezpieczeństwa²⁶².

Gromadzi on informacje na temat tegoż popytu, przekazuje je do produkcji i systemu materiałowego.

Prognozowanie rozpoczyna się od najniższego szczebla kanału dystrybucji, a więc np. magazynu. Poprzez sumowanie harmonogramów potrzeb niższych szczebli uzyskuje się ilościowy rozkład popytu dla ogniw położonych wyżej w strukturze. Ten typ planowania pozwala na sporządzenie dość dokładnych prognoz popytu, jak również zaplanowanie właściwego poziomu zapasów i miejsca ich składowania w ramach wszystkich ogniw zintegrowanego łańcucha.

Metoda DRP stanowi zwierciadlane odbicie MRP (*Material Requirements Planning*), wykorzystuje też te same co MRP zasady operacyjne²⁶³: rozkład czasowy zapotrzebowania w obrębie systemu dystrybucji firmy, potrzeby brutto, które wynikają z zapotrzebowania na wyrób finalny, potrzeby netto dla otwartych zamówień, czyli rzeczywiste potrzeby w danym okresie (po uwzględnieniu posiadanych zapasów i dostaw w drodze), składanie zamówień uzupełniających w sytuacji występowania rzeczywistej potrzeby (na poziomie równym potrzebom netto lub określonym przez producenta), synchronizacja zapotrzebowania, która dotyczy precyzyjnego określenia terminu złożenia zamówienia na konkretną ilość wyrobu (znając czas realizacji zamówienia przez dany magazyn oraz długość cyklu produkcyjnego produktu).

Dane dotyczące popytu są przekazywane do systemu informacyjnego obsługującego produkcję oraz do systemu planowania potrzeb materiałowych (systemy MRP).

²⁶¹ Por. A. Langevin, D. Riopel, *Logistics Systems: Design and Optimization*, Springer, 2005, s. 85.

²⁶² Zob. *Logistyka dystrybucji*, pod red. K. Rutkowskiego, Difin, Warszawa 2001, s. 159.

²⁶³ Por. *Logistyka w przedsiębiorstwie, przewodnik do ćwiczeń*, pod red. G. Radziejowskiej, Gliwice 2001, s. 53.

Prognozowanie zapotrzebowania rozpoczyna się od najniższego ogniwa w kanale dystrybucji (np. podmiotu bezpieczeństwa). Potrzeby niższych szczebli zostają zsumowane, uzyskując tym samym wielkość popytu w ujęciu ilościowym dla ogniwa występujących wyżej w hierarchii.

Zastosowanie przedstawionego systemu, poza znaczną precyzją w prognozowaniu popytu, zapewnia również zaplanowanie właściwego poziomu i miejsca składowania zapasów w obrębie całego zintegrowanego łańcucha dystrybucji. Zsumowane wielkości popytu z poszczególnych centrów dystrybucyjnych, określone samodzielnie lub przez klientów, odbiorców dla przyjętych okresów w przyszłości, tworzą harmonogram popytu na zapasy i są przekazywane do ogniwa w łańcuchu, które zajmuje się produkcją. Po porównaniu z przygotowanymi uprzednio przewidywaniami, dotyczącymi wielkości produkcji, dokonuje się niezbędnych dostosowań przy równoczesnym uwzględnieniu potrzeb odbiorców i ograniczonych zdolności produkcyjnych. Na tej podstawie możliwe jest opracowanie planów produkcji i zarazem planów zapotrzebowania materiałowego.

Opracowywany jest również plan dystrybucji obrazujący rozkład dostaw do poszczególnych ogniwa dystrybucyjnych zgodnie ze zgłaszanym przez nie zapotrzebowaniem.

System zarządzania magazynem WMS

Magazynowy system informatyczny WMS (*Warehouse Management System*) – program informatyczny do zarządzania strumieniem rzeczowym w magazynach, centrach dystrybucji, zwany potocznie przez logistyków systemem do obsługi magazynu wysokiego składu. Wspomaga on realizację, kontrolę i sterowanie przepływem przez magazyn oraz dostarcza informacji o tym przepływie i tworzenie dokumentacji towarzyszącej temu przepływowi²⁶⁴.

Rozwiązania WMS nierzadko mają budowę modułową. Ich podstawą jest program główny, który odpowiada za takie aspekty, jak zarządzanie składowaniem czy zarządzanie towarami. W kwestii architektury WMS istotne są moduły mające za zadanie określanie maszyn składających. Na główne moduły systemów *Warehouse Management System* składają się takie elementy, jak²⁶⁵: obsługa dostaw, nadzór wejściowy, obsługa wysyłek, nadzór wyjściowy, wspomaganie spedycji, zmiany wewnątrz magazynu, inwentaryzacja, raporty,

²⁶⁴ Por. *Słownik terminologii logistycznej*, red. nauk. M. Fertsch, ILiM, Poznań 2006, s. 99; A. Ramaa, K.N. Subramanya, T.M. Rangaswamy, *Impact of Warehouse Management System in a Supply Chain*, [w:] *International Journal of Computer Applications* (0975 – 8887), Volume 54, No. 1, September 2012.

²⁶⁵ Por. I. Pisz, T. Sęk, W. Zielecki, *Logistyka w przedsiębiorstwie*, PWE, Warszawa 2013, s. 237, 238; J. Majewski, *Informatyka dla logistyka*, ILiM, Poznań 2002, s. 69 i następane.

konfekcjonowanie, klasyfikacja towarów wg metod ABC oraz XYZ, co pozwala na zarządzanie miejscem w magazynie i przyspiesza operacje wejścia/wyjścia.

Systemy WMS posiadają szereg funkcji, składających się na ich specyfikę i trafnie opisujących mechanizm ich działania.

Będzie to między innymi²⁶⁶: maksymalne wykorzystanie miejsca w magazynie, redukcja czasu poświęconego na wykonywanie działań dotyczących dostarczania i zamawiania towarów, podniesienie obrotu zapasów oraz aktywów, udoskonalenie jakości usług wykonywanych przez producentów, redukcja możliwych do popełnienia błędów, dzięki zaawansowanej kontroli i szybkiemu rozwiązywaniu ewentualnych problemów pomiędzy producentami i dostawcami, duża elastyczność i mobilność wymiany danych z systemem, ułatwiony dostęp do danych, całkowity nadzór nad zamówieniami, możliwość zarządzania ruchem magazynowym, ułatwienie tworzenia dokumentacji w zakresie przygotowania towarów do wysyłki oraz automatyzacja tego procesu, możliwość wykorzystania technologii kodów kreskowych lub RFID, za pomocą których są znakowane towary i jednostki logistyczne, możliwość zapisywania stanów magazynowych wg określonych lokalizacji, partii czy dat przydatności, automatyzacja procesu inwentaryzacji.

W firmach świadczących usługi logistyczne systemy WMS stanowią często technologię wspierającą działanie systemu zarządzającego klasy ERP. Pomiędzy tymi systemami powinna funkcjonować sprawna wymiana danych, oparta na ujednoczonych standardach przekazywania informacji. Nowe klasy oprogramowania zapewniają zwykle obsługę zróżnicowanych danych w poszczególnych podsystemach informatycznych przedsiębiorstw i swobodne przenoszenie ich z modułu do modułu. To z kolei pozwala na całkowite automatyzowanie ruchu produktów w magazynach z wykorzystaniem oprogramowania WMS.

Niektórzy dostawcy systemów ERP oferują funkcjonalność WMS jako jeden z modułów integralnie wbudowanych w pakiet ERP lub obsługują ją częściowo w ramach modułów gospodarki magazynowej.

System zarządzania transportem TMS

System zarządzania transportem TMS (*Transportation Management System*) to oprogramowanie, które pozwala przewoźnikom branży TSL na przetwarzanie w formie elektronicznej danych niezbędnych do efektywnego zarządzania transportem²⁶⁷.

System TMS współpracuje z system zarządzania flotą FMS, który odpowiada za przetwarzanie danych, takich jak informacje o stanie pojazdu, czasie jazdy i odpoczynku, czasie załadunku i rozładunku, czasie obsługi

²⁶⁶ Por. A. Szymonik, *Informatyka dla...*, op. cit., s. 82 i 83.

²⁶⁷ Zob. M. Verwijmeren, *Software component architecture in supply chain management*, [w:] *Computers in Industry*, Volume 53, Issue 2, February 2004, ss. 165-178.

serwisowej, zachowaniu się kierowcy na drodze bądź stopniu i stanie załadunku lub rozładunku. Sercem systemu FMS jest otwarta struktura baz danych. Za zbieranie niezbędnych informacji na temat kierowcy, pojazdu i ładunku odpowiada komputer pokładowy²⁶⁸.

Główne funkcje realizowane przez TMS, przy współudziale FMS²⁶⁹: optymalizacja dostaw poprzez: konsolidację zamówień, planowanie transportu i dostaw, zarządzanie kierowcami, flotą pojazdów i dostawcami usług transportowych, monitoring zdarzeń transportowych, obsługa nietypowych zleceń spedycyjnych, dzięki funkcji definiowania cech dla różnych branż, według indywidualnych potrzeb, pełna obsługa zamówień w łańcuchu dostaw; obsługa umów dotyczących zadań transportowych oraz floty transportowej, przygotowanie analiz i raportów, możliwość definiowania przez użytkownika cenników na usługi transportowe oraz rozliczanie usług transportowych, raportowanie kosztów transportu, selekcjonowanie przewoźników, w tym najbardziej popularnych, i optymalizowanie tras na podstawie wydruków porównawczych kosztów, łatwa integracja z systemami nadrzędnymi ERP/WMS, wybór dostępnych samochodów (domyślnie wszystkie), wybór zamówień (domyślnie wszystkie na dany dzień), długość rozładunku (globalnie lub dla klienta), maksymalna ilość postojowych punktów na trasie, maksymalny czas pracy kierowcy i tolerancja przekroczenia czasu pracy, maksymalna ładowność pojazdów i tolerancja przekroczenia ładowności pojazdu.

System przechowuje i ostrzega o upływie terminów związanych m.in. z ubezpieczeniem OC, AC, NW, przeglądami technicznymi i gwarancyjnymi, datą legalizacji tachografu, zdarzeniami, np. wymianą opon itp., ważnością dokumentów.

Planowanie potrzeb logistycznych LRP

LRP (ang. *Logistic Resources Planning*) – system planowania potrzeb (zasobów) logistycznych integruje funkcje modułów MRP i DRP, ponieważ dostarczane w ich obrębie informacje wzajemnie się dopełniają. Zastosowanie takiego rozwiązania wynika z tendencji charakteryzujących nowoczesną logistykę, polegających na odstąpieniu od wykorzystywania metod optymalizacyjnych dla dużych ilości zapasów oraz zorientowania na eliminację tychże zapasów oraz skracanie cyklu realizacji zamówienia. Wśród podstawowych zalet stosowania LRP wyróżnia się możliwość obniżenia poziomu kosztów ponoszonych przez poszczególnych partnerów łańcucha

²⁶⁸ Por. A. Szymonik, *Informatyka...*, op. cit., s. 83.

²⁶⁹ Por. I. Pisz, I. Łapuńska, *Systemy transportowe wspomagające realizację projektów logistycznych w branży transport spedycja logistyka*, [w:] *Logistyka* 2013/5, s. 362 i następane.

dostaw, dzięki dokonywanym na bieżąco korektom prognoz popytu, co wpływa również na poprawę poziomu obsługi klientów²⁷⁰.

W systemie LRP dane obrazujące prognozę popytu w poszczególnych punktach sprzedaży z uwzględnieniem rozkładu czasowego zapotrzebowania w poszczególnych ogniwach sieci dystrybucyjnej są przekazywane w formie harmonogramu do firmy produkcyjnej. Znajduje tutaj zastosowanie moduł DRP. Wskazane dane są wykorzystywane na tym etapie do planowania potrzeb materiałowych na ustalony okres, co z kolei stanowi obszar zastosowania MRP. Moduł MRP umożliwia redukcję poziomu zapasów materiałowych do zapotrzebowania wynikającego z głównego harmonogramu produkcji, który powinien odzwierciedlać aktualny popyt rynkowy. W ten sposób równocześnie redukowane są poziom zapasów materiałowych oraz wielkość zapasów dystrybucyjnych²⁷¹.

System zarządzania środkami trwałymi EAM

Systemy EAM (*Enterprise Asset Management* – zarządzanie majątkiem firmy) służą wsparciu utrzymania ruchu w firmach produkcyjnych, zarządzania najemcami, umowami czy powierzchniami. Ich zadaniem jest także pomoc w nadzorowaniu długofalową wartością nieruchomości, a także zrównoważonym rozwojem czy też inicjatywami ekologicznymi²⁷².

Najogólniej można stwierdzić, że EAM ułatwia (rys. 5.2): prowadzenie ewidencji majątkiem, zarządzanie majątkiem, prowadzenie inwentaryzacji.

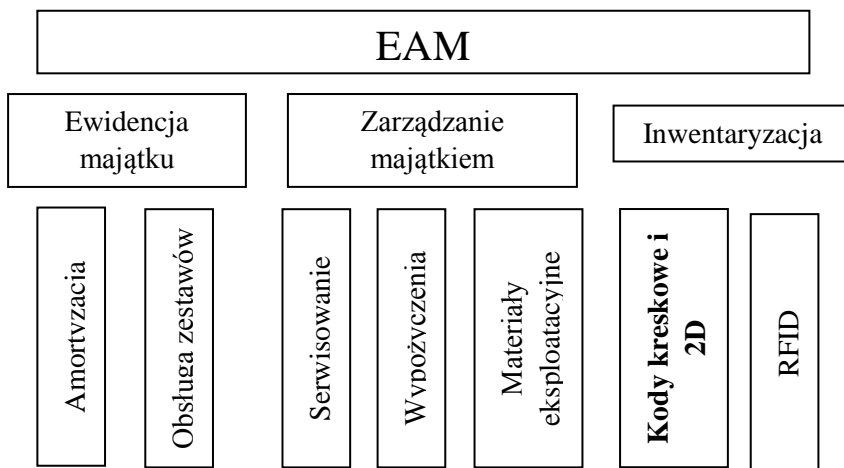
Systemy EAM mają przewagę nad modułami będącymi częściami składowymi systemu ERP, jako że one tylko pozwalają na ewidencję składników majątku oraz generowanie odpowiednich dokumentów, pomijając takie procesy, jak dalsza obsługa aktywów i inwentaryzacja majątku. Pobieżne traktowanie dwóch ostatnich elementów często może przyczyniać się do niewłaściwego wykorzystania posiadanych środków trwałych i wyposażenia, przynosząc tym samym straty w przedsiębiorstwie²⁷³.

²⁷⁰ Por. Yan-yan Li, W. Long, *The Integration Model of Supply Chain Resource Allocation: LRP*, *International Asia Conference on Industrial Engineering and Management Innovation (IEMI2012) Proceedings*, May 2013, ss. 1279-1285.

²⁷¹ Zob. A. Szymonik, *Zarządzanie dystrybucją*, WSOWL, Wrocław 2015, ss. 52-59.

²⁷² Por. A. Sinha, R.N. Lahiri, S. Chowdhury, S.P. Chowdhury, Y.H. Song, *Complete IT solution for Enterprise Asset Management (EAM) in Indian power utility business*, *Universities Power Engineering Conference*, 2007. UPEC 2007. 42nd International, 4-6 Sept. 2007, ss. 645-650.

²⁷³ Por. K. Jagodzińska, *Zarządzanie majątkiem przedsiębiorstwa – czy warto rozbudować posiadany system ERP?* <http://www.insoftconsulting.pl/>, 12.01.2015.



Rys. 5.2. Obszary odpowiedzialności EAM

Źródło: A. Szymonik, *Informatyka dla...*, op. cit., s. 86.

Najpopularniejszymi systemami EAM, które zostały wdrożone w firmach np. z branży metalowej są systemy producentów: IFS, SAP, Neuron oraz Junisoftex. Wykorzystuje się je w obszarach²⁷⁴: gospodarki zakupowej i magazynowej (do obsługi zapotrzebowań zakupów, dostępu do stanów magazynowych, np. części zamiennych czy materiałów eksploatacyjnych), zarządzania majątkiem ruchomym, w tym środkami trwałymi (rejestr, wyposażenie, koszty, lokalizacje, numery inwentarzowe), zarządzania powierzchniami lub najemcami (tj. powierzchniami, przypisaniem wyposażania i zasobów do powierzchni, lokali, najemców, umowami najmu, przeprowadzkami, optymalizacją powierzchni), obsługi zgłoszeń (np. incydentów, problemów, rezerwacji zasobów), zarządzania pojazdami (tj. rejestrem, danymi technicznymi, rejestrowymi, ubezpieczeniowymi, serwisem, wyposażeniem), zarządzania pracami planowanymi (np. pracami planowanymi – prewencyjnymi), utrzymania majątku, pracami konserwacyjnymi, umowami serwisowymi i organizacji.

5.2. Elektroniczna platforma logistyczna

Widoczny na przestrzeni ostatnich lat dynamiczny rozwój działalności przedsiębiorstw logistycznych, przewozowych oraz deweloperów, oferujących wciąż nowe lokalizacje i kolejne powierzchnie magazynowe o wysokim standardzie w Polsce i w Europie powoduje, iż coraz bardziej widoczna staje się

²⁷⁴ Zob. *Efektywne zarządzanie aktywami*, <http://www.4metal.pl>, 18.01.2015.

konieczność opracowania i wdrożenia instytucjonalnej formy zarządzania popytem i podażą usług logistycznych w skali międzynarodowej.

Tego typu narzędzie będzie niewątpliwie pomocne, gdy wystąpią duże potrzeby w związku ze stratami, szkodami, jakie wystąpiły po zdarzeniach kryzysowych.

Jednocześnie, wraz z rozwojem gospodarki i idącymi w ślad za tym zmianami koncepcji organizacji przedsiębiorstw, zmniejszyło się znaczenie hierarchicznych struktur wielu firm na rzecz struktur spłaszczonych; nieporównywalnie zwiększyła się zarazem automatyzacja systemu pracy i roli menedżerów.

Realizacja transakcji biznesowych aktualnie jest rozpatrywana z punktu widzenia podejścia procesowego, czyli jednej z najistotniejszych charakterystyk zorientowanego rynkowo zarządzania przedsiębiorstwem. Funkcjonowanie w praktyce takich struktur wymusza potrzebę poszukiwania nowych rozwiązań umożliwiających kompleksową obsługę wszystkich płaszczyzn współpracy partnerów gospodarczych, w tym podmiotów bezpieczeństwa, a szczególnie²⁷⁵: wymagań informacyjnych, wymagań standaryzacyjnych, zapotrzebowania na narzędzia i dokumenty, wymagań bezpieczeństwa, wymagań ochrony prawnej.

Próbą rozwiązania problemu w zakresie szeroko rozumianej logistyki jest stworzenie platformy elektronicznej, kojarzącej podmioty oferujące zarówno usługi, jak i informacje wspomagające działalność transportowo-logistyczno-magazynowo-spedycyjną z firmami szukającymi możliwości realizacji tego typu usług w określonym czasie i miejscu. Oferta takiej platformy byłaby udostępniana na określonych warunkach dostępowych w formie usługi o charakterze publicznym²⁷⁶.

Elektroniczna Europejska Platforma Logistyczna (EPL) świadczyłaby usługi specjalistyczne w zakresie organizacji, planowania, kontroli i realizacji transakcji w zakresie transportu, logistyki, magazynowania i dystrybucji oraz spedycji. Ponadto jej zadaniem byłoby udostępnianie wiedzy i informacji z szeroko rozumianego obszaru TSL (*Transport, Spedycja, Logistyka*), świadczenie usług wymiany danych i dokumentów, a także usług ASP (*Application Service Provider*), polegających na udostępnianiu za pośrednictwem Internetu dowolnego oprogramowania, w tym na przykład zintegrowanego systemu zarządzania przedsiębiorstwem klasy ERP, czy specjalistycznych programów optymalizacji planowania tras transportowych.

²⁷⁵ Por. E. Kulińska, *Wspomaganie zarządzania procesami logistycznymi – elementy metody ebXML*, [w:] *Komputerowo zintegrowane zarządzanie*, tom I, Wydawnictwa Naukowo-Techniczne, Warszawa 2005, s. 698.

²⁷⁶ Por. K. Kolińska, I. Jeleń, M. Cudziło, *Elektroniczna platforma logistyczna jako narzędzie wzbogacenia procesu edukacyjnego*, [w:] *Logistyka*, 2011/6, ss. 1669-1679; B. Śliwczyński, *Elektroniczna Platforma Logistyczna – internetowe środowisko pracy logistyka*, [w:] *Logistyka*, 2/2010, ss. 20-23.

Trzeba w tym miejscu zwrócić uwagę na fakt, iż automatyzacja procesów biznesowych jest dziś jednym z najważniejszych wyzwań dla firm. Jednakże poważną przeszkodą dla jej sprawnego funkcjonowania jest wykorzystywanie wielu różniących się znacznie od siebie rozwiązań informatycznych, zarówno przez usługodawców i producentów, jak i ich klientów. Kupujący są zainteresowani taką automatyzacją zamówień, dzięki której mogliby składać zamówienia jednocześnie do różnych dostawców w formie zunifikowanej, obejmującej określone, wspólne dla wszystkich standardy. Główną determinantą tych działań pozostawałaby oczywiście odpowiednia jakość i terminowość realizacji złożonego zamówienia za określoną cenę. W praktyce usługobiorcy przy wyborze dostawców najczęściej są zainteresowani wcześniejszym dostępem do ich katalogów informacyjnych dla zapewnienia spójnej specyfikacji produktowej, oznaczeń partii produktów itd. Z kolei sprzedawcy, chcąc dotrzeć do jak największej liczby odbiorców, starają się maksymalnie uprościć procedury zamawiania oferowanych produktów, zwłaszcza standardyzowanych, oferując zarazem możliwość śledzenia nadawanych przesyłek przez klientów. Dodatkowo w coraz większym stopniu wykorzystuje się koncepcję zarządzania zapasami²⁷⁷ odbiorcy, co umożliwia automatyczne generowanie zamówień w sytuacji, gdy poziom zapasu (produktu lub surowca) będzie mniejszy od poziomu minimalnego. Generalnie dostawcy dążą do ustanowienia maksymalnej liczby połączeń elektronicznych, aby uczestniczyć w jak największej ilości rynków elektronicznych.

Dzięki wykorzystaniu rozwiązań oferowanych przez współczesne technologie informacyjne i komunikacyjne (ICT – *Information and Communication Technologies*) w zakresie szeroko rozumianej logistyki i transportu, ale i wielu innych branż, wydaje się wręcz konieczne opracowanie i wdrożenie otwartej, elektronicznej platformy logistycznej o zasięgu międzynarodowym. Nabiera to szczególnego znaczenia w obecnej sytuacji, gdy mamy do czynienia z bardzo rozczłonkowanym rynkiem z wielością narzędzi i wersji informatycznych oraz informacyjnych, które z trudem mogą komunikować się między sobą, a dotychczasowe wysiłki w sprawie wprowadzenia ujednoczonych (ujednolicających się) modeli i standardów nie przyniosły szczególnych rezultatów ze względu na znaczne koszty ich przystosowania do wielu już istniejących rozwiązań.

²⁷⁷ Zarządzanie zapasami przez dostawcę (VMI – *Vendor Managed Inventory*) – sytuacja w której dostawcy monitorują poziom zapasów w magazynie swoich odbiorców, w oparciu o prognozy sprzedaży i dane sprzedażowe odbiorcy, utrzymując i rozwijając dostępność produktów w łańcuchu dostaw, *Słownik terminologii logistycznej*, ILiM, Poznań 2006, s. 247.

Wpływają na to również pewne ograniczenia, dotyczące tych rozwiązań²⁷⁸, jako że większość powstało, aby zaspokoić potrzeby firm prywatnych i ulepszyć ich organizację wewnętrzną. Rozwiązania te często są przystosowane do indywidualnych potrzeb pojedynczego przedsiębiorstwa i zwykle brakuje im funkcjonalności wsparcia współpracy między firmami. Kolejnym utrudnieniem jest fakt, iż znaczna ilość proponowanych aplikacji ICT jest związana z podażową częścią sektora logistycznego, czyli na przykład dość łatwo jest znaleźć narzędzie służące do zarządzania flotą lub planowania i monitorowania przewozów, zaś możliwości dotyczące struktury i organizacji części popytowej logistyki są trudno dostępne. Większość rozwiązań ICT, ze względu na swoją złożoność i koszty, jest dostępna tylko dla dużych i średnich przedsiębiorstw. Sprawia to, iż większość firm małych i mikro pozostaje poza głównymi nurtami innowacji. Kolejną barierą w wielu rozwiązaniach ICT jest fakt nieuwzględniania trudności związanych z różnorodnością praw i ograniczeń występujących w różnych krajach oraz w różnych środkach transportu. Istniejące rozwiązania ICT nie biorą też pod uwagę barier wynikających z różnic kulturowych i językowych.

Ciekawym przykładem rozwiązania z zakresu platformy elektronicznej jest system zbudowany dla General Motors (GM) przez Schneider Logistics. Uruchomione aplikacje obsługują gospodarkę częściami zamiennymi, obejmując zasięgiem 3200 dostawców, 25 centrów dystrybucyjnych oraz 9 tys. amerykańskich dilerów GM. W ramach tej ogromnej sieci jest transportowanych 16 mln przesyłek rocznie. System wspiera zarządzanie procesami logistycznymi – od złożenia zamówienia do harmonogramowania i realizacji wysyłki.

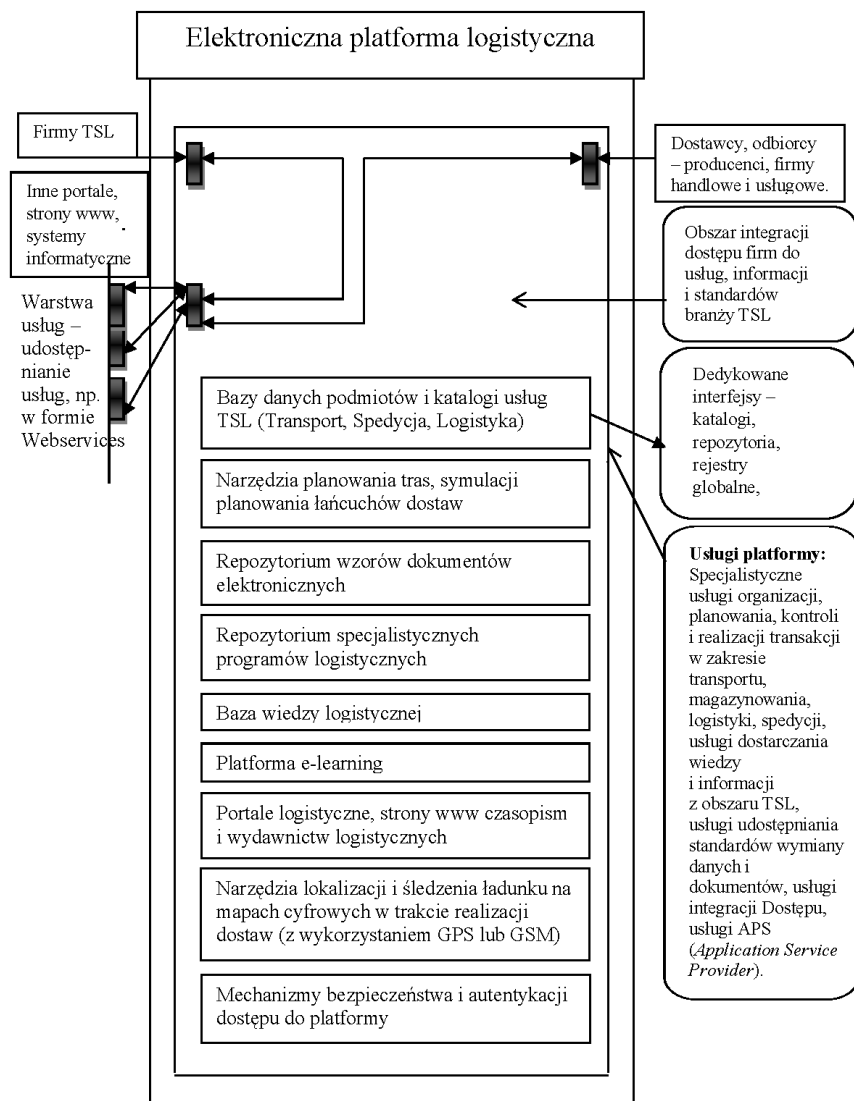
Umożliwia m.in. dostęp w czasie rzeczywistym do informacji o bieżącym statusie zamawianych części, określenie priorytetów realizacji zamówień i przyspieszenie wysyłki, jeśli tylko doszło do sytuacji wyczerpania się zapasu danej części u dilerów, oraz automatyczną konsolidację przesyłek. Podstawowe korzyści, jakie odniósł GM z wdrożenia systemu, to przede wszystkim redukcja kosztów osiągnięta dzięki automatyzacji procesów rezerwacji wysyłek, obniżenie poziomu utrzymywanych zapasów na skutek radykalnego zmniejszenia niepewności co do rzeczywistych dat dostaw oraz podniesienie poziomu obsługi klientów dzięki dostępności do precyzyjnej i wiarygodnej informacji²⁷⁹.

Wychodząc naprzeciw potrzebom wsparcia działalności logistycznej przedsiębiorstw (zwłaszcza sektora MSP), Instytut Logistyki i Magazynowania (ILiM) w Poznaniu udostępnił Elektroniczną Platformę Logistyczną (EPL). Internetowe środowisko współpracy i zarządzania wspólnym łańcuchem dostaw

²⁷⁸ Por. F. Bonfatti, *Gdy marzenia się spełniają – wizja platformy e-logistycznej*, [w:] *Logistyka* 2/2009, s. 16.

²⁷⁹ Por. P. Dura, *E-logistyka oraz zaawansowane systemy planowania i harmonogramowania APS*, Dział Doradztwa Gospodarczego Deloitte & Touche, <http://www.mspstandard.pl/>, 14.01.2014.

umożliwia przedsiębiorcom definiowanie ról w łańcuchu – np. dostawcy, odbiorcy, operatora logistycznego, przewoźnika – wykorzystując wiele funkcji operacyjnych, m.in. przyjmowania i potwierdzania zamówień, planowania tras transportowych i doboru pojazdów, śledzenia dostaw. Ogólny schemat środowiska operacyjnego wykorzystania Elektronicznej Platformy Logistycznej w łańcuchu dostaw przedstawiono na rys. 5.3.



Rys. 5.3. Elektroniczna platforma logistyczna

Źródło: A. Szymonik, *Informatyka dla...*, op. cit., s. 99.

Elektroniczne wsparcie współpracy partnerów obejmuje szerszy kontekst obsługi społeczności logistycznej, udostępniając mechanizmy tworzenia i obsługi klastrów logistycznych, dostęp do bazy wiedzy logistycznej czy prowadzenia wideokonferencji wśród wielu rozproszonych partnerów jednocześnie.

Organizację funkcji operacyjnych platformy EPL podporządkowano w znacznym stopniu logice procesów obsługi logistycznej realizacji zamówienia. Podstawą obsługi przepływu produktów i ładunków jest wiele danych podstawowych, zgromadzonych w globalnej bazie danych produktów identyfikowanych wg standardów GS1 oraz w tworzonym na platformie EPL wewnętrznym katalogu produktów obsługiwanych przez przedsiębiorstwo oraz w katalogu partnerów-kontrahentów powiązanych z bazą danych przedsiębiorstw zarejestrowanych w EPL (w tym odbiorców i dostawców usług logistycznych), w bazie danych usług logistycznych i zasobów logistycznych – stanowiącej parametryczny opis infrastruktury magazynowej i terminalowo-przeładunkowej, floty transportowej, systemów informatycznych itp. oraz w słownikach opakowań, nośników magazynowych, jednostek transportowych itp.

Modelowa EPL składałaby się z następujących elementów: bazy danych (obejmującej na przykład wykaz firm oferujących usługi, rozkłady jazdy, stawki frachtowe); narzędzi obsługi (złożonych na przykład z portalu wiedzy, serwisów informacyjnych); finansowego modułu rozliczeniowego (na przykład wzory dokumentów, płatności elektroniczne); modułu planowania (zawierającego na przykład planowanie łańcuchów dostaw, porównywanie ofert pod względem cen, czasu i potencjału realizacji zamówienia, zakresu oferowanych usług); modułu transakcyjnego (umożliwiający na przykład złożenie zlecenia, potwierdzenie transakcji), a także modułu operacyjnego (monitorowanie dostaw i ich status, instrukcje transportowe, załadunkowe, śledzenie położenia przesyłek w transporcie).

Przykładowa dokumentacja technologiczna wymagań oprogramowania i analizy procesowej w zakresie administrowania kontami firm i użytkowników, obejmowałaby takie elementy, jak: obsługa statusów kont firm i użytkowników, rejestracja firmy, rejestracja użytkowników indywidualnych, rejestracja użytkowników firmowych, przypominanie haseł, zmiana statusu kont, edycja kont, wyszukiwanie firm użytkowników, usuwanie kont, weryfikacja firmy, użytkownicy firmowi, nadawanie uprawnień użytkownikom firmowym, użytkownicy zewnętrzni i ich role w platformie, zarządzanie rolami w platformie, zakładanie użytkowników wewnętrznych, prawa redaktorów, prawa operatorów systemu platform, nowe konto/konta, logowanie do system, profile użytkowników.

Natomiast w obrębie na przykład planowania tras przejazdu i harmonogramów przewozowych mogłyby się tam znaleźć takie elementy, jak: obsługa bazy środków transportu, wyszukiwanie danych w bazie środków transportu, zarządzanie danymi w bazie środków transportu, import danych do bazy środków transportu, eksport danych z bazy środków transportu, baza punktów odbioru i dostawy, baza relacji biznesowych spedytor – przewoźnik, zlecenia

transportowe, generowanie trasy, wizualizacja trasy, wydruk wygenerowanej trasy, raporty o warunkach na danej trasie, tabela odległości, słownik typów opakowań transportowych.

Konstrukcja platformy, prezentowanej na tym rysunku, pod względem technologicznym byłaby otwarta na architekturę SOA (*Service Oriented Architecture*), z możliwością współpracy z innymi platformami oferującymi usługi sieciowe, a wymiana usług na tej platformie mogłaby się odbywać za pomocą Web Serwisów.

5.3. Automatyczna identyfikacja

Pełne zgromadzenie danych niezbędnych do zarządzania elektronicznym przepływem w systemach logistycznych jest możliwe dzięki nowoczesnym narzędziom pozwalającym na zbieranie, analizowanie i przesyłanie danych wewnątrz każdej firmy i instytucji oraz w ich relacjach z otoczeniem bliższym i dalszym.

W praktyce gospodarczej narzędziem tym jest automatyczne gromadzenie danych ADC – *Automatic Data Capture* (wcześniejsze określenia: AI, Auto ID, AIDS). ADC to automatyczne, bezpośrednie wprowadzanie danych do komputerowych systemów informatycznych lub innego sprzętu sterowanego mikroprocesorem za pomocą specjalnych urządzeń (bez użycia klawiatury)²⁸⁰. Urządzenia te w postaci czytników lub skanerów zapewniają szybkie i bezbłędne wprowadzenie danych do systemu. W praktyce, systemy ADC to między innymi:

- świetlne sygnalizatory pobrań;
- OCR (*Optical Character Recognition*) – zestaw technik lub oprogramowanie służące do rozpoznawania znaków i całych tekstów w pliku graficznym o postaci rastrowej²⁸¹ (zadaniem OCR jest zwykle rozpoznanie tekstu w zeskanowanym dokumencie)²⁸²;
- RFID (*Radio-frequency identification*) – technika, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu

²⁸⁰ Por. I. Kudelska, A. Ponikierska, *Analiza technik automatic data capture w organizacji przepływu materiałów przez magazyn*, [w:] *Logistyka* 2009/2, ss. 48-49.

²⁸¹ Grafika rastrowa – prezentacja obrazu za pomocą pionowo-poziomej siatki odpowiednio kolorowanych pikseli na monitorze kolorowym, drukarce lub innym urządzeniu wyjściowym.

²⁸² Por. Suruchi G. Dedgaonkar, Anjali A. Chandavale, Ashok M. Sapkal, *Survey of Methods for Character Recognition*, [w:] *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 1, Issue 5, May 2012, ss. 180-189.

stanowiącego etykietę obiektu przez czytnik, w celu identyfikacji obiektu (technika umożliwia odczyt, a czasami także zapis układu RFID)²⁸³;

- systemy głosowe – użycie technologii głosowych zapewnia łatwy, dwukierunkowy sposób komunikacji między systemem informatycznym, np. WMS²⁸⁴, a jego użytkownikiem, np. pracownikiem magazynu, który kompletuje towar do wydania z magazynu (zamiast zleceń na papierze czy instrukcji wyświetlanych na ekranach terminali przenośnych pracownicy magazynu korzystają z najbardziej naturalnej formy komunikacji, jaką jest głos);
- czytniki kodów kreskowych, popularnie nazywane skanerami, są urządzeniami, które zamieniają światło odbite od kodu kreskowego na sygnał elektroniczny, zrozumiały dla kasy lub komputera (w zależności od rodzaju mechanizmu odczytu różnią się czytniki kodów laserowe i diodowe/CCD);
- terminale RF – bezprzewodowa wymiana informacji drogą radiową on-line, terminale takie często są wyposażone w skaner kodów kreskowych;
- komputery montowane w pojazdach oraz przenośne komputery – mają przewagę nad urządzeniami podręcznymi (większy ekran, większa klawiatura), są wyposażone w przyjazny dla użytkownika interfejs GUI²⁸⁵ (generalnie urządzenia montowane na pojazdach korzystają z zewnętrznego przewodowego lub bezprzewodowego czytnika kodów kreskowych w celu przetwarzania danych).

ADC służy do usprawniania m.in. następujących operacji: przyjmowania i wydawania materiałów oraz towarów z automatyczną kontrolą dostaw, ewidencjonowania obrotów z automatyczną aktualizacją stanów magazynowych, składowania i przemieszczania materiałów i towarów z automatyczną rejestracją ich lokalizacji (skąd, dokąd i gdzie), pobierania i kompletacji dostaw do produkcji lub zużycia oraz towarów na zewnątrz przedsiębiorstw czy instytucji z automatyczną kontrolą wydań, przeprowadzania inwentaryzacji itp.

²⁸³ Por. Maloni M., DeWolf, F., *Understanding radio frequency identification (RFID) and its impact on the supply chain. Penn State Behrend – RFID Center of Excellence, available at, www. ebizitpa. org/Education/Operations/RFID/RFIDresearchPSU. pdf* (accessed April 2, 2007).

²⁸⁴ WMS, *Warehouse Management System* – system informatyczny wspomagający zarządzanie procesami magazynowymi, nadzorujący racjonalne rozmieszczenie zapasów, wykorzystujący techniki ADC.

²⁸⁵ GUI graficzny interfejs użytkownika (*Graphical User Interface*), często nazywany też *środowiskiem graficznym* – ogólne określenie sposobu prezentacji informacji przez komputer oraz interakcji z użytkownikiem, polegające na rysowaniu i obsługiwaniu podstawowych elementów, np. okno, pole edycji, suwak, przycisk.

W zależności od konkretnych potrzeb do ADC wykorzystuje się następujące grupy technik²⁸⁶: optyczne (kody kreskowe, rozpoznawanie znaków graficznych, pisma, obrazu), magnetyczne (taśmy magnetyczne, rozpoznawanie atramentu magnetycznego), elektromagnetyczne (w tym elektroniczne metki odczytywane drogą radiową – RFID), biometryczne (rozpoznawanie głosu, odciski palców, tęczęwki oka itd.), dotykowe (karty inteligentne), głosowe (słuchawki i mikrofon oraz informatyczny syntezytor mowy ludzkiej).

Każda z tych technik pozwala zbierać i przysyłać dane do systemów informatycznych, które je analizują, przechowują i udostępniają zainteresowanym. W praktyce wykorzystuje się często rozwiązania mieszane, łącząc różne techniki w jeden system, przygotowany na bazie specjalistycznych projektów w oparciu o technologie informatyczne.

Kody kreskowe

Wśród technik optycznych kody kreskowe są powszechnie wykorzystywane, zwłaszcza w logistyce, jako metoda najłatwiej dostępna i najtańsza, a tym samym zalecana jako podstawowa technika ADC do usprawniania zarządzania logistycznego²⁸⁷. Do tej pory opracowano kilkaset rodzajów i odmian kodów kreskowych (kody liniowe, w tym zredukowane, dwuwymiarowe, złożone, kompozytowe), ale tylko kilka z nich znalazło powszechne zastosowanie, przede wszystkim w logistyce, pełniąc funkcje uniwersalnych, międzynarodowych standardów.

W logistyce kody kreskowe wykorzystuje się do: identyfikacji towarów, wykonywania operacji magazynowych, znakowania produktów, śledzenia przesyłek, rejestrowania dokumentów w systemie logistycznym i ewidencji środków trwałych systemu logistycznego.

Zastosowanie kodów kreskowych pozwala przede wszystkim na radykalny wzrost szybkości wprowadzania danych do systemu komputerowego oraz eliminację błędów.

Budowa i wykorzystanie kodów kreskowych w oparciu o międzynarodowe standardy spowodowało, że są one chętnie wykorzystywane w systemach ADC.

Rozwiązania ADC oparte na kodach kreskowych występują w układzie stacjonarnym – komunikowanie z bazą danych systemu informatycznego poprzez

²⁸⁶ Zob. *Kody kreskowe i inne globalne standardy w biznesie*, red. nauk. E. Hałas, ILiM, Poznań 2012, s. 196.

²⁸⁷ Por. S. Hong-ying, *The Application of Barcode Technology in Logistics and Warehouse Management*, Education *Technology and Computer Science*, 2009, [w:] ETCS '09. First International Workshop on (Volume:3), ss. 732-735.
DOI: 10.1109/ETCS.2009.698

media typu światłowód czy kabel oraz mobilnym – komunikowanie z bazą danych systemu informatycznego poprzez łącza radiowe (WLAN²⁸⁸, standard Wi-Fi²⁸⁹).

Systemy stacjonarne przesyłają dane na zasadzie odczyt – zapis. Są one skonstruowane do pracy samodzielnej. Wyposaża się je w specjalne statywy lub obudowy umożliwiające przytwierdzenie ich do podłoża. Często stosowane w boksach kasowych ze względu na swobodę pracy kasjera i możliwość skanowania kodów niezależnie od ułożenia (w pionie, w poziomie oraz pod skosem).

Systemy mobilne – (przenośne) urządzenie elektroniczne pozwalające na przetwarzanie danych bez konieczności utrzymywania przewodowego połączenia z siecią. Urządzenie mobilne może być przenoszone lub przewożone.

Systemy ADC są zbudowane ze skanerów (czytników kodów kreskowych), terminali, drukarek. Skanery możemy podzielić na: stacjonarne, bezprzewodowe, przenośne (mobilne). Czytniki kodów kreskowych mogą czytać kody: jednowymiarowe, 1D – czytniki laserowe lub diodowe, dwuwymiarowe 2D – skanery wizyjne (imagery).

Tam gdzie priorytetem jest mobilność i niezależność, idealnym rozwiązaniem jest stosowanie przenośnych (mobilnych) terminali²⁹⁰ komputerowych (zwanymi również kolektorami danych²⁹¹) wyposażonych w skaner kodów kreskowych lub tagów RFID. Kolektory danych posiadają wbudowane: czytnik kodów kreskowych, klawiaturę, wyświetlacz LCD, pamięć oraz system operacyjny np. Windows CE lub Windows Mobile. Przeznaczone są do gromadzenia, przechowywania i transmisji danych.

W skład systemu ADC wchodzi drukarki służące do umieszczania na etykietach kodów kreskowych i informacji w nich zawartych, które następnie są wykorzystywane do oznakowania odpowiedniego przedmiotu czy produktu. Dostępne są drukarki o różnych parametrach technicznych.

Elektroniczne oznakowanie produktu

W zakresie oznaczania produktów (w tym i opakowań) nastąpił przełom, kiedy to zastosowano nowy sposób nazwany elektronicznym oznakowaniem produktu EPC (*Electronic Produkt Code*). Zamiennie używa się synonimów

²⁸⁸ WLAN – sieć bezprzewodowa (*Wireless LAN*) zrealizowana bez użycia przewodów, zasięg do 100 m.

²⁸⁹ Wi-Fi – sieci bezprzewodowe oparte na standardach 802.11, zasięg do 10 m.

²⁹⁰ Terminal (*terminal* – końcówka) to urządzenie pozwalające człowiekowi na pracę z komputerem lub systemem komputerowym.

²⁹¹ Kolektory danych to przenośne, kieszonkowe, komputery PDA (*Personal Digital Assistant*), palmtopy wyposażone w zintegrowany czytnik kodów kreskowych, klawiaturę, wyświetlacz LCD oraz pamięć. Przeznaczone są do gromadzenia, przechowywania i transmisji danych.

znacznik RFID (*Radio Frequency IDentification*), identyfikator radiowy RFID, tag, transponder²⁹².

Pierwsze zastosowania RFID sięgają czasów II wojny światowej. Wynaleziony w Wielkiej Brytanii system IFF (*Identification, Friend or Foe*) służył do identyfikacji samolotów i można śmiało nazwać go poprzednikiem RFID.

W 1948 roku powstała praca Harrego Stockmana, która zapoczątkowała koncepcję pasywnych systemów RFID. W latach 50-60. poprzedniego stulecia naukowcy w Stanach Zjednoczonych, Europie i Japonii prowadzili badania nad wykorzystywaniem fal radiowych do zdalnego identyfikowania przedmiotów. Pierwsze komercjalizacje technologii RFID dotyczyły systemów zabezpieczających przed kradzieżą. Lata 90. XX w. to okres, w którym RFID stało się częścią codziennego życia i działalności gospodarczej. Od tego czasu na świecie powstało już tysiące firm pracujących nad rozwojem i zastosowaniami technologii RFID²⁹³.

Do znanych firm globalnych, które rozpoczęły wdrażanie technologii RFID do elektronicznego znakowania produktów można zaliczyć: Wal-Mart, Target, Albertsons, Metro, Tesco, Max&Spencer, Procter&Gamble, Gillette. Technologia RFID zastąpi w nieodległej przyszłości system kodów paskowych służący do znakowania towarów, co podniesie wydajność transportu, magazynowania oraz procesu sprzedaży towarów. Przykładem udanego wdrożenia takiego systemu jest amerykańska sieć handlowa Wal-Mart. Obecnie RFID znajduje coraz szersze zastosowania w logistyce, transporcie publicznym, systemach zabezpieczeń, a także na rynku płatności elektronicznych²⁹⁴.

System identyfikacji radiowej zawiera bazę, do której jest dołączona antena wypromieniowująca energię niezbędną do zasilania transpondera. Ta sama antena stacji bazowej służy do komunikacji z transponderem RFID, umożliwiając odczyt i zapis danych do/ze znacznika. Stacja bazowa jest podłączona do komputera zewnętrznego poprzez interfejs przewodowy. Stacja bazowa, komunikując się z transponderem, używa interfejsu radiowego. Obwody nadajnika i odbiornika nastrojone są na tę samą częstotliwość. Używane transpondery RFID można podzielić na dwie grupy: tylko do odczytu RO (*Read-Only*) oraz do odczytu i zapisu RW (*Read-Write*). Te drugie mają możliwość modyfikowania zawartości.

Natomiast ze względu na zasilanie, transpondery dzielimy na: aktywne – posiadają własne źródło zasilania, które dostarcza energii do układu

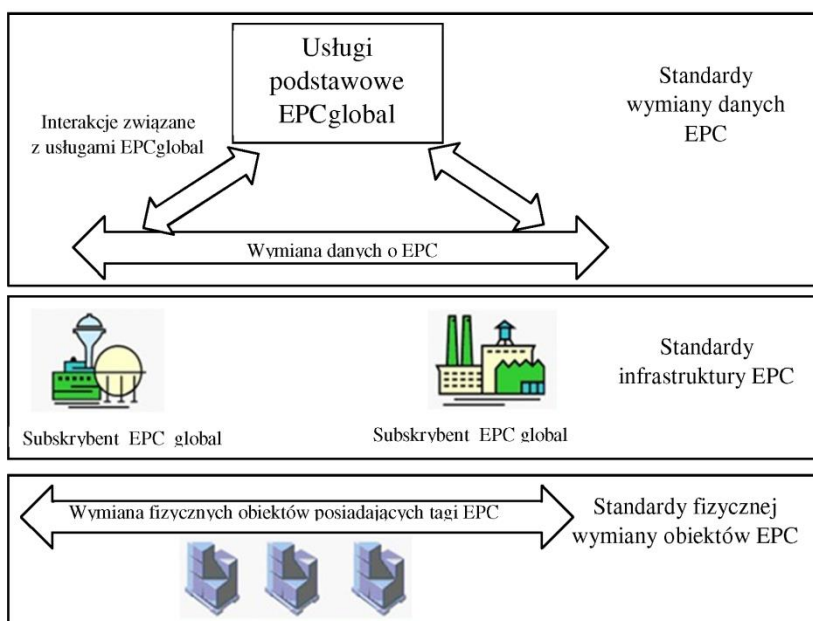
²⁹² Por. C. Bolan, *A Review of the Electronic Product Code Standards for RFID Technology, proceedings of the 7th International Network Conference*, University of Plymouth, UK, 8-10 July 2008, ss. 171-178.

²⁹³ Zob. A. Szymonik, *Zarządzanie zapasami i łańcuchem dostaw*, Difin, Warszawa 2013, s. 275.

²⁹⁴ Tamże.

mikroprocesorowego oraz przekaźnika z anteną, pasywne – nie mają własnego źródła zasilania, energię elektryczną potrzebną do chwilowego zasilenia układu mikroprocesorowego pobierają z pola elektromagnetycznego emitowanego przez czytnik, semipasywne – są rodzajem kompromisu pomiędzy tagami pasywnymi a aktywnymi. Zasięg oddziaływania zależy również od zakresu fal radiowych stosowanych w układach RFID, co obrazuje tabela w załączniku 5.1.

EPC jest tak zbudowany, że możliwe jest identyfikowanie wszystkich pojedynczych produktów i towarów w łańcuchu dostaw. Do najczęściej stosowanych tagów zaliczamy te, które są produkowane w standardzie GS1. Do nich zliczamy: SGTIN (*Serialized Global Trade Identification Number*) – Seryjny Globalny Numer Jednostki Handlowej, SSCC (*Serial Shipping Container Code*) – Seryjny Numer Jednostki Logistycznej, SGLN (*Serialized Global Location Number*) – Seryjny Globalny Numer Lokalizacyjny, GRAI (*Global Returnable Asset Identifier*) – Globalny Identyfikator Zasobów Zwrotnych, GIAI (*Global Individual Asset Identifier*) – Globalny Indywidualny Identyfikator Zasobów.



Rys. 5.4. Architektura EPCglobal

Źródło: *EPCglobal – The EPC global Architecture Framework, Final Version of 1 July, 01.02.2014.*

Dla logistycznej funkcji identyfikowania opakowań z produktami, najczęściej spośród wymienionych występują dwa pierwsze identyfikatory: SGTIN i SSCC.

W świecie biznesu została stworzona przez GS1 sieć EPCglobal, oparta na globalnych standardach. Zachęca ona dostawców rozwiązań do tworzenia oprogramowania i sprzętu, który posługuje się interfejsami zbudowanymi wyłącznie na tych standardach. Architektura EPCglobal jest opisana w sposób otwarty i niekomercyjny. Wszystkie interfejsy pomiędzy elementami sieci EPCglobal są określone jako otwarte standardy i rozwijane głównie przez społeczność związaną z Procesem Rozwoju Standardów EPCglobal. Architektura EPCglobal jest zaprojektowana w ten sposób, by móc funkcjonować we wszystkich istniejących strukturach i standardach branżowych. Wszelkie prace związane z rozwojem standardów odbywają się za pośrednictwem grup roboczych EPC, które działają zarówno na poziomie biznesowym, jak i technicznym²⁹⁵.

Rozróżniamy trzy podstawowe grupy standardów (rys. 5.4)²⁹⁶: fizycznej wymiany obiektów EPC, wymiany danych EPC, infrastruktury EPC.

Specyfikacja EPC w standardzie GS1 wyróżnia cztery typy zdarzeń²⁹⁷:

Pierwszy – *Object Event* (identyfikacja obiektów) – dotyczy faktu zaobserwowania pewnej grupy kodów EPC, nie mówi nic o relacjach między obiektami.

Drugi – *Aggregation Event* (agregacja danych) – dotyczy faktu zaobserwowania pewnej grupy kodów EPC, np. produktów przyporządkowanych do palety, albo zmian czy zdarzeń dotyczących takiej grupy, np. załadunek czy rozładunek.

Trzeci – *Quantity Event* (identyfikacja ilości) – dotyczy faktu zaobserwowania pewnej grupy kodów EPC reprezentujących jedną klasę obiektów, np. 10 puszek napoju i zmian zachodzących w tej grupie (zmiana ilości).

Czwarty – *Transaction Event* (identyfikacja transakcji) – dotyczy przyporządkowania obserwacji do transakcji biznesowej lub zmiany w takim przyporządkowaniu, np. przekazanie towaru firmie transportowej, przyjęcie na magazyn w centrum dystrybucji.

Analizując przydatność stosowanych obecnie kodów kreskowych oraz RFID, można dojść do następujących wniosków:

- ilość informacji, jakie możemy pozyskać on-line o ładunku logistycznym jest znacznie większa w przypadku zastosowania EPC, jako że możemy

²⁹⁵ Zob. P. Kaźmierczyk, J. Majewski, *EPC Global – wprowadzenie*, <http://rfid-lab.pl/epc/>, 23.03.2014.

²⁹⁶ Zob. A. Szymonik, *Zarządzanie zapasami ...* op. cit., s. 278.

²⁹⁷ Por. *Kody kreskowe i inne globalne standardy w biznesie*, red. nauk. Hałas E., ILiM, Poznań 2012, s. 126.

dane umieścić w samym znaczniku, jak i w systemie informatycznym, natomiast np. etykieta logistyczna z kodem kreskowym informuje o ładunku logistycznym, np. palecie, a nie o jej zawartości²⁹⁸;

- w przypadku odczytu kodu kreskowego trzeba dotrzeć z czytnikiem do opakowania (lub odwrotnie), co znacznie wydłuża czas odczytu i angażuje pracownika (powiększa koszty), a tych niedogodności nie mamy w przypadku EPC, gdzie wszystko odbywa się automatycznie, a więc bez udziału człowieka;
- w czasie odczytu kodu kreskowego jesteśmy pewni, czy wyrób jest czy go nie ma, np. na regale, co stwierdza operator i czytnik; natomiast w przypadku RFID może dojść do sytuacji, że brak informacji z czytnika można zinterpretować jako brak towaru albo że zawiódł któryś element systemu identyfikacji radiowej (spowodowane to może być np. brakiem łączności pomiędzy stacją bazową i transponderem, zakłóceniami w rozprzestrzenianiu się fal radiowych, zbyt dużą odległością tag – stacja bazowa, uszkodzonym elementem elektronicznym, brakiem zasilania, niewłaściwy system rozpoznawania i identyfikacji);
- EPC zabezpiecza przed produktami podrabianymi (ilość informacji umieszczona w bazie pozwala na kodowanie danych o wyrobie), a ponadto ułatwia identyfikowanie i śledzenie w całej globalnej sieci dostaw pojedynczą sztukę opakowań, np. dla celów traceability²⁹⁹;
- EPC umożliwia odczyt wielu etykiet jednocześnie, co nie jest możliwe w przypadku kodów kreskowych;

²⁹⁸ Por. A. Szymonik, *Information Technologies in Logistics*, Lodz University of Technology, monographs 2012, ss. 98-99.

²⁹⁹ Traceability to zdolność śledzenia (odtworzenia historii) przepływu dóbr w łańcuchach i sieciach dostaw, wraz z rejestracją parametrów identyfikujących te dobra oraz wszystkie lokalizacje objęte przepływem. Zapewnienie bezpieczeństwa dostarczanych na rynek produktów wiąże się z rejestrowaniem i gromadzeniem danych na ich temat na każdym etapie łańcucha dostaw żywności, a więc na poziomie każdego z przedsiębiorstw biorących udział w tym łańcuchu. Ma to istotne znaczenie, zwłaszcza w sytuacji, gdy z jakichś względów dany produkt musi zostać wycofany z łańcucha dostaw. Zgodnie z wymogami prawa (m.in. Rozporządzenie (WE) nr 178/2002) wymóg traceability jest obligatoryjny dla branży żywnościowej i od 1 lipca 2013 r. kosmetycznej (Rozporządzenie (WE) nr 1223/2009). Jednym z najważniejszych elementów procesu traceability jest wycofanie towarów z rynku (*Recall*). Najczęściej system śledzenia ruchu i pochodzenia produktów jest wykorzystywany do lokalizowania wadliwej lub niebezpiecznej żywności, farmaceutyków lub innych niebezpiecznych dla klientów produktów znajdujących się w obrocie, [w:] G. Sokołowski, *Traceability & Recall*, <http://www.gs1pl>, 22.06.2013.

- EPC – usprawnia np. zarządzanie bagażami na lotniskach w porównaniu z kodami kreskowymi, które można sczytać w granicach 70-80% (EPC pozwala sczytać bagaż w granicach 99,3%)³⁰⁰;
- RFID likwiduje kolejki kasowe, pod warunkiem zastosowania dobrych i niezawodnych systemów identyfikacji radiowych (wielokierunkowych anten bazowych);
- kody kreskowe jeszcze długo będą używane w logistyce z powodu swojej niezawodności (jeżeli transponder umieścimy bezpośrednio np. na opakowaniach metalowych, to zasięg jego działania wynosi zero³⁰¹), powszechności i stosunkowo niewielkich kosztach wdrażania i eksploatacji.

Przedstawiona analiza z jednej strony wykazuje zalety kodów kreskowych, ale i pokazuje, że przed RFID w logistce, nie ma ucieczki, jako że przyszłościowa technika i technologia dają coraz lepsze i tańsze rozwiązania, a korzyści zastosowania identyfikacji radiowej są niepodważalne (np. szybkość, odczyt bez udziału człowieka, zabezpieczenie produktów przed podrabianiem). Obecnie najlepszym rozwiązaniem w przypadku wartościowych „przesyłek” i „terminowych” jest stosowanie jednocześnie etykiety zawierającej tag RFID oraz nadrukowany kod produktu.

Rozpoznawanie znaków metodą optyczną

Analizując systemy identyfikacji druku i pisma łatwo zauważyć, że rozwijają się one wraz z postępem w elektronice i informatyce. Wyróżniamy trzy rodzaje technik rozpoznawania tekstu OCR, ICR, OMR.

OCR (*Optical Character Recognition*) – technologia umożliwiająca przetworzenie zeskanowanego tekstu do formy cyfrowej³⁰². OCR rozwija się w dwóch kierunkach. Z jednej strony są opracowywane coraz to lepsze metody rozpoznawania pisma (również ręcznego) i wtedy już mówi się o technice ICR, z drugiej tworzone są specjalne czcionki ułatwiające odczyt, tj. OCR-A i OCR-B. Do rozpoznawania używa się programów, które działają w oparciu o obrazy przesyłane ze skanerów i kamer cyfrowych. Specjalnych czcionek używa się zwykle tam, gdzie istnieje potrzeba częstego, szybkiego i prostego odczytu informacji.

³⁰⁰ Por. J. Ejsymont, Czy nowa technologia EPC zastąpi kody kreskowe, [w] Logistyka 6/2006, s. 85.

³⁰¹ Zob. *Automatyczna identyfikacja w systemach logistycznych*, red. nauk. S. Kwaśniewski, P. Zajac, PW, Wrocław 2004, s. 137.

³⁰² Por. D. Berchmans, S.S. Kumar, *Optical character recognition*, [w:] An overview and an insight, Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on 2014, ss. 1361-1365.

W obrębie systemów OCR wyróżniamy technologie: kodów kreskowych, pisma maszynowego i magnetycznego³⁰³, pisma blokowego³⁰⁴.

ICR to skrót od *Intelligent Character Recognition*, czyli inteligentne rozpoznawanie znaków. Podstawowym zadaniem tego systemu jest rozpoznanie znaków alfanumerycznych zapisanych odręcznie, czyli rozpoznanie pisma ręcznego³⁰⁵. Do rozpoznawania są używane mechanizmy sieci neuronowych.

OMR oznacza *Optical Mark Recognition* — optyczne rozpoznawanie znaczników. Polega na rozpoznawaniu znaków innych niż alfanumeryczne, np. pól wyboru lub kodów kreskowych³⁰⁶. Czytniki OMR znacznie ułatwiają analizę dużej ilości zestandaryzowanych formularzy oraz umożliwiają kontrolę poprawności ich wypełnienia. System ten wymaga specjalnie przygotowanych formularzy oraz skanerów czytających wybrane rodzaje zaznaczeń umieszczanych w ściśle określonych miejscach formularza. Oprogramowanie systemów OMR zauważa obecność, bądź brak, zaznaczenia w określonych miejscach formularza i przetwarza ten sygnał na zapis komputerowy, uwzględniając położenie tych znaków. Technologia jest przydatna przy gromadzeniu danych pod warunkiem, iż są one stosunkowo proste (np. odpowiedzi na pytania typu Tak, Nie lub odpowiedzi z zamkniętego typu wyboru), a formularze są dobrze przygotowane. Technika OMR nie zdaje egzaminu, gdy mamy do czynienia z dużą ilością tekstu. W takich sytuacjach techniki OCR lub ICR są bardziej przydatne.

Systemy OCR, ICR i OMR znajdują zastosowanie na różnych polach. Z tego względu ich skuteczność musi być badana według odmiennych kryteriów. Jeśli przyjąć za podstawowe kryterium odsetek prawidłowo odczytanych i przeanalizowanych danych, to najbardziej skuteczne są techniki OMR (nawet 99,9%), mniej skuteczne są systemy OCR, a największym procentem błędnych interpretacji cechują się systemy ICR. Dwa ostatnie systemy (OCR i ICR) również mogą osiągać około 99% skuteczności, ale tylko w bardzo ściśle określonych, niemal „laboratoryjnych”, warunkach oraz po ręcznej edycji błędów³⁰⁷.

³⁰³ Pismo magnetyczne jest pisane szczególnym gatunkiem atramentu, zawierającym sproszkowane substancje magnetyczne, używane do ręcznego wypełniania formularzy i druków, które są odczytywane za pomocą specjalnych czytników pisma.

³⁰⁴ Pismo blokowe – typ pisma pośredni między pismem zwykłym a technicznym; nie posiada wiązań międzyliterowych.

³⁰⁵ Por. P. Ogden, *Applying intelligent character recognition in the “real world”*, [w:] *Document Image Processing and Multimedia* (Ref. No. 1999/041), IEE Colloquium on, 1999, ss. 11/1-11/4.

³⁰⁶ Por. J.L. Pérez-Benedito, E.Q. Aragón, J.A. Alriols, L. Medic L., *Optical Mark Recognition in Student Continuous Assessment*, *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje*, 2014, Volume: 9, Issue: 4, ss. 133-138.

³⁰⁷ A. Szymonik, *Informatyka dla ...*, op. cit., s. 273.

Komunikacja głosowa

Systemy głosowe znalazły zastosowanie szczególnie w magazynach (poczynając od małych magazynów spożywczych, a kończąc na wielkopowierzchniowych hurtowniach farmaceutycznych czy narzędziowych), w których często dokonuje się kompletacji.

Głównym nośnikiem informacji w systemach głosowych są komunikaty głosowe przesyłane pomiędzy operatorem i systemem informatycznym WMS.

Zadania do wykonania są generowane przez system zarządzający magazynem i za pomocą sieci radiowej transmitowane do terminala głosowego³⁰⁸ (przytwierzonego do paska), w którym działa oprogramowanie rozpoznające mowę.

Operator otrzymuje z systemu polecenia głosowe i głosem potwierdza ich wykonywanie, zgodnie z zaprojektowanym scenariuszem.

Metody biometryczne

Biometria to matematyczno-statystyczne metody badania prawidłowości kierujących zmiennością populacji organizmów żywych³⁰⁹. Biometria to również rozpoznawanie osób na podstawie jego specyficznych cech fizycznych i behawioralnych. Do cech tych zalicza się charakterystyki linii papilarnych, kształtu twarzy czy dłoni, tęczówki oka, pisma ręcznego, jak również mowy, czy sposobu chodzenia, a nawet układ żył nadgarstka.

Biometria jest wykorzystywana przede wszystkim jako kontrola dostępu do chronionych pomieszczeń lub identyfikacji użytkowników korzystających z określonych urządzeń (np. komputer), danych, informacji. Coraz częściej systemy biometryczne wspomagają wyszukiwanie wybranych osób oraz rejestrację czasu pracy.

Wraz z rozwojem różnorodnych technik i technologii powstają niezawodne systemy, umożliwiające identyfikowanie ludzi na podstawie charakterystycznych dla nich cech. Przeprowadzają one weryfikację lub identyfikację osoby w sposób całkowicie zautomatyzowany. Specjalistyczna aparatura, wspomagana komputerowo, automatycznie pobiera dane istotne dla procesu rozpoznawania, poddaje je obróbce oraz porównuje ze wzorcem z bazy danych.

³⁰⁸ Terminal głosowy to rozwiązanie umożliwiające dialog między pracownikami magazynu a systemem zarządzania magazynem. Urządzenie łączy w sobie szybkie i precyzyjne rozpoznawanie komend głosowych z odpornością i niezawodnością wymaganą w trudnych warunkach przemysłowych, [w:] *Efektywność w zasięgu głosu*, <http://synergia-it.pl/>, 20.01.2016.

³⁰⁹ Por. W. Kopaliński, *Słownik wyrazów obcych*, <http://www.slownik-online.pl/kopalinski/>, 01.04.2014; A.K. Jain, A. Ross, S. Prabhakar, *An introduction to biometric recognition*, [w:] *IEEE Transactions on Circuits and Systems for Video Technology*, Volume 14 Issue 1, January 2004, ss. 4-20.

W praktyce funkcjonuje wiele typów systemów biometrycznych, do których możemy zaliczyć³¹⁰:

Rozpoznawanie odcisku palca (Fingerprint Recognition) – system tego typu składa się ze skanera, którego zadaniem jest pobranie danych do analizy oraz z oprogramowania, które zapisuje charakterystyczne dane naszego odcisku palca w specyficznym formacie. Informacja ta jest umieszczana w bazie danych jako wzorzec i porównywana z nowo wprowadzanymi przez skaner odciskami za każdym razem, kiedy użytkownik chce uzyskać dostęp do systemu. Użytkownik będzie rozpoznany, nawet gdy palec będzie skaleczony lub brudny. Większość systemów wprowadza do bazy danych więcej niż jeden palec jako zabezpieczenie na wypadek, gdyby system z jakichś przyczyn nie rozpoznał użytkownika. W chwili obecnej rozpoznawanie odcisku palca jest najbardziej rozpowszechnioną technologią biometryczną.

Rozpoznawanie twarzy (Face Recognition) – kształt twarzy, wszystkie jej elementy (nos, oczy, usta itd.) oraz wzajemne relacje pomiędzy nimi (odległość, proporcje, itp.) tworzą bardzo unikalną strukturę dla systemów biometrycznych. Zasada działania systemu jest analogiczna jak w przypadku rozpoznawania odcisku palca. Kamera rejestruje obraz twarzy, a później program wybiera szczegółowe informacje, które porównuje z zarejestrowanym w bazie danych wzorcem. W procesie rozpoznawania twarzy są używane dwie technologie. Pierwsza z nich porównuje rozmiary poszczególnych elementów twarzy i relacje między nimi. Na przykład długość nosa i rozstaw źrenic. Druga metoda porównuje najbardziej charakterystyczne dane z obrazu przesłanego z kamery (np. rozmiar nosa) z wzorcem twarzy zapisanym w bazie danych. System rozpoznawania twarzy jest niezawodny, lecz ze względu na wysoki koszt sprzętu oraz skomplikowany sposób konfiguracji systemu nie jest rozpowszechniony.

Rozpoznawanie tęczówki oka (Iris Recognition) – tęczówka oka jest złożona z bardzo dużej ilości punktów charakterystycznych i unikalnych dla każdej osoby. Dla systemów biometrycznych jest niemal idealnym źródłem danych. Kamera skanuje obraz tęczówki użytkownika i przesyła próbkę do analizy. Program porównuje przesłane dane z zapamiętanym wzorcem i na podstawie rezultatu identyfikuje użytkownika.

Rozpoznawanie siatkówki oka (Retina Recognition) – jest to prawdopodobnie najbardziej zaawansowany i bezpieczny system biometryczny. Obraz siatkówki, która umiejscowiona jest z tyłu oka jest bardzo trudny do uchwycenia. Podczas wpisywania użytkownika do systemu musi on skierować wzrok na specyficzny punkt i utrzymać go w tym stanie przez kilka sekund, zanim kamera zarejestruje poprawnie obraz tęczówki. Jedyną rzeczą jaką jest rejestrowana to układ naczynek krwionośnych. Układ ten jest unikalny dla

³¹⁰ Por. J. Zaworski, *Systemy biometryczne* – Monitor 01/10/2002, <http://www.infolinia.com/monitorarticle,01.04.2014>.

każdej osoby, tak więc identyfikacja na tej podstawie jest bardzo dokładna. Systemy rozpoznawania siatkówki i tęczówki oka oferują największe bezpieczeństwo systemu ze względu na unikalne źródła danych, z których korzystają, a także ze względu na jakość urządzeń do odczytu (specjalistyczne kamery do odczytu oka)³¹¹.

Rozpoznawanie geometrii ręki (Hand Geometry) – w tym systemie użytkownik kładzie rękę na czytniku zgodnie z zalecanym przez producenta urządzenia ułożeniem. Czytnik rejestruje trójwymiarowy obraz palców i dłoni. Zapamiętany obraz jest zapisywany w bazie danych jako wzorzec. System rozpoznawania geometrii ręki jest jednym z najbardziej dokładnych i powszechnie wykorzystywanych systemów biometrycznych. Już podczas olimpiady w 1996 roku był zastosowany do kontroli bezpieczeństwa w całej olimpijskiej wiosce³¹².

Rozpoznawanie geometrii palca (Finger Geometry) – system działa analogicznie jak poprzedni. Czytnik rejestruje trójwymiarowy obraz jednego lub dwóch palców³¹³.

Rozpoznawanie linii dłoni (Palm Recognition) – system bardzo podobny w działaniu do systemu rozpoznającego odcisk palca. W tym przypadku rejestrowane przez skaner są linie na wewnętrznej stronie dłoni³¹⁴.

Rozpoznawanie głosu (Voice Recognition) – w metodzie tej rejestrowany jest dźwięk głosu użytkownika, a także jego językowe nawyki (akcent, intonacja itp.) oraz wszystkie inne charakterystyczne dla niego wady wymowy mogące ułatwić proces identyfikacji. Największy problem występujący przy tego typu rozwiązaniach to łatwość z jaką system może być oszukany za pomocą głosu nagranych na taśmie. Bardziej zaawansowane rozwiązania wymagają od użytkownika wypowiedzenia dłuższych i trudniejszych kwestii niż typowo imię i nazwisko. Często wymagane jest też wypowiadanie innych sentencji za każdym razem, kiedy użytkownik loguje się do systemu. Proces ten wydłuża istotnie czas weryfikacji i wpływa na wydajność całego systemu. Kolejną wadą tego rozwiązania jest duża czułość systemu na wszelkie zmiany w głosie użytkownika spowodowane na przykład przeziębieniem czy też nadwyżeniem

³¹¹ Por. R. Choraś, *Retina recognition for biometrics*, [w:] Digital Information Management (ICDIM), 2012 Seventh International Conference on, 2012, ss. 177-180.

³¹² Por. O. Ayurzana, B. Pumbuurei, K. Hiesik, *A study of hand-geometry recognition system*, [w:] Strategic Technology (IFOST), 2013 8th International Forum on, 2013, Volume 2, ss. 132-135.

³¹³ Por. S. Malassiotis, N. Aifanti, M.G. Strintzis, *Personal authentication using 3-D finger geometry*, [w:] IEEE Transactions on Information Forensics and Security, 2006, Volume 1, Issue, 1, ss. 12-21.

³¹⁴ Por. H Zhang, D. Hu, *A Palm Vein Recognition System*, [w:] Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on 2010, Volume 1, ss. 285-288.

strun głosowych. Inną wadą to fakt, że na pracę systemu istotny wpływ mają wszystkie dźwięki. Zaletą jest stosunkowo niski koszt implementacji dla dużej liczby użytkowników, jako że urządzenia, z którymi system pracuje to telefony lub bardzo proste mikrofony. Są to więc rzeczy już zainstalowane lub takie, których koszt zakupu jest niski³¹⁵.

Rozpoznawanie podpisu (Signature Recognition) – jest to najłatwiej akceptowany system przez wszystkich użytkowników. Wynika to z naszych nawyków i przyzwyczajzeń. Odkąd pamiętam, własnoręczny podpis na wszelkiego rodzaju dokumentach służył jako forma weryfikacji tożsamości. Ten system wykracza daleko poza prostą analizę podpisu. Oprócz kształtu podpisu i jego treści, sprawdza również nacisk pióra, szybkość pisania, miejsca, w których pióro zostaje uniesione. Rejestrowane jest to wszystko dzięki użyciu specjalnie do tego celu skonstruowanego pióra i tabletu. Dane po przetworzeniu są zapisywane w bazie jako wzorzec do porównań. Główny problem tego systemu to fakt, że nasz podpis zmienia się w miarę upływu czasu. Baza danych wymaga więc stałej aktualizacji lub przechowywania odpowiednio dużej liczby próbek³¹⁶.

Systemy biometryczne w praktyce mogą być wykorzystywane w następujących dziedzinach naszego życia: w służbie zdrowia, gdzie identyfikacja pacjentów odbywała się poprzez wprowadzenie karty mikroprocesorowej (rozważa się, by do uwierzytelniania posiadacza karty wykorzystać jego cechy biometryczne), w zabezpieczeniu krytycznej infrastruktury, w tym dostępu do budynków i systemów, w tworzeniu nowych poziomów bezpieczeństwa dla konsumentów w sektorze bankowym i zróżnicowanych usług opartych na szybkim oraz skutecznym uwierzytelnianiu klienta w miejscu użytkowania.

5.4. Elektroniczna wymiana danych

Przesłankami do zastosowania elektronicznej wymiany danych (EDI) były³¹⁷: wzrastające zainteresowanie logistyką, szczególnie w kwestiach związanych ze skróceniem czasu realizacji zamówień, globalizacja transakcji handlowych, wymuszająca uzgodnienie ogólnościowego standardu dokumentów oraz rozwój technologii komputerowych i obniżenie kosztów ich wykorzystania.

³¹⁵ Por. A. Gupta, N. Patel, S. Khan, *Automatic speech recognition technique for voice command*, [w:] Science Engineering and Management Research (ICSEMR), 2014 International Conference on, 2014, ss. 1-5.

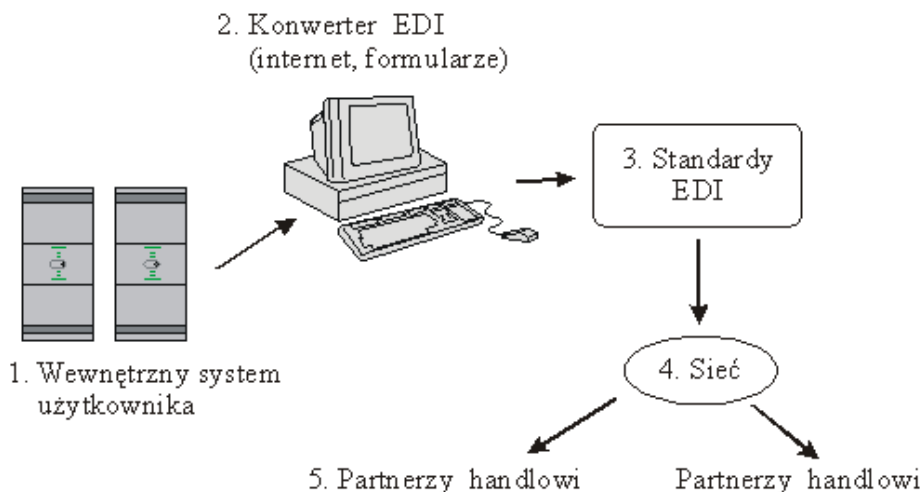
³¹⁶ Por. M.D. Deore, S.M. Handore, *A survey on offline signature recognition and verification schemes*, [w:] Industrial Instrumentation and Control (ICIC), 2015 International Conference on, 2015, ss. 165-169.

³¹⁷ *Logistyka dystrybucji...*, op. cit., s. 223.

Elektroniczna wymiana danych to elektroniczna transmisja standardowo sformatowanych danych między systemami informatycznymi partnerów handlowych przy minimalnym udziale człowieka³¹⁸.

Nowoczesna telekomunikacja oferuje różnorodne możliwości transmisji komunikatów EDI przy wykorzystaniu publicznych sieci telekomunikacyjnych, poprzez prywatne sieci świadczące dodatkowe usługi, tzw. sieci VAN (*Value Added Network*) czy Internet. System EDI jest zbudowany z elementów powiązanych w logiczną sieć (rys. 5.5).

Wspólnym językiem w EDI są standardy, które stanowią zbiór danych i kodów, służących do tworzenia komunikatów zrozumiałych dla zainteresowanych stron, będących w sieci komputerowej. Wśród komunikatów standardowych wyróżniamy cztery podstawowe grupy, co obrazuje załącznik 5.2³¹⁹.



Rys. 5.5. Standardy EDI

Źródło: *Kody kreskowe*, IliM, Poznań 2000, s. 227.

Najpopularniejszymi obecnie standardami EDI są: ANSI X12 oraz UN/EDIFACT (*Electronic Data Interchange For Administration, Commerce and Transport*), posiadające akceptację Rządu Federalnego USA i Organizacji Narodów Zjednoczonych.

W USA głównym standardem jest X12, a w pozostałych krajach EDIFACT. Obecnie wszystkie organizacje odpowiedzialne za standaryzację EDI podjęły decyzję o migracji do standardu EDIFACT.

³¹⁸ *Kody kreskowe i inne globalne standardy w biznesie*, red. nauk. Hałas E., IliM, Poznań 2012, s. 141.

³¹⁹ Por. *Kody kreskowe i inne globalne standardy w biznesie*, red. nauk. Hałas E., IliM, Poznań 2012, ss. 145-147.

Komunikaty (dokumenty) standardu EDIFACT umożliwiają przesyłanie informacji niezbędnych do realizacji transakcji handlowych. Komunikaty te można podzielić na trzy grupy³²⁰:

- komunikaty handlowe (katalog cenowy, zamówienie, faktura), które umożliwiają wymianę informacji pomiędzy sprzedającym i kupującym;
- komunikaty transportowe (zlecenie transportowe, awizo dostawy) używane w celu organizacji dostawy towaru;
- komunikaty finansowe (przelew, informacja o ruchu na koncie) używane do realizowania płatności i informowania o ruchach pieniężnych.

W ostatnich latach intensywnie rozwija się standard dokumentów elektrycznych tworzonych z wykorzystaniem języka XML (*eXtensible Mark-up Language*), który jest uniwersalnym metajęzykiem, umożliwiającym zapisywanie danych wraz z ich strukturą. Funkcjonalność ta jest realizowana przez użycie znaczników (tagów) oraz ich atrybutów, w których są zapisywane konkretne wartości. Pod tym względem sposób zapisu struktury dokumentu XML-owego jest zbliżony do stosowanego w języku HTML systemu znaczników. Od czasu definicji standardu XML 1.0 w 1998 r. obserwuje się jego stale rosnącą popularność, głównie w aplikacjach webowych oraz w zastosowaniach wymiany danych między systemami.

Koncepcyjnie XML jest bardzo zbliżony do EDI i w pewnym sensie stanowi jego rozszerzenie. Z racji swojej uniwersalności umożliwia zarówno obieg danych w ramach systemu jednego przedsiębiorstwa, jak i wielu przedsiębiorstw. Do głównych zalet XML należą³²¹: elastyczność – łatwiejsze zmiany w strukturze komunikatu, niezależność od platformy sprzętowej i systemu operacyjnego – brak konieczności instalacji sieci prywatnych lub VAN, jak w tradycyjnym EDI, integracja z technologiami internetowymi, dostępność narzędzi programistycznych, niskie koszty, możliwość integracji z innymi systemami EDI.

Pomimo powyższych cech, technologia XML obecnie nie jest jeszcze dostatecznie dojrzała, by całkowicie zastąpić EDI. Podstawową wadą XML jest brak jednolitej specyfikacji formatów danych, w przeciwieństwie do dobrze udokumentowanego słownika EDI.

Niewątpliwym atutem XML jest zapis struktur w przejrzystej tekstowej postaci, umożliwiającej szybki i wygodny wgląd w strukturę dokumentu. Stanowi to główny aspekt przemawiający na korzyść XML wszędzie tam, gdzie w procesie przetwarzania i interpretacji danych występuje czynnik ludzki. Ma to znaczenie przede wszystkim w systemach interaktywnej wymiany danych między użytkownikiem a siecią.

³²⁰ Tamże.

³²¹ A. Szymonik, *Informatyka dla ...*, op. cit., s. 124.

5.5. Traceability w logistyce

Traceability, inaczej system TTC (*Track, Trace and Control*), który daje możliwość: śledzenia (prześledzenia) drogi produktu, od momentu jego powstania z surowców, do momentu gdy trafi on do ostatniego klienta w łańcuchu dostaw oraz rejestracji parametrów identyfikujących te dobra oraz wszelkich lokalizacji objętych przepływem.

System TTC stosujemy między innymi w branży żywnościowej, farmacji, sektorze kosmetycznym.

Stosowanie *traceability* w wymienionych obszarach zostało wymuszone rozporządzeniami Komisji UE i ustawami krajowymi (załącznik 5.3).

Traceability pozwala identyfikować dokładnie procesy strumienia rzeczowego realizowanego na rynku dostawców i odbiorców, pod warunkiem, że wszyscy uczestnicy będą stosować te same reguły i unormowania, np. w oparciu o standardy GS1 i wymagania Unii Europejskiej.

Do podstawowych standardów GS1 zaliczamy: identyfikacje jednostek handlowych (towarów) – GTIN (*Global Trade Item Number*), identyfikacje jednostek logistycznych – SSCC (*Serial Shipping Container Code*), identyfikacje lokalizacji – GLN (*Global Location Number*), opis standardów (kody kreskowe, EPC, komunikaty elektroniczne eCom³²² i inne).

Wymienione standardy definiują i zapewniają, że³²³: wszystkie śledzone towary lub ładunki są rozpoznawalne dzięki tym samym zastosowanym identyfikatorom, identyfikacja pozostaje na towarze/ładunku przez cały czas jego śledzenia, wszystkie lokalizacje (punkty modalne) są identyfikowane numerem GLN w całym łańcuchu dostaw, dane o produktach i ich fizycznym przepływie są gromadzone i udostępniane wg uzgodnionych reguł między partnerami handlowymi (np. przez GDSN³²⁴, komunikaty EDI, rozwiązania internetowe EPC IS³²⁵).

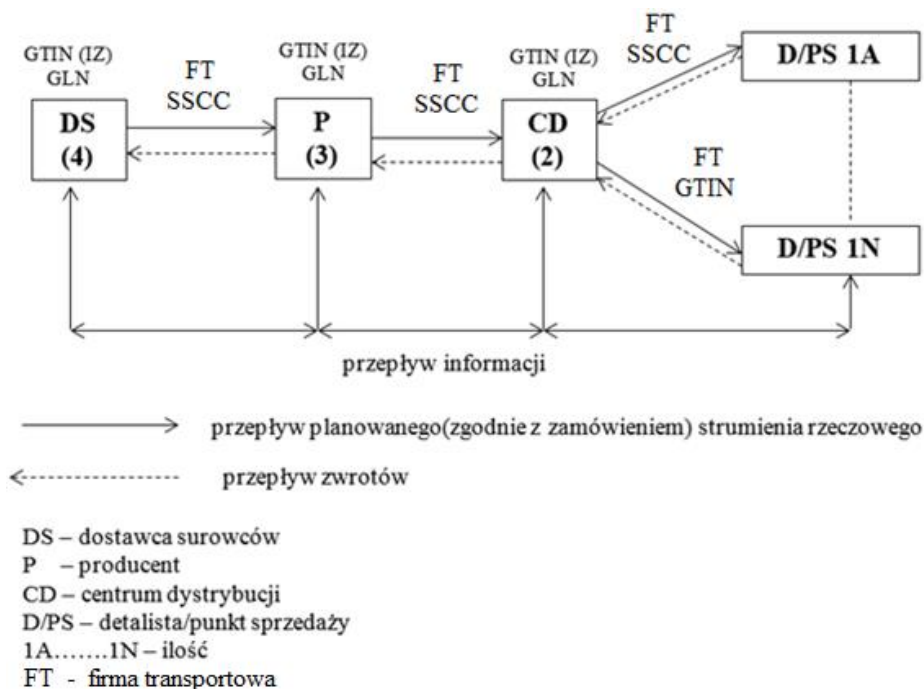
Model funkcjonowania systemu *traceability*, w łańcuchu dostaw, w praktyce przedstawia rys. 5.6.

³²² GS1 eCom to zbiór standardowych komunikatów elektronicznych, które pozwalają firmom na szybkie, sprawne i dokładne przesyłanie danych biznesowych między partnerami handlowymi drogą elektroniczną, w postaci: klasycznych komunikatów Elektronicznej Wymiany Danych – EDI lub w postaci dokumentów XML.

³²³ *Kody kreskowe i inne globalne standardy w biznesie*, red. nauk. ILiM, Poznań 2012, E. Hałas, s. 337.

³²⁴ GDSN (Global Data Synchronisation Network) – sieć globalna synchronizacji danych.

³²⁵ EPC IS *PC Information Service* – serwer umożliwiający użytkownikom wymianę danych między partnerami handlowymi w oparciu o kody EPC. Serwer utrzymuje dane dotyczące EPC, czyli działa jako repozytorium dla EPC i związanych z nimi informacji. Serwer ten używa języka PML.



Rys. 5.6. Model funkcjonowania systemu *traceability* w łańcuchu dostaw

Źródło: opracowanie własne.

Podstawowymi elementami modelu są: detaliści – punkty sprzedaży (1A...1N), centrum dystrybucji (2), producent (3), dostawca surowców (4), firmy transportowe, które fizycznie dostarczają surowce i wyroby odbiorców, system informacyjny zapewniający przepływ informacji pomiędzy ogniwami łańcucha dostaw.

Jeśli model łańcucha dostaw funkcjonuje bez zakłóceń, to przepływ strumienia rzeczowego odbywa się zgodnie z zamówieniami, które składają kolejno detaliści/punkty sprzedaży (1A...1N) do centrum dystrybucji (2), ono do producenta (3), a ten z kolei do dostawcy surowców (4).

W przypadku pojawienia się trudności z jakością wyrobów, zostają uruchomione wcześniej opracowane procedury, które pozwalają na szybkie podjęcie działań, by eliminować powstające zakłócenie. Dzięki zastosowanym standardom i odpowiednim technologiom informatycznym, w przypadku dostarczenia do konsumenta końcowego wadliwego wyrobu, są podejmowane czynności, i tak³²⁶:

³²⁶ Zob. G. Sokołowski, *Traceability – bezpieczeństwo i śledzenie przepływu produktów w łańcuchach dostaw, w oparciu o standardy GS1 i wymagania UE*, ILiM, Poznań 2014, materiały z Webinar – 06.01.2014.

- detalista – punkt sprzedaży (1A):
 - ✓ identyfikuje nazwę wadliwego produktu, jego numer (GTIN), dostawcę (GLN), numer serii produkcyjnej (IZ 10),
 - ✓ przekazuje sygnał do dystrybutora produktu (2),
 - ✓ zabezpiecza wszystkie produkty dotyczące zidentyfikowanej partii przed dalszą sprzedażą;
- centrum dystrybucji (2):
 - ✓ identyfikuje wszystkie produkty (GTIN) dotyczące wadliwej serii produkcyjnej, które aktualnie posiada (IZ 10),
 - ✓ sygnalizuje problem do dostawcy partii produktów (GLN),
 - ✓ informuje odbiorców (GLN) o wadliwej partii produktów (SSCC, IZ 10),
 - ✓ zabezpiecza wadliwą partię produktów przed dalszą dystrybucją;
- producent (3):
 - ✓ identyfikuje surowce związane z anomaliami i identyfikuje ich dostawcę (GLN),
 - ✓ sygnalizuje mu zaistniały problem,
 - ✓ zabezpiecza jeszcze niewysłane partie produktów wytwarzanych ze zidentyfikowanych surowców przed dalszą sprzedażą,
 - ✓ informuje odbiorców (GLN), do których zostały wysłane wadliwe partie produktu (SSCC, IZ 10);
- dostawca surowców (4):
 - ✓ analizuje powód problemu – znajduje i potwierdza przyczynę,
 - ✓ informuje wszystkich odbiorców (GLN) o istocie problemu i ujawnia numer partii surowców (IZ 10),
 - ✓ identyfikuje wszystkie towary wysłane z tych partii dostaw (SSCC),
 - ✓ zabezpiecza pozostałe surowce z tych partii przed dalszym użyciem;
- producent (3) – na podstawie danych historycznych:
 - ✓ odszukuje wadliwe partie produktów, wyprodukowane w przeszłości,
 - ✓ identyfikuje numery SSCC pudeł i palet zawierające partie produktów, które mają być wycofane,
 - ✓ identyfikuje odbiorców (centrum dystrybucji 3) wadliwych wyrobów (GLN) i dostarcza im informacje dotyczące produktów, które mają być zwrócone (SSCC, GTIN, IZ 10);
- centrum dystrybucji – na podstawie dodatkowych danych otrzymanych od producenta (3):
 - ✓ identyfikuje pudła i palety (GTIN, SSCC), które mają być zwrócone,
 - ✓ usuwa i zwraca wadliwe produkty z terenu centrum dystrybucyjnego (GTIN, SSCC),
 - ✓ dostarcza detalistom i punktom sprzedaży (1A...1N) numery SSCC i/lub numery GTIN oraz numery partii wysłanych artykułów, które mają być usunięte;

- detalista – punkt sprzedaży (1A....1N):
 - ✓ detaliści identyfikują podejrzone produkty (znając GTIN, numer partii IZ 10) i zwracają je do dostawcy – centrum dystrybucji (2).

System śledzenia coraz częściej jest również stosowany w: przedsiębiorstwach produkcyjnych, z sektora OEM³²⁷, branży motoryzacyjnej (np. identyfikacja części/komponentów stosowanych w sektorze motoryzacyjnym – prowadzony przez GS1 Niemcy), sektorze finansowym (np. identyfikacja globalnych transakcji – prowadzony przez GS1 US, a więc w USA), branży gastronomicznej (poprawa bezpieczeństwa żywności), służbie zdrowia (np. obsłudze chorego, ewidencji środków trwałych).

Traceability to również system automatycznego śledzenia partii produkcyjnej (rys. 5.7).



Rys. 5.7. Traceability w śledzeniu partii produkcji
Źródło: A. Szymonik, *Informatyka dla ...*, op. cit., s. 129.

Wykorzystując etykiety kodów kreskowych lub RFID, system rejestruje wszystkie operacje wykonywane na danej partii lub produkcie i dzięki temu jest możliwe³²⁸: odtworzenie genealogii produktu (kto, kiedy, na której maszynie, z jakiego surowca, przy jakich parametrach procesu), kontrolowanie poprawności przebiegu procesu (czy zostały wykonane wszystkie czynności, we

³²⁷ OEM (*Original Equipment Manufacturer*), producent oryginalnego wyposażenia – przedsiębiorstwo sprzedające pod własną marką produkty wytworzone przez inne firmy. Termin jest mylący, gdyż OEM nie zawsze jest wytwórcą, a nawet nie jest producentem, lecz czasem tylko sprzedawcą sprzętu dla użytkownika końcowego, choć zdarza się też, że jest jego projektantem.

³²⁸ Zob. A. Szymonik, *Informatyka ...*, op. cit., s. 129.

właściwej kolejności i odstępie czasowym), wyszukanie numerów wszystkich partii, dla których zachodzi podejrzenie nieprawidłowości.

W przedsiębiorstwach produkcyjnych do *traceability* wykorzystuje się między innymi systemy informatyczne klasy MES (*Manufacturing Execution Systems*) – System Realizacji Produkcji³²⁹. System ten wykorzystuje odpowiednie technologie informatyczne, oprogramowanie, elementy automatyki, dane zbierane bezpośrednio ze stanowisk produkcyjnych. Cały proces dzieje się w czasie rzeczywistym, co umożliwia ich transfer do obszaru biznesowego³³⁰.

Dzięki funkcjonalności systemu można uzyskać natychmiastowy sygnał zwrotny o stopniu wykonania produkcji, podejmować na bieżąco właściwe decyzje i reagować na bieżąco na nieprawidłowości pojawiające się w czasie procesu produkcyjnego. Pozyskane dane z procesu produkcyjnego pozwalają na analizę kluczowych wskaźników efektywności produkcji i uzyskanie prawdziwego obrazu wykorzystania zdolności produkcyjnych.

Do przykładowych funkcji systemu klasy MES możemy zaliczyć³³¹: śledzenie przepływu, genealogię produkcji, śledzenie i wizualizację produkcji w toku w czasie rzeczywistym, śledzenie rzeczywistego czasu i wydajności pracy maszyn i ludzi, śledzenie przestojów, rejestrację przyczyn przestojów, planowanie wykonania zleceń produkcyjnych i kontrolę ich wykonania na poziomie operacyjnym, aktualizację stanów magazynów materiałów, półproduktów, produktów finalnych, zbieranie informacji o jakości produkcji, generowanie automatycznych raportów, analizę zgromadzonych informacji, rozliczenia kosztów produkcji.

5.6. Bezpieczeństwo procesów informacyjnych

Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego w kontekście logistyki nie jest możliwe bez zapewnienia informacyjnej ciągłości działania³³². Także funkcjonowanie bezpieczeństwa logistyki na korzyść podmiotu bezpieczeństwa jest w znacznym stopniu uzależnione od narastających i nabierających na sile zagrożeń dla procesów

³²⁹ Por. I. Chao, Q. Li, *Manufacturing Execution Systems (MES) assessment and investment decision study*, [w:] *Systems, Man and Cybernetics*, 2006. SMC'06. IEEE International Conference on, 2006, Volume: 6, ss. 5285- 5290.

³³⁰ Por. Z. Banaszak, S. Kłós, J. Mleczo, *Zintegrowane systemy zarządzania*, PWE, Warszawa 2011, s. 179.

³³¹ Tamże, ss. 180, 181.

³³² Por. P. Zaskórski, *Informacyjna ciągłość działania determinantą bezpieczeństwa organizacji*, [w:] *Nie-bezpieczny świat Systemy Informacja Bezpieczeństwo*, AON, Warszawa 2015, s. 450.

informacyjnych, dotyczących gromadzenia, analizowania, przechowywania i udostępniania danych.

Pod pojęciem bezpieczeństwa informacyjnego można rozumieć ogół metod, środków i procedur mających na celu niedopuszczenie do zniszczenia, utraty, kopiowania i modyfikacji treści informacji³³³. Bezpieczeństwo w kontekście zasobów i procesów informacyjnych jest rozumiane przez siedem atrybutów³³⁴.

1. Dostępność – oznacza niczym nieograniczoną możliwość korzystania z informacji w procesie informacyjnym przez uprawnionych do tego użytkowników. Informacja powinna być zatem dostępna dla osób upoważnionych w określonym miejscu i czasie. Naruszenie dostępności może być efektem działań nieupoważnionego użytkownika, błędów popełnionych przez osobę zaangażowaną w realizację procesu informacyjnego, a także wynikiem awarii, zakłóceniem transmisji, błędów oprogramowania. Utrata dostępności może być skutkiem zdarzeń losowych, jak i działań celowych.

2. Poufność – oznacza niedostępność informacji dla wszystkich podmiotów nieuprawnionych. Jednym ze sposobów zapewnienia poufności jest szyfrowanie danych. Utrata poufności może być skutkiem zarówno niewłaściwego zabezpieczenia, jak i celowego ataku. Procesom informacyjnym, w których ujawnienie informacji byłoby kosztowne, przypisuje się odpowiednio wysoki poziom bezpieczeństwa.

3. Integralność – informacja nie może zostać zmieniona lub zniszczona przez osoby do tego nieuprawnione. Integralność może być naruszana poprzez nieuprawnionego użytkownika, błędy lub zaniedbania osób odpowiedzialnych za realizację procesu informacyjnego. Utrata integralności może być skutkiem błędów w procesie przetwarzania informacji, zakłóceń, wirusów, błędów oprogramowania.

4. Niezawodność – spójność, zamierzone zachowania.

5. Autentyczność – właściwość zapewniająca tożsamość informacji zgodną z deklaracją, autentyczność, jest efektem kontroli czy ktoś lub coś jest tym lub czymś, za kogo się podaje.

6. Tajność – stopień ochrony danych.

7. Rozliczalność – właściwość zapewniająca, że działanie podmiotu może być jednoznacznie przypisane tylko temu podmiotowi.

³³³ Por. M. Pałęga, *Bezpieczeństwo informacji w logistycznym systemie informatycznym klasy CRM*, [w:] *Logistyka* 2014/3, ss. 4931-4936.

³³⁴ Por. J. Ejdys, A. Lulewicz, J. Obolewicz, *Zarządzania bezpieczeństwem w przedsiębiorstwie*, PB, Białystok 2008, s. 157.

Bezpieczeństwo procesu informacyjnego jest zapewnione, jeżeli istnieje możliwość sprawnego i poufnego gromadzenia informacji, ich przetwarzania, przetrzymywania, przesyłania³³⁵, wykorzystując środki bezpieczeństwa, czyli zabezpieczenia technologiczne i środki organizacyjne, które można zastosować dla komputerów, programów, danych, procesów i ich użytkowników w celu zapewnienia ochrony interesów przedsiębiorstwa oraz poufności indywidualnej³³⁶.

Zagrożenia

Przy swobodnym przepływie informacji i wysokiej dostępności wielu zasobów, osoby korzystające z sieci informatycznych muszą zrozumieć wszelkie możliwe zagrożenia, które należy utożsamiać z potencjalnymi incydentami, których skutkiem są szkody dla podmiotu bezpieczeństwa³³⁷.

Włamanie się do systemów następuje z wielu powodów, najczęściej w celu uzyskania poufnych danych (z reguły dla korzyści materialnych), osiągnięcia uznania w kręgu własnej społeczności lub zakłócenia pracy serwera w sieci technikami DoS (*Denial of Service*)³³⁸.

Przy próbie penetracji systemu działania przebiegają w sposób systematyczny, zazwyczaj metodą kolejnych kroków. Na kroki te składają się: rozpoznanie systemu, wejście do systemu, wykorzystanie słabych punktów systemu, uzyskanie dostępu do zasobów, opanowanie systemu lub wyprowadzenie z niego interesujących hackera informacji, zatarcie śladów włamania i pozostawienie w systemie luki umożliwiającej ponowne włamanie.

Zagrożenia te mogą przyjmować różne formy, ale wynikiem wszystkich jest pewna utrata prywatności i być może zniszczenie informacji oraz zasobów, które mogą prowadzić do strat materialnych.

Według danych opublikowanych przez IDC³³⁹ ilość włamań oraz przestępstw komputerowych gwałtownie rośnie, a około 80% wszystkich ataków przeprowadzają partnerzy, obecni i byli pracownicy. Wykres 5.1 przedstawia liczbę ujawnionych, udanych włamań do systemów, a wykres. 5.2 – liczbę incydentów zgłaszanych w latach 2005-2011.

³³⁵ Por. M.E. Whitman, H.J. Mattord, *Reading and cases in the management of information security*, Thomson Course Technology, Boston 2006, s. 142.

³³⁶ Por. P. Sienkiewicz, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, AON, Warszawa 2008, ss. 89-90.

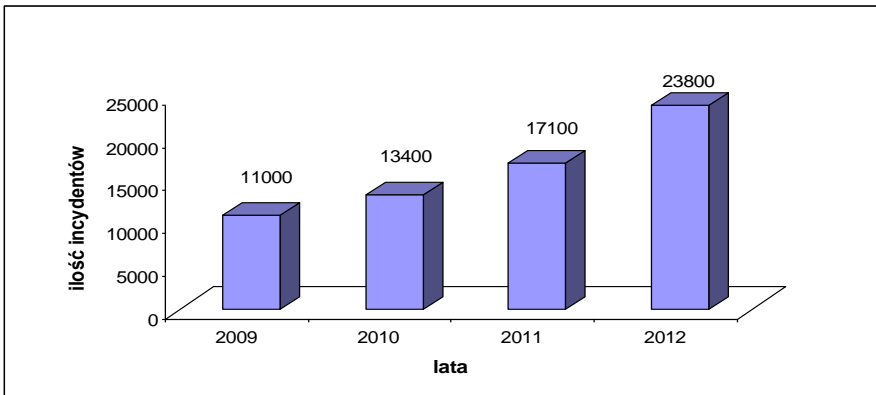
³³⁷ Por. T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania. Business continuity management*, Difin, Warszawa 2009, s. 271.

³³⁸ Por. V.D. Katkar, S.V. Kulkarni, *Experiments on detection of Denial of Service attacks using ensemble of classifiers*, [w:] Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on, 2013, ss. 837-842.

³³⁹ IDC (*International Data Corporation*) – organizacja zajmująca się badaniem rynku, specjalizuje się w technologiach ICT.

Wykres 5.1

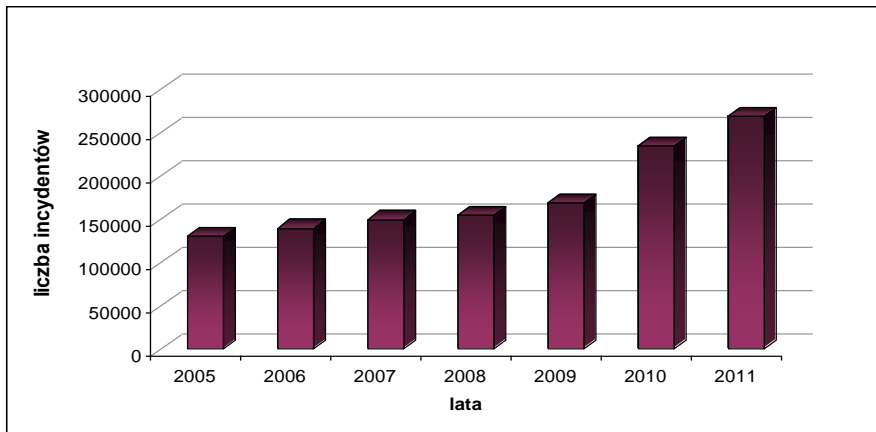
Liczba udanych ataków hackerskich



Źródło: opracowanie własne na podstawie *Hakerzy kosztują nas co roku 100 milionów złotych*, <http://interaktywnie.com/biznes/artykuly/>, 22.07.2014.

Wykres 5.2

Liczba incydentów zgłaszanych w latach 2005-2011



Źródło: A. Szymonik, *Informatyka dla ...*, op. cit., s. 169.

Coraz częściej do publicznej wiadomości podaje się informacje o spustoszeniach, jakie wynikają z kradzieży danych. A oto przykłady³⁴⁰:

³⁴⁰ B. Mszyca, D. Szyller, M. Fabjański, *Cyberprzestępcy ukradli dane klientów UPS*, <http://www.ekonomia.rp.pl/>, 30.01.2015.

1. United Parcel Service (UPS)³⁴¹ poinformowała, że w wyniku działań cyberprzestępców doszło do wycieku danych w 51 oddziałach firmy na terenie Stanów Zjednoczonych. Problem dotyczy około 105 tys. transakcji. Według przedstawicieli UPS w efekcie włamania do systemów komputerowych firmy mogło dojść do kradzieży danych kart kredytowych i debetowych jej klientów, ich nazwisk, adresów pocztowych i e-mailowych. Cyberprzestępcy przeprowadzili operację pomiędzy 20 stycznia a 11 sierpnia 2014.
2. W kwietniu 2014 roku, firma Community Health Systems, która zarządza 206 szpitalami w 29 amerykańskich stanach poinformowała, że cyberprzestępcy wykradli dane 4,5 mln pacjentów. Wśród nich znajdowały się m.in. nazwiska pacjentów, ich adresy, daty urodzenia, numery telefonów czy numery Social Security. Według zapewnień Community Health Systems, łupem hakerów nie padły numery kart kredytowych pacjentów ani ich dokumentacja medyczna. Za atakami stoją najprawdopodobniej chińscy hakerzy.
3. Łupem cyberprzestępców padło 1,2 mld haseł i loginów oraz ponad 500 mln adresów e-mail. O sprawie poinformował jako pierwszy „New York Times”, powołując się na raport zajmującej się bezpieczeństwem Hold Security z amerykańskiego Milwaukee. Firma nie ujawnia konkretnych nazw stron, z których wykradzono dane, ale wiadomo, że problem dotyczy 420 tys. stron internetowych. Hakerzy nie atakowali tylko amerykańskich firm, ich celem były wszystkie witryny, na jakie mogli się włamać, poczynając od przedsiębiorstw znajdujących się na liście Fortune 500, a kończąc na bardzo małych stronach.

Z danych opublikowanych w sierpniu 2014 roku przez *New York Times* wynika, że kradzież danych jest coraz bardziej kosztowna dla podmiotów, które dotyka ten proceder. Powołując się na wspólny raport *Ponemon Institute* oraz IBM gazeta wskazuje, że w ujęciu rok do roku przeciętna strata wynikająca z takiej kradzieży wzrosła o 15 proc. O ile w 2013 r. była to kwota średnio 3,1 mln dol., to w 2014 wynosi ona już 3,5 mln dolarów.

Do czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji należy zaliczyć³⁴²: rozproszenie zasobów teleinformatycznych na dużym terenie, eksploatawanie nielicencjonowanego sprzętu komputerowego, eksploatawanie „pirackiego” oprogramowania (systemowego i użytkowego), stosowanie do ochrony informacji niewłaściwych środków ochrony (mechanizmów programowych i urządzeń technicznych), stosowanie sprzętu i oprogramowania niesprawdzonego na obecność tzw. „pluskiew” programowych i sprzętowych (należy stosować sprzęt i oprogramowanie od uznanych dostawców lub

³⁴¹ UPS to jedna z największych na świecie firm zajmujących się przewozem przesyłek i logistyką.

³⁴² A. Szymonik, *Informatyzacja zarządzania logistycznego*, Bellona, Warszawa 2005, s. 117.

rekomendowanych przez jednostki certyfikujące), niechęć użytkowników i projektantów do stosowania środków ochrony informacji.

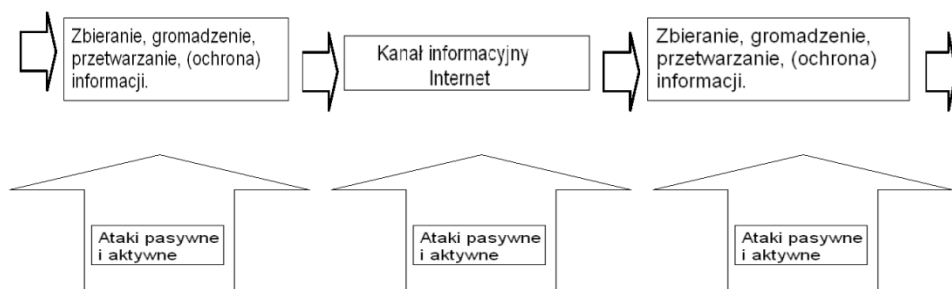
Ataki na sieci informatyczne są prowadzone w różnych miejscach (rys. 5.8). Dotyczą one zarówno obszarów gromadzenia, przetwarzania, przechowywania, ale także przesyłania i udostępniania informacji i danych.

Nie jest możliwe, by opisać każdy atak sieciowy, bowiem jest ich cała gama i występują pod różną postacią. Taktyka działania jest zmienna i zależy od umiejętności hackera oraz rodzaju atakowanego celu, a także od jego słabych punktów.

Zagrożenia dla systemu informacyjnego pod względem źródła pochodzenia można podzielić na³⁴³: losowe (np. temperatura, wilgotność, zanieczyszczenia, zakłócenia systemu zasilania, kataklizmy, wojna, błędy operatora, błędy administratora, wadliwa konfiguracja systemu, zaniedbania, defekty struktury, sprzętu); intencjonalne (świadome i zamierzone).

Jednym z podstawowych rodzajów ataków jest wyszukanie konkretnego IP za pomocą skanera sieciowego, a następnie gdy już „ofiara” będzie upatrzona, skorzystanie z całej palety narzędzi do włamania się. Ogólnie można podzielić atak na: pasywny i aktywny.

Pasywny – polega na przechwytywaniu określonych pakietów danych, które przepływają siecią. Przeważnie stosuje się do tego sniffery, jak również ich zaawansowane modyfikacje, automatycznie „tłumaczące” pakiety. Ataki takie są bardzo trudne do wykrycia, teoretycznie jest to możliwe, ale nie sposób przewidzieć czasu podsłuchu sieci i skutecznie się bronić. Programy wykrywające sniffery trochę „opóźniają” przepływ informacji, ale dla masowego użytkownika jest to prawie niezauważalne. Z drugiej strony człowiek, który z każdym kliknięciem myszki chciał sprawdzać czy nie jest podsłuchiwany mógłby czuć duży dyskomfort pracy.



Rys. 5.8. Uproszczony schemat informacyjny z miejscami narażonymi na ataki aktywne i pasywne

Źródło: opracowanie własne.

³⁴³ Por. A. Szymonik, *Technologie informatyczne w logistyce*, Placet, Warszawa 2010, s. 171.

Aktywny – polega na bezpośrednim naruszeniu bezpieczeństwa naszego systemu poprzez atak, wykorzystujący słabe luki systemu operacyjnego lub jakiegos̄ uruchomionego programu. Jako przykład moŹe posłuŹyć tutaj mechanizm udostępniania plików i folderów. Często zdarza się, Źe uŹytkownik nie stosuje Źadnego hasła, co jest zachęta dla hackera i zwykłym niedbalstwem. Tego rodzaju atak stosuj również konie trojańskie, które podrzucione niepostrzeŹenie do komputera ofiary praktycznie otwieraj nieograniczony dostę do niego.

Innym podziałem jest ich klasyfikacja na ataki skierowane i losowe.

Atak skierowany – w przypadku tego rodzaju ataku mamy do czynienia z konkretnym komputerem o wiadomym IP (uzyskanym np. dzięki skanowaniu sieci) lub okrešlon grup (sieci) komputerów. Wartościowe informacje przy tego rodzaju ataku uzyskujemy dzięki samemu mechanizmowi DNS³⁴⁴ (np. traceret, whois itd.). Jest to skomplikowana procedura i zwykle podstawowe środki zapobiegawcze mog nie być skuteczne. Ataku skierowanego nie planuje się ad hoc, trzeba poznać ofiarę, znaleźć jej słabe punkty. Dlatego teŹ, aby wykryć dziury, trzeba się wczuć w hackera i sprawdzać po kolei niezabezpieczone miejsca naszego systemu. RównieŹ waŹne jest, by nie pobierać oprogramowania z niewiadomego Źródła, bo nigdy nie wiadomo co jest „przyczepione” do naszego pliku .exe (instalki – wykonywalnego).

Atak losowy – jest najczęściej stosowany przez hackerów, gdyŹ jedynym (głównym) kryterium jego wyboru jest skanowanie sieci i szukanie takiego IP (komputera), który jest słabo zabezpieczony.

W sieciach komputerowych techniki ataków moŹna sklasyfikować w trzech kategoriach³⁴⁵: sieciowe, na system operacyjny, na aplikacje.

Ataki sieciowe dotycz infrastruktury komunikacyjnej, a ich celem mog być urzdzenia sieciowe, takie jak rutery i przełczniki, a takŹe protokoły warstwy sieci na serwerze (*warstwa 3*).

Celem ataku sieciowego jest zazwyczaj uzyskanie uprawnień pozwalajcych na manipulowanie ustawieniami konfiguracyjnymi, majcymi wpływ na trasowanie ruchu komunikacyjnego. Ataki w warstwie 3 lub niŹszej – często s to ataki typu DoS (*Denial of Service*) – dotycz modułów oprogramowania sieciowego na serwerze. W tym przypadku celem jest załamanie serwera lub, co najmniej, znaczne spowolnienie jego pracy.

Now odmian DoS jest technika DDoS (*Distributed Denial of Service*), w której szereg agentów rozproszonych w sieci przypuszcza taki atak DoS na wybrany serwer. Moduły agentów s rozsyłane przez hakera do opanowanych przez niego komputerów – najczęściej w Internecie – i uaktywniane w odpo-

³⁴⁴ DNS pełni funkcję systemu informacji o adresach oraz tłumaczy adresy symboliczne (np. www.katowice.com.pl/) na adresy IP.

³⁴⁵ *Vademecum teleinformatyka II*, Praca zbiorowa, wydanie specjalne Networld, Wyd. IDG Poland S.A., Warszawa 2002, s. 177.

wiednim czasie dla wykonania skoordynowanego ataku na wybrany cel, podjęcia działań oszustwa, spenetrowania cudzych zasobów bądź przejęcia nad nimi kontroli³⁴⁶.

Ataki na system operacyjny wykorzystują cały szereg błędów i luk w powszechnie stosowanych systemach operacyjnych. Najczęściej wykorzystywany jest atak na konto super użytkownika (*root* w systemach *Unix* czy *administrator* w systemach *Microsoft Windows*). Taki uprzywilejowany użytkownik posiada uprawnienia do wykonania wszystkich operacji w systemie – może więc mieć dostęp do wszystkich plików (*łącznie z systemowymi*) i urządzeń, tworzyć nowych użytkowników i nadawać im uprawnienia.

Większość technik uzyskiwania uprawnień superużytkownika wykorzystuje tzw. efekt przepełnienia bufora. Technika ta pozwala hackerowi na wprowadzenie swojego kodu do innego programu pracującego na komputerze i wykonaniu go w kontekście uprawnień przewidzianych dla tego programu. Zazwyczaj taki podrzucony kod zakłada konto nowego, uprzywilejowanego użytkownika. Umożliwia to hackerowi legalne wejście do systemu przez zalogowanie się jako ten nowy użytkownik.

Ataki aplikacyjne – wraz z rozwojem Internetu pojawiły się powszechnie stosowane aplikacje, takie jak serwery webowe, serwery poczty elektronicznej czy serwery DNS. Takie aplikacje są idealnym celem, ponieważ – z definicji – są nastawione na ciągle oczekiwanie na komunikację wchodzącą z Internetu, a użytkownicy zewnętrzni mogą uzyskiwać do nich dostęp z każdego miejsca w sieci.

Na pierwszy ogień idą przeważnie serwery webowe. Do ataku na serwer webowy są wykorzystywane odpowiednio przygotowane zlecenia HTTP, uznawane za legalne z punktu widzenia zapory ogniowej, ale przygotowane do wykorzystania słabych punktów serwera i uzyskania dostępu do poufnych informacji zgromadzonych w bazach danych lub wykonania własnego programu na zaatakowanym serwerze webowym.

Inne sposoby ataków są związane z programami CGI (*Common Gateway Interface*). Programy te są podstawowym środkiem do implementacji aplikacji webowych. Serwer webowy po otrzymaniu zlecenia CGI wywołuje odpowiedni program, przekazując do niego otrzymane parametry. Błędy projektowe, popełniane często na etapie tworzenia takich programów, zwłaszcza w zakresie kontroli zakresu danych, stwarzają okazję do ataków.

Innym przypadkiem są serwery DNS, po opanowaniu których można łatwo manipulować bazą adresową Internetu, kierując poufne informacje pod podmienione adresy fizyczne.

Nie jest możliwe by opisać każdy atak sieciowy, który występuje pod różnymi postaciami i technikami działania. Może on być przeprowadzony na

³⁴⁶ Zob. M. Szmít, M. Gusta, M. Tomaszewski, *101 zabezpieczeń przed atakami w sieci komputerowej*, Helion, Gliwice 2005, s. 155.

różne sposoby w zależności od rodzaju atakowanego celu oraz od jego słabych punktów.

Główne rodzaje ataków:

1. Przepelnienie bufora (*Buffer overflow*)³⁴⁷ – jest popularną metodą ataku na serwery internetowe. Jest ono możliwe, gdy oprogramowanie serwera aplikacji zawiera błędy logiczne, które mogą być wykorzystane przez włamywacza do wysyłania łańcuchów danych o rozmiarach przekraczających bufor wejściowy. Można w ten sposób uzyskiwać uprawnienia do zasobów serwera i wykonywać własne programy na serwerze. Wyszukiwanie hostów podatnych na tego typu ataki odbywa się zwykle metodą skanowania portów, umożliwiającą znalezienie komputerów, na których jest uruchomiona dana usługa, a w dalszej kolejności wykorzystanie słabych punktów (luk) w zabezpieczeniach systemu operacyjnego.

2. Wirusy, robaki i konie trojańskie – specyficzna grupa programów, które w złej intencji udostępniają, zmieniają lub usuwają dane zarażonego komputera. Są zazwyczaj niewielkie, co utrudnia ich wykrycie, ale w kodzie zawierają funkcje i polecenia mogące zaszkodzić właścicielowi zarażonego komputera – od szpiegowania i przechwytywania danych osobistych po usuwanie plików z dysku. Dzieli się je na trzy podstawowe grupy: trojany (konie trojańskie), robaki i wirusy³⁴⁸.

Wirusy to programy zajmujące się reprodukcją i przenoszeniem się na inne komputery. Infekują pliki lub bootsektory nośników danych. Przemieszczają się niezauważone na dyskietkach, dyskach, przez sieci komputerowe (także Peer-to-Peer), pocztą elektroniczną lub przez zwykłe pobieranie plików z Internetu. Umieszczają swoje kopie w różnych miejscach na dysku i działają na różne sposoby³⁴⁹.

Robak (*worm*) to program, którego głównym celem jest rozprzestrzenianie się za pośrednictwem sieci komputerowej. Po przemieszczeniu robak dalej się przemieszcza (jeżeli jest taka możliwość, np. wykorzystanie osób z książki adresowej programu pocztowego i wysłanie do nich swojej kopii) oraz może wykonać określone przez jego autora zadania.

Konie trojańskie to szkodliwe programy, które nie potrafią się automatycznie kopiować. Są one tworzone w celu uzyskania zdalnego dostępu do komputerów będących celem ataku. Po zainstalowaniu konia trojańskiego haker może zdalnie korzystać z komputera i wykonywać praktycznie dowolne operacje. To, jakie operacje są możliwe, zależy od właściwości konia trojańskiego oraz uprawnień użytkowników skonfigurowanych na zaatakowanym komputerze. Często będzie to: modyfikowanie plików, kradzież danych

³⁴⁷ Por. *Vademecum teleinformatyka II...*, op. cit., s. 180.

³⁴⁸ Por. A. Szymonik, *Technologie informatyczne ...*, op. cit., 176.

³⁴⁹ Tamże.

(danych osobowych, kart kredytowych, haseł itp.), rejestrowanie sekwencji klawiszy, instalowanie innego oprogramowania (w tym szkodliwego)³⁵⁰.

3. Malware (*MALicious software*, złośliwe oprogramowanie) – to wszelkie aplikacje, skrypty, których intencją jest złośliwe, szkodliwe bądź przestępcze działanie. Malware stanowi jedno określenie na wszelkie rodzaje złośliwych kodów, takich jak np. wirusy, robaki, trojany, spyware. Istnieje bardzo wiele różnych rodzajów złośliwego oprogramowania oraz sposobów ich działania i rozpowszechniania się. Chociażby w zależności od sposobu rozprzestrzeniania się i infekcji czy w zależności od skutków, jakie wywołują, czyli te groźniejsze i mniej niebezpieczne. Złośliwe programy często mają postać mieszaną, czyli łączą w sobie kilka różnych funkcji (tzw. hybrydowe), np. mogą rozpowszechniać się jak robak i zawierać funkcje trojana oraz infekować na różne sposoby. Do malware zaliczamy wiele rodzajów złośliwych kodów, takich jak: virus, worm, spyware, adware, trojan, rootkit, backdoor, keylogger³⁵¹.

4. Sieci botnet – sieć komputerów złożona z maszyn zainfekowanych szkodliwym backdoorem, który umożliwia cyberprzestępcom zdalną kontrolę nad zainfekowanymi komputerami (może to oznaczać kontrolowanie pojedynczej maszyny, niektórych komputerów tworzących sieć lub całą sieć)³⁵².

Botnety posiadają potężną moc obliczeniową. Stanowią potężną cyberbroń i skuteczne narzędzie do nielegalnego zarabiania pieniędzy. Właściciel botnetu może kontrolować komputery tworzące sieć z dowolnego miejsca na świecie – z innego miasta, państwa, a nawet kontynentu. Internet jest skonstruowany w taki sposób, że jest możliwe kontrolowanie botnetu anonimowo.

Komputery zainfekowane botem mogą być kontrolowane bezpośrednio albo pośrednio. W przypadku pośredniej kontroli, cyberprzestępca ustanawia połączenie z zainfekowaną maszyną i zarządza nią za pomocą wbudowanych do programu bota poleceń. W przypadku bezpośredniej kontroli, bot łączy się z centrum kontroli lub z innymi maszynami w sieci, wysyła żądanie, a następnie wykonuje zwrócone polecenie.

Właściciel zainfekowanej maszyny zwykle nawet nie podejrzewa, że komputer jest wykorzystywany przez cyberprzestępców. To dlatego komputery zainfekowane botem i potajemnie kontrolowane przez cyberprzestępców nazywane są również zombie. Sieci złożone z zainfekowanych maszyn są

³⁵⁰ Tamże.

³⁵¹ Zob. M. Szmit, M. Tomaszewski, D. Lesiak, I. Politowska, *13 najpopularniejszych sieciowych ataków na twój komputer*, Helion, Gliwice 2008, s. 77.

³⁵² Por. M., Feily, A. Shahrestani, S. Ramadass, *A Survey of Botnet and Botnet Detection*, [w:] *Emerging Security Information, Systems and Technologies*, 2009. SECURWARE '09. Third International Conference on, 2009, ss. 268-273.

określane jako sieci zombie. Większość maszyn zombie to komputery PC użytkowników domowych³⁵³.

5. Falszowanie adresu IP (*IP Address Spoofing*)³⁵⁴ – technika ta polega na podszywaniu się osoby nieuprawnionej pod zaufane adresy IP w celu przejścia przez system ochrony opierający się wyłącznie na adresach komputerowych IP. Większość ścian ogniowych wykrywa i zapobiega przekazywaniu pakietów z fałszywym adresem zwrotnym³⁵⁵.

6. Łatwe hasła³⁵⁶ – programy do łamania haseł są zdolne do wypróbowania tysięcy kombinacji haseł w ciągu minuty i mogą wykorzystać fakt niewłaściwie wybranego hasła w celu przejęcia konta użytkownika lub, w gorszym przypadku, administratora. Aby się przed tym zabezpieczyć, stosuje się politykę wymuszania zmian haseł i używania haseł „trudnych” (tzn. w postaci fraz, a nie pojedynczych wyrazów, z wykorzystaniem znaków specjalnych). Hasła stosuje się też dla ruterów, przełączników i innego wyposażenia infrastruktury sieciowej.

7. Uprowadzenie sesji (*Session Hijacking*)³⁵⁷ – odgadując numer sekwencyjny IP, włamywacz przejmuje istniejące połączenie między dwoma komputerami i gra rolę jednej strony takiego połączenia. Legalny użytkownik zostaje rozłączony, a włamywacz „dziedziczy” możliwość dostępu do danych w aktualnej sesji. Możliwość taką stwarza niewłaściwa implementacja randomizacji (*zabieg polegający na losowym przypisaniu podmiotów do grupy badanej lub kontrolnej tak, by główne charakterystyki obu grup były takie same*) numerów sekwencyjnych w stosie protokołów TCP/IP systemu operacyjnego³⁵⁸.

8. Namierzanie sieci (*Network Snooping*) – ten rodzaj ataku jest przez wielu uważany za najbardziej wyrafinowaną metodę ataku. Do jej przeprowadzenia wykorzystuje się różnego rodzaju analizatory sieci, dzięki którym potencjalny włamywacz wybiera taką metodę ataku, która w danym przypadku będzie najbardziej efektywna. Bardzo często *Network Snooping* sprowadza się do analizowania protokołów czy śledzenia ruchu sieciowego – włamywacz szuka najsłabszego punktu danej sieci czy serwera pod kątem stosowanych zabezpieczeń, aby następnie wykorzystać ów słaby punkt za pośrednictwem

³⁵³ Zob. M. Szmit, M. Tomaszewski, D. Lesiak, I. Politowska, *13 najpopularniejszych ...*, op. cit., s. 114.

³⁵⁴ *Vademecum teleinformatyka II ...*, op. cit., s. 180.

³⁵⁵ Por. J. Bi, B. Liu, J. Wu, Y. Shen, *Preventing IP source address spoofing*, [w:] *A two-level, state machine-based method*, Tsinghua Science and Technology, 2009, Volume 14, Issue 4, ss. 413-422.

³⁵⁶ Tamże, s. 180.

³⁵⁷ Tamże, s. 180.

³⁵⁸ Por. W. Yongle, Ch. JunZhang, *Hijacking spoofing attack and defense strategy based on Internet TCP sessions*, [w:] *Instrumentation and Measurement, Sensor Network and Automation (IMSNA)*, 2013 2nd International Symposium on, 2013, ss. 507-509.

określonej techniki włamaniowej, np. sniffing (podsluch sieciowy). Tak więc *Network Snooping* jest bronią, która przygotowuje do przeprowadzenia innego skutecznego ataku. Odmianą *Network Snooping*u jest technika zwana próbkowaniem (ang. *probe*) polegająca na przeprowadzeniu wywiadu oraz uzyskiwaniu dostępu do obiektu i badanie jego charakterystyki. Działanie to jest na tyle niebezpieczne, iż pozostaje praktycznie niezauważalne, gdyż jest przeprowadzane poprzez legalne formy dostępu. W ten sposób są zbierane wrażliwe informacje wystawione na światło dzienne, przez co działanie takie nie jest wychwytywane przez standardowe systemy zabezpieczeń. Wprawny intruz przygotowujący atak zazwyczaj potrzebuje przeprowadzenia jednorazowego badania systemu, by wstępnie oszacować metody przeprowadzenia skutecznego ataku na system³⁵⁹.

9. Tylne drzwi (*Back Door*) – aplikacja, która umożliwi swojemu autorowi wielokrotny nieautoryzowany dostęp do zdalnego systemu po uprzednim zdobyciu na nim praw administratora (bądź adekwatnie od sytuacji, przydzielenie odpowiednich praw „złośliwej aplikacji”)³⁶⁰. Mogą to być np. konta użytkownika z uprawnieniami administratora. Jednym ze sposobów wprowadzenia tylnego wejścia do systemu jest utworzenie konta lub procesu umożliwiającego uruchomienie innych programów z uprawnieniami super użytkownika. Liczba możliwych tylnych wejść dla każdej platformy jest praktycznie nieograniczona. Zastąpienie jednej z usług konkretnym programem, czy też podstawienia z uprawnieniami superużytkownika, umożliwi przejęcie kontroli nad systemem³⁶¹.

10. Odmowa usługi (*DoS-Denial of Service*)³⁶² – Atak typu DoS – Denial of Service jest jednym ze skuteczniejszych sposobów unieruchomienia serwera sieciowego. Głównym celem takiego ataku jest częściowe zablokowanie dostępu do wybranych usług, np. www czy e-mail, lub całkowite unieruchomienie serwera. W skrajnych przypadkach dochodzi nawet do zupełnego zawieszenia pracy systemu – co wymaga podniesienia takiego systemu poprzez fizyczną interwencję administratora, czyli „reset”. Atak ten polega na wysyłaniu w krótkim czasie bardzo dużej ilości zapytań do serwera sieciowego. Serwer na każde zapytanie stara się odpowiedzieć, hacker natomiast, nie czekając na

³⁵⁹ Por. P. Krawaczyński, D. Zelek, *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, <http://hackme.pl/>, 30.01.2015.

³⁶⁰ Por. K. Alminshid, M.N. Omar, *Detecting backdoor using stepping stone detection approach*, [w:] Informatics and Applications (ICIA), 2013 Second International Conference on, 2013, ss. 87-92.

³⁶¹ Tamże.

³⁶² Por. *Vademecum teleinformatyka II ...*, op. cit., s. 186; Z. Fu, *Mitigating Distributed Denial-of-Service Attacks*, [w:] Application-Defense and Network-Defense Methods, Computer Network Defense (EC2ND), 2011 Seventh European Conference on, 2011, ss. 59-59.

odpowieź ze strony serwera, ciągle wysyła kolejne zapytania. Doprowadza to do sytuacji, w której serwer jest wręcz „zalany” zapytaniami i nie nadaje z odpowiedziami. Wzrasta obciążenie systemu i kiedy ilość zapytań przekroczy możliwości obliczeniowe serwera, następuje jego blokada.

11. Inżynieria społeczna, inżynieria socjalna³⁶³, socjotechnika – w bezpieczeństwie teleinformatycznym zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę. Hackerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników systemów informatycznych, aby pokonać zabezpieczenia odporne na wszelkie formy ataku. Wyszukują przy tym najsłabszy punkt systemu bezpieczeństwa, którym jest człowiek.

Komputerowi oszuści często podają się za inne osoby, aby wyłudzić od swoich ofiar cenne dane. Cracker może na przykład podać się za administratora banku i przesłać ofiarom adres swojej strony, która łudząco przypomina stronę banku internetowego. Dzięki opanowaniu inżynierii socjalnej oszust wie, że przeciętny użytkownik nigdy nie sprawdza, czy strona jego banku jest oznaczona kłódką symbolizującą nawiązanie bezpiecznego połączenia. Nieostrożni klienci pozostawiają internetowemu złodziejowi swoje dane, które ten może wykorzystać do oczyszczenia ich kont z pieniędzy. Działanie opisane w tym przykładzie jest określane nazwą „phishing”.

Wielkie korporacje wydają ogromne sumy na zapewnienie sobie informatycznego bezpieczeństwa. Koszty obejmują zakup wyspecjalizowanej infrastruktury (np. zaporę sieciową) oraz zatrudnianie najlepszych administratorów dbających o stałe aktualizowanie oprogramowania. Jednak wszystkie wydatki na bezpieczeństwo mogą okazać się bezowocne, jeżeli każdy pracownik firmy nie zostanie poddany szkoleniu uczącemu go technik obrony przed inżynierią socjalną.

Stosowanie technik inżynierii społecznej jest przestępstwem ściganym przez prawo polskie. Podszywanie się pod inną osobę oraz przejmowanie informacji niejawnych jest zagrożone karą pozbawienia wolności. Instytucje publiczne oraz firmy muszą wprowadzać systemy uwierzytelniania osób kontaktujących się z pracownikami firm elektronicznych. Konieczne jest ciągle podnoszenie kwalifikacji wszystkich pracowników posiadających dostęp do informacji niejawnych w zakresie zasad bezpieczeństwa teleinformatycznego³⁶⁴.

System zarządzania bezpieczeństwem informacji

System zarządzania bezpieczeństwem informacji można zdefiniować jako zestaw skoordynowanych działań (planowanie, organizowanie, motywowanie, kontrolowanie, koordynacje, decydowanie) dotyczących zasobów informacyj-

³⁶³ Por. F. Mouton, M.M. Malan, Leenen L., H.S. Venter, *Social engineering attack framework*, [w:] Information Security for South Africa (ISSA), 2014, ss. 1-9.

³⁶⁴ Zob. A. Kwaśniewski, *Człowiek piętą achillesową*, <http://www.nowebiuro.pl>, 30.01.2015.

nych podmiotu bezpieczeństwa (finanse, personel, technologie informatyczne, telekomunikacyjne, procedury, bazy: danych, modeli, wiedzy, dokumentów) z zamiarem osiągnięcia celów (tj. pożądanego poziomu bezpieczeństwa informacji, poufności, integralności, dostępności, rozliczalności, autentyczności, wiarygodności) w sposób sprawny i skuteczny³⁶⁵.

A zatem system zarządzania bezpieczeństwem informacji obejmuje: funkcje zarządzania, zasoby (aktywa) informacyjne, strukturę organizacyjną, polityki, zasady, procedury, procesy.

Ochrona informacji niejawnych winna być realizowana w ramach jednego dobrze przemyślanego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), dopasowanego do kultury, specyfiki działania określonego podmiotu bezpieczeństwa.

Istnieje wiele sposobów na ochronę przed czyhającymi zagrożeniami oraz na dostosowanie się do wymogów prawnych. Ogólnie można je wszystkie określić terminem „zarządzanie bezpieczeństwem informacji”.

Aby zapewnić bezpieczeństwo przetwarzanych informacji, firmy i urzędy są zobligowane przestrzegać ustaw, rozporządzeń oraz norm, a wszystkich tych dokumentów obecnie w Polsce istnieje ponad 200. Niektóre z nich zostały wymienione w załączniku 5.4.

ISO/IEC 27001 – norma międzynarodowa, która została opracowana 14 października 2005 r. na podstawie brytyjskiego standardu BS 7799-2 jest specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność, z którą mogą być prowadzone audyty, na podstawie których są wydawane certyfikaty.

Norma PN-ISO/IEC 27001 stosuje znany już dobrze model „Planuj – Wykonuj – Sprawdzaj – Działaj” (PDCA), który jest stosowany do całej struktury procesów SZBI. Proces wdrażania SZBI został przedstawiony na rys. 5.9 i zdefiniowany jako³⁶⁶:

Planuj – prace rozpoczynają się od określenia zakresu, strategii oraz polityki systemu zarządzania bezpieczeństwem informacji, wyznaczających kierunek działania w zakresie ochrony informacji. Po akceptacji dokonuje się analizy ryzyka, która obejmuje inwentaryzację aktywów, zidentyfikowanie zagrożeń i podatności oraz określenie skutków, jakie mogą przynieść dla firmy. Wynikiem prac tego etapu jest dokumentacja systemu zarządzania bezpieczeństwem informacji zawierająca plan postępowania z ryzykiem oraz deklarację stosowania mechanizmów kontroli ryzyka.

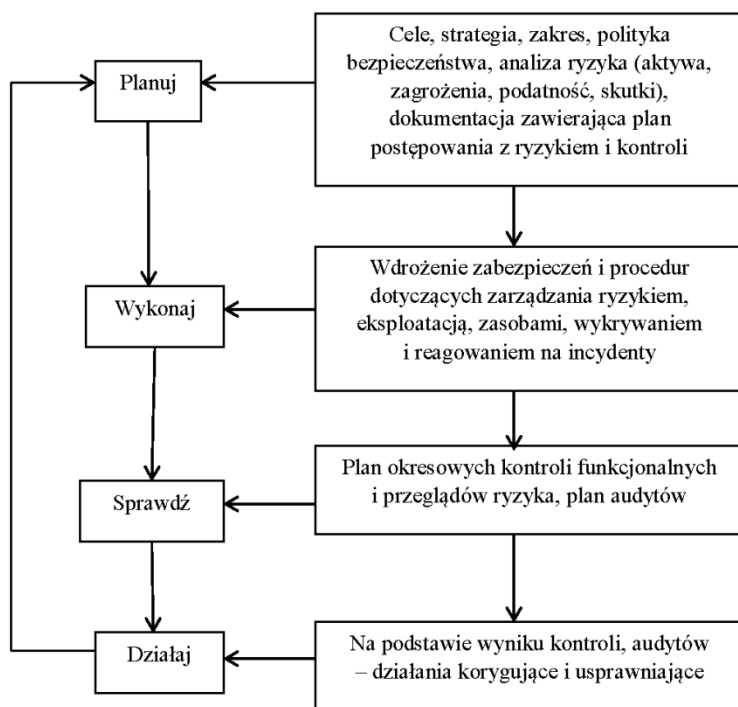
³⁶⁵ Zob. E. Schetina, K. Green, J. Carlson, *Bezpieczeństwo w sieci*, HELLION, Gliwice 2002, s. 258.

³⁶⁶ Por. A. Szymonik, *Informatyka ...*, op. cit., s. 181.

Wykonuj – na tym etapie dokonuje się wdrożenia zabezpieczeń i procedur zapewniających sprawne działanie systemu zarządzania bezpieczeństwem informacji dotyczących m.in.: zarządzania ryzykiem, zarządzania eksploatacją, zarządzania zasobami, wykrywania incydentów związanych z bezpieczeństwem informacji, reagowania na incydenty. Również przygotowuje się oraz przeprowadza cykl szkoleń dla personelu z zakresu wdrożonych procedur, jak i świadomości bezpieczeństwa informacji w firmie.

Sprawdź – w ramach implementacji procedur związanych z monitoringiem i przeglądem systemu zarządzania bezpieczeństwem informacji wykonuje się plan okresowych kontroli funkcjonalnych i przeglądów ryzyka, jak również przy zaangażowaniu audytu wewnętrznego opracowuje się plan audytów.

Działaj – ten etap cyklu PDCA jest w całości obsługiwany przez struktury wewnętrzne firmy, powołane w celu zarządzania bezpieczeństwem informacji. Na podstawie wyników audytów, przeglądów oraz okresowych kontroli podejmują działania korygujące i usprawniają system zarządzania bezpieczeństwem informacji.



Rys. 5.9. Procesy wdrażania i zarządzania bezpieczeństwem informacji

Źródło: opracowano na podstawie ISO/EC 27001 oraz J. Gryz, *Zarys podstaw teorii bezpieczeństwa*, AON, Warszawa 2010, s. 63.

W normie ISO/IEC 27001 wyróżniono jedenaście obszarów, mających wpływ na bezpieczeństwo informacji w organizacji: polityka bezpieczeństwa, organizacja bezpieczeństwa informacji, zarządzanie aktywami, bezpieczeństwo zasobów ludzkich, bezpieczeństwo fizyczne i środowiskowe, zarządzanie systemami i sieciami, kontrola dostępu, zarządzanie ciągłością działania, pozyskiwanie, rozwój i utrzymanie systemów informatycznych, zarządzanie incydentami związanymi z bezpieczeństwem informacji, zgodność z wymaganiami prawnymi i własnymi standardami.

Na uwagę zasługuje obszar związany z polityką bezpieczeństwa oraz bezpieczeństwem fizycznym i środowiskowym.

Polityka bezpieczeństwa informacji (information security policy) jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne³⁶⁷. Określa ona, które zasoby i w jaki sposób mają być chronione.

Polityka powinna obejmować wskazanie możliwych rodzajów naruszenia bezpieczeństwa (jak np. utrata danych, nieautoryzowany dostęp), scenariusze postępowania w takich sytuacjach i działania, które pozwolą uniknąć powtórzenia się danego incydentu. Polityka bezpieczeństwa definiuje ponadto poprawne i niepoprawne korzystanie z zasobów (np. kont użytkowników, danych, oprogramowania).

Istotne jest, aby polityka bezpieczeństwa była dokumentem spisanim i znanym oraz zrozumianym przez pracowników organizacji korzystających z zasobów informatycznych. Dotyczy to także klientów organizacji (użytkowników jej zasobów).

Przy projektowaniu polityki należy rozważyć, czy organizacja będzie w stanie ponieść koszty wprowadzania tej polityki w życie. Podwyższanie poziomu bezpieczeństwa organizacji/systemu odbywa się najczęściej kosztem wygody i efektywności działania. Opierając się na zalecanych modelach czy standardach w tej dziedzinie, należy więc pamiętać o dostosowaniu rozwiązania do specyfiki organizacji, tak aby nadać jej cechy ułatwiające zastosowanie w praktyce. Podstawowym zadaniem jest przeprowadzenie analizy ryzyka i ustalenie akceptowalnego poziomu ryzyka.

Tworząc politykę bezpieczeństwa informacji, należy mieć na uwadze cele firmy, które należy osiągnąć. Do nich zaliczmy między innymi³⁶⁸: zagwarantowanie prawnych wymagań ochrony informacji, zagwarantowanie poufności, integralności, dostępności przetwarzanych informacji, bezpieczeństwo informacji

³⁶⁷ Por. N. Pałęga, M. Knapiński, *Polityka bezpieczeństwa informacji narzędziem ochrony zasobów informacyjnych w działalności logistycznej firm*, [w:] *Logistyka* 2013/6, ss. 678-681.

³⁶⁸ Por. T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2006, ss. 48-52.

strategicznych, zagwarantowanie zaufania publicznego i prestiżu przedsiębiorstwa, bezpieczeństwo procesu ciągłości funkcjonowania przedsiębiorstwa, redukcję kosztów.

Polityka bezpieczeństwa informacji powinna zawierać wyłącznie ogólny opis wybranych strategii i dotyczyć³⁶⁹: metod osiągnięcia optymalnego poziomu bezpieczeństwa, ról i odpowiedzialności w procesie tworzenia bezpieczeństwa, zarządzania przez systemy jakościowe, rozwoju poszczególnych polityk, bezpieczeństwa wymiany informacji, standaryzacji i spełnienia norm, bezpieczeństwa informacji w otoczeniu wewnętrznym i celowym przedsiębiorstwa, reakcji na incydenty.

Bezpieczeństwo fizyczne ma za zadanie zabezpieczenie przed dostępem osób nieuprawnionych do informacji niejawnych.

Według K. Lidermana w ramach bezpieczeństwa fizycznego wyszczególniamy następujące zagadnienia³⁷⁰: organizacja i systemy kontroli dostępu, zabezpieczenia przeciw włamaniom (konstrukcje antywłamaniowe, urządzenia alarmowe), systemy i procedury zapewniające ciągłość pracy urządzeń składowych sieci, instalacje i utrzymywanie systemów zabezpieczeń przeciwpożarowych.

System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. W zależności od poziomu zagrożeń, określonego w wyniku przeprowadzenia analizy, o której mowa, stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego³⁷¹:

- personel bezpieczeństwa – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;
- bariery fizyczne – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;
- szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

³⁶⁹ B. Ciecierska, J. Łunarski, R. Perłowski, K. Stadnicka, *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, PRz, Rzeszów 2006, s. 251.

³⁷⁰ Por. K. Liderman, *Podręcznik administratora bezpieczeństwa teleinformatyczne*, MIKOM, 2003, s. 204.

³⁷¹ Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

- system kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;
- system sygnalizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;
- system dozoru wizyjnego – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;
- system kontroli osób i przedmiotów – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

Tworzy się następujące strefy ochronne³⁷²:

- strefę ochronną I – obejmującą pomieszczenie lub obszar, w których informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:
 - ✓ wyraźnie wskazana w planie ochrony najwyższa klauzula tajności przetwarzanych informacji niejawnych,
 - ✓ wyraźnie określone i zabezpieczone granice,
 - ✓ wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy, pełnienia służby albo wykonywania czynności zleconych,
 - ✓ wstęp możliwy jest wyłącznie ze strefy ochronnej;
- strefę ochronną II – obejmującą pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne” lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:

³⁷² Tamże.

- ✓ wyraźnie określone i zabezpieczone granice,
- ✓ wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy, pełnienia służby albo wykonywania czynności zleconych,
- ✓ wstęp możliwy jest wyłącznie ze strefy ochronnej;
- strefę ochronną III – obejmującą pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów;
- specjalną strefę ochronną – umiejscowioną w obrębie strefy ochronnej I lub strefy ochronnej II, chronioną przed podsłuchem, spełniającą dodatkowo następujące wymagania:

Klucze i kody dostępu do szaf, pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, mogą być udostępnione tylko tym osobom, którym posiadanie kluczy lub znajomość kodów są niezbędne do wykonywania obowiązków służbowych. Kody zmienia się co najmniej raz w roku, a także w przypadku każdej zmiany składu osób znających kod oraz zaistnienia podejrzenia, że osoba nieuprawniona mogła poznać kod, gdy zamek poddano konserwacji lub naprawie.

6. MODEL ZARZĄDZANIA BEZPIECZEŃSTWEM GOSPODARCZYM I LOGISTYCZNYM NA POTRZEBY SYSTEMU BEZPIECZEŃSTWA NARODOWEGO

Modelowanie tak złożonego rzeczywistego systemu dynamicznego, jakim jest system logistyczny w połączeniu z systemem gospodarczym i systemem bezpieczeństwa narodowego jest bardzo skomplikowane, chociaż możliwe. Pomocne w budowaniu modelu rzeczywistego opartej o przedstawioną teorię są zaprezentowane badania przeprowadzone w firmach z wykorzystaniem kwestionariusza ankietowego. Niezwykle pomocne w interpretacji wyników były również rozmowy z ekspertami, logistykami dużych firm. Badania pozwoliły na: uzyskanie ocen, określających aprobatę lub dezaprobatę modelu oceanowego w zależności od typu i rodzaju firmy określonej branży; uzyskanie określonych decyzji niezbędnych do zapewnienia stanu pożądanego z uwagi na przyjęte kryterium; przyjęcie określonego aspektu dociekań: morfologicznych, funkcjonalnych, rozwojowych; określenie zależności w kierowaniu w systemach aktywnych logistycznych.

6.1. Modelowanie systemowe w zarządzaniu i logistyce

Modelowanie jest szczególną relacją między oryginałem, czyli obiektem rzeczywistym, a jego obrazem wyrażonym w określonym języku i postaci (formie). Modelowanie jest procesem odwzorowania obiektu traktowanego jako oryginał w jego obraz. Celem opracowania modelu może być poznanie, czyli opis (deskrypcja), diagnoza, ocena, prognoza, decyzja, dotyczące badanego obiektu (systemu) rzeczywistego. Postać modelu zależy np. od jego przeznaczenia (celu badań), ale także przyjętego języka modelowania, kwalifikacji i kompetencji badacza. W rozdziale szeroko wykorzystano propozycje metodologiczne przedstawione w pracy P. Sienkiewicz, *Inżynieria systemów kierowania*, PWE Warszawa 1998, ss. 89-132.

Terminu „model” używa się najczęściej w dwóch różnych ujęciach dla oznaczenia:

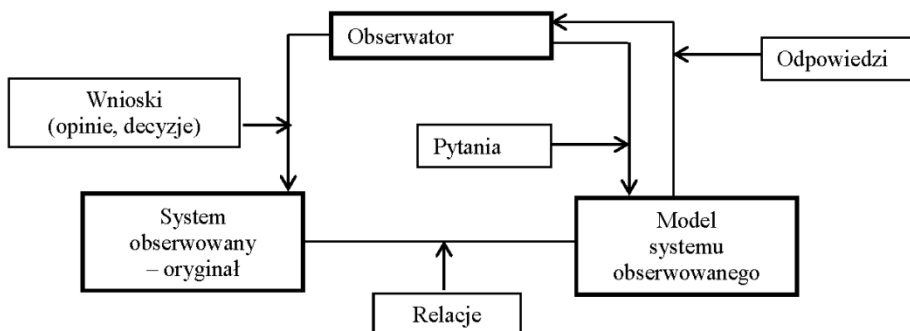
- 1) teorii, która jest strukturalnie podobna do innej, co umożliwia przechodzenie od jednej teorii do innej za pomocą zwykłej zmiany terminologii – w tym znaczeniu model jest środkiem poznania;
- 2) systemu, do którego odnosi się pewna teoria dla uproszczonego odzwierciedlenia badanej rzeczywistości – w tym ujęciu model jest przedmiotem poznania.

Model definiowany jest najczęściej jako:

- układ, który odzwierciedlając lub odtwarzając przedmiot badania, jest zdolny zastępować go tak, że jego badanie dostarcza nam nowej informacji o tym przedmiocie;
- zastępnik oryginału, przyjętą formę reprezentacji, wykorzystywaną do wyjaśnienia i przewidywania zachowania się rzeczywistego systemu, przy czym model musi odwzorowywać rzeczywistość w sposób adekwatny do celu badań;
- pewna idealizacja lub uproszczenie rzeczywistości.

Sam charakter i stopień uproszczenia zależy od wiedzy, potrzeb i świadomości badacza i może się zmieniać w zależności od celu badań. Wspólną dla teorii i modelu jest właściwość odnoszenia się do rzeczywistości, postrzeganej w uproszczonej, abstrakcyjnej formie.

Przyjmując założenie, że pewien system **M** jest modelem innego systemu **O** (zwanego oryginałem) i jeśli między **M** i **O** zachodzą określone współzależności (relacje), to możliwe jest sformułowanie pewnych wniosków co do natury czy istoty **O** na podstawie obserwacji **M**.



Rys. 6.1. Rola modelu w obserwacji systemu

Źródło: *Wstęp do informatyki gospodarczej*, red. nauk. Anna Rokicka-Broniatowska, SGH, Warszawa 2006, s. 49.

Model jest pośrednikiem między obserwatorem a systemem obserwowanym (oryginałem), przy czym o jakości tego odwzorowania decyduje (rys. 6.1)³⁷³:

- stopień zgodności z celem obserwacji;
- zgodność z potrzebami obserwatora;
- stopień prawidłowości doboru stosowanego rodzaju modelu.

Model charakteryzuje się:

³⁷³ *Wstęp do informatyki gospodarczej*, red. nauk. A. Rokicka-Broniatowska, SGH, Warszawa 2006, s. 49.

- względnością – obserwator decyduje o ważności i istotności relacji, jakie występują pomiędzy **M** i **O**;
- użytecznością – wiedza na podstawie **M** o **O** pozwala na doskonalenie funkcjonowania systemu zwanego oryginałem.

Relacje jakie zachodzące pomiędzy **O** i **M** mają charakter podobieństwa lub analogii.

Zasady opisu systemów działania

Określenie dziedziny badań systemowych wymaga sprecyzowania:

- „sfery pozajęzykowej”, którą identyfikuje się z całokształtem systemów rzeczywistych (empirycznych);
- „sfery językowej”, którą identyfikuje się z całokształtem systemów pojęciowych;
- metod powiązania (przechodzenia, przekształcania, odwzorowywania) obu wyżej wymienionych „sfer”.

Opis dowolnego systemu rzeczywistego, takiego jak np. dowolny system gospodarczy (logistyczny) wymaga ustalenia cech parametrów charakteryzujących obiekt z określonego punktu widzenia, czyli dokonania *konceptualizacji*. Konkretniej konceptualizacji odpowiada zawsze pewien obserwator realizujący cel badań (projektu, strategii, polityki).

Precyzując zasady opisu systemów, należy wyróżnić aspekty charakterystyczne dla badań systemowych. Istotne znaczenie we wstępnej fazie opisu systemów ma *eksplikacja pojęć pierwotnych*, czyli nadawanie pojęciom powszednim powszechnie używanym, rangi ścisłych pojęć matematycznych. Jest to zabieg często stosowany w badaniach systemowych. W tym miejscu celowe jest przytoczenie opinii: „... należy przestrzec przed nieostrożnym przenoszeniem rozważań przeprowadzonych dla konkretnego uściślenia, czyli eksplikacji danego pojęcia na przypadek ogólny, w którym pojęcie to ma charakter intuicyjny. Badanie eksplikacji dowodzi, że jedno i to samo pojęcie może mieć różne uściślenia o różnych własnościach. Zmusza to do szczególnej ostrożności wobec wywodów nieścisłych lub przenoszenia wywodów ścisłych na przypadki, w których występują pojęcia intuicyjne. W istocie działa tu zasada proporcjonalności między ścisłością wywodu i dokładnością stwierdzenia”³⁷⁴.

Dyskusja nad poprawnością, adekwatnością itp. opisu ma sens, gdy uwzględnia przyjęty aspekt badań oraz właściwości zastosowanego języka i metody opisu. Powyższa uwaga pozwala uniknąć wielu nieporozumień formalnych. Z ogólnej interpretacji twierdzenia K. Goedla o niepełności wynika, że w języku odwzorowującym dany system, jeżeli jest on niesprzeczny, istnieją wypowiedzi, o których nie potrafimy orzec, czy trzeba je przyjąć czy odrzucić (tj. nie można ich w tym języku ani udowodnić, ani uznać za fałszywe).

³⁷⁴ Por. J.A. Szejder, *Równość, podobieństwo, porządek*, Warszawa 1975, s. 7.

Do ich oceny potrzebny jest metajęzyk, którego obiektem jest dany język. Formą reprezentacji badanych systemów są modele stosowane do opisu, wyjaśniania i przewidywania zachowania się systemów w różnych warunkach.

Między systemem pojęciowym przyjętym jako model danego systemu rzeczywistego a oryginałem (tj. systemem rzeczywistym) musi zachodzić co najmniej *relacja homomorfizmu*, czyli relacja jednoznaczna-dwuczłonowa, przeciwsymetryczna, wyrażająca większe lub mniejsze podobieństwo (strukturalne, funkcjonalne) modelu i oryginału.

Istnieją różnorokie klasyfikacje modeli stosowanych w badaniach (tabele 6.1, 6.2).

Tabela 6.1

Klasyfikacja modeli badawczych

| Forma \ Warstwa | Modele (M) Opisowe (Op) | Modele (M) Formalne (F) | Modele (M) Matematyczne (Mt) |
|-----------------------|-------------------------|-------------------------|------------------------------|
| Modele Zjawiskowe (Z) | MOpZ | MFZ | MMtZ |
| Modele Ocenowe (O) | MOpO | MFO | MMtO |
| Modele Decyzyjne (D) | MOpD | MFD | MMtD |

Źródło: J. Konieczny, *Podstawy eksploatacji urządzeń*, Warszawa 1975, s. 71.

W celu dokonania klasyfikacji podstawowych modeli stosowanych w badaniach systemowych organizacji przyjęto trzy kryteria podziału. *Pierwsze kryterium* wyraża cel poznawczy (rezultat modelowania) i pozwala na wyróżnienie modeli:

- desygnujących (wyjaśniających), których celem jest uzyskanie pożądanego wyjaśnienia istoty cech (zjawisk) systemu;
- ocenowych, których celem jest uzyskanie ocen, czyli wypowiedzi wyrażających aprobatę lub dezaprobatę dla stanu (przeszłego, bieżącego, przyszłego) systemu;
- decyzyjnych, których celem jest uzyskanie określonych decyzji, niezbędnych do zapewnienia stanu systemu pożądanego z uwagi na przyjęte kryterium.

W badaniach systemowych organizacji gospodarczych (logistycznych) są stosowane wszystkie wymienione rodzaje modeli, przy czym modele desygnujące (w tym diagnostyczne i prognostyczne) są podstawowym narzędziem w teorii systemów rzeczywistych (organizacji), natomiast modele ocenowe i decyzyjne w analizie systemowej i inżynierii systemów działania.

Ze względu na *drugie kryterium* podziału, wyrażające formę przekazu (język modelowania), rozróżnia się modele:

- opisowe, wyrażane w języku naturalnym;
- formalne, wyrażane w języku logiki, głównie logiki matematycznej;

- matematyczne, wyrażane w języku matematyki (np. teorii mnogości, algebry, analizy funkcjonalnej, probabilistyki).

Trzecie kryterium wiąże się z przyjmowanym aspektem badań systemowych. Wyróżniamy trzy podstawowe aspekty:

- morfologii (struktury, budowy) systemu;
- funkcjonowania (zachowania, działania) systemu;
- rozwoju (ewolucji, przemian) systemu.

Tabela 6.2

Rodzaje modeli i kryteria ich wyróżnienia

| Kryterium języka modelowania | Kryterium przeznaczenia modeli | Kryterium cech systemowych |
|--|--|--|
| Modele werbalne (opisowe) wyrażone w języku naturalnym | Modele zjawiskowe, wyjaśniające sens (istotę) rozpatrywanych zjawisk realnych | Modele strukturalne, odwzorowujące struktury obiektów |
| Modele ideograficzne wyrażone za pomocą symboli pozajęzykowych, np. schematy | Modele ocenowe, służące do oceny obiektów, zjawisk, procesów z określonego punktu widzenia (w aspekcie) | Modele funkcjonalne, odwzorowujące dynamikę procesów realizowanych przez obiekt/ system` |
| Modele formalne wyrażone w języku logiki formalnej | Modele prognostyczne, służące do przewidywania przebiegu określonych zjawisk procesów w bliższej i dalszej przyszłości | Modele rozwojowe, odwzorowujące zjawiska rozwoju, czyli zmian ilościowych i jakościowych obiektu/systemu |
| Modele matematyczne wyrażone w języku współczesnej matematyki | Modele decyzyjne, służące do wspomagania realnych procesów decyzyjnych | Dekalog cech konstytutywnych badań systemowych |

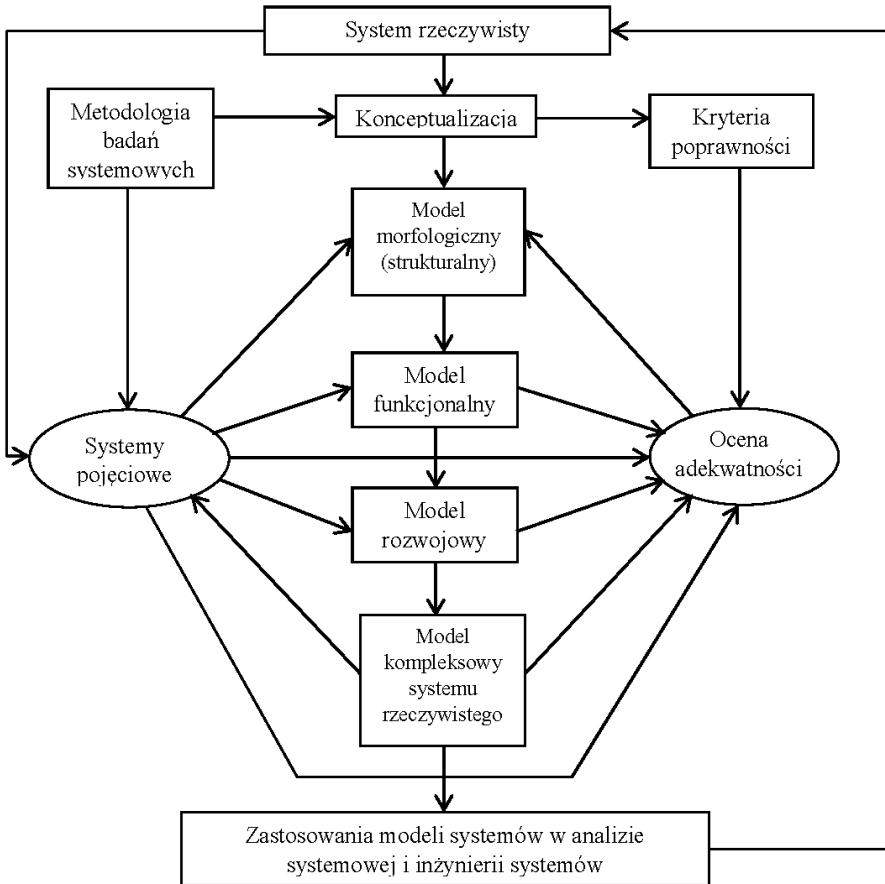
Źródło: zob. P. Sienkiewicz, *Analiza systemowa, Podstawy i zastosowania*, Bellona Warszawa 1994, ss. 53-54.

Wyróżnione aspekty wyrażają także postępujący stopień poznania systemu: pierwszy stopień wiąże się z poznaniem budowy systemu (jego elementów i powiązań (relacji) między nimi), drugi – z poznaniem funkcjonowania systemu, a więc realizowanych w nim procesów, trzeci – z poznaniem praw rozwoju systemu, czyli określeniem kierunków przemian jego struktur, funkcji, procesów itp. „Zerowy” poziom poznania systemu stanowi opis parametryczny polegający na specyfikacji cech systemowych. Poszczególne poziomy poznania systemu wyrażają swoiste ujęcie obiektu poprzez opis:

- parametryczny – charakter jakościowy;

- morfologiczny – charakter strukturalny;
- funkcjonalny – charakter procesualny;
- rozwojowy – charakter prognostyczny.

Modele systemów można sklasyfikować ze względu na język, przeznaczenie, cechy (tabela 6.2).



Rys. 6.2. Ogólny schemat modelowania systemowego

Źródło: opracowanie własne, P. Sienkiewicz, *Inżynieria systemów kierowania*, PWE, Warszawa 1988, s. 93

Ogólny schemat pełnego cyklu modelowania systemów, ze względu na przedmiot i metodę odwzorowywania, będziemy nazywać *modelowaniem systemowym*. Jest on procesem twórczym i stanowi taki ciąg czynności, w wyniku których uzyskuje się, np. matematyczny model oceny (decyzyjny) systemu, nową strukturę, nowy model procesów realizowanych w badanym systemie itp. Jeżeli uzyskany model dotyczy tylko wybranego aspektu badań,

to można mówić o modelu cząstkowym (jednoaspektowym), jeśli zaś wszystkich, to – o modelu kompleksowym (wieloaspektowym). Należy zwrócić uwagę, że prezentowany schemat modelowania systemowego jest uściślony o aspekty: metodologii badań, kryterium poprawności, ocenę adekwatności, pojęć systemowych (rys. 6.2).

Opis morfologiczny systemu jest wyrazem ujęcia strukturalnego, w którym są wykorzystywane takie kategorie, jak: element, skład, relacje, struktura, morfologia itp. Opis ten jest stosowany w rozwiązywaniu zadań, w których istotne znaczenie ma uzyskanie odpowiedzi na pytania:

- jakie elementy tworzą system i jakie między nimi występują różnice?
- jakiego typu powiązania między elementami systemu tworzą jego strukturę (struktury)?
- jaki powinien być najbardziej pożądaný skład tworzonego systemu ze względu na określone kryterium efektywności?
- jakie powinny być najbardziej pożądane relacje między elementami systemu (struktury) ze względu na określone kryterium efektywności?
- w jaki sposób dana struktura systemu wpływa na realizowane funkcje?
- w jakim kierunku przebiegać będą przemiany struktur systemu itp.?

Opis morfologiczny charakteryzuje przede wszystkim dążenie do odwzorowania organizacji wewnętrznej systemu, przestrzennego rozmieszczenia elementów oraz sposobów ich wzajemnych powiązań. W badaniach systemowych wyróżnimy dwa rodzaje wewnętrznych powiązań w systemie:

- sprzężenia między obiektami (elementami systemu);
- oddziaływania między procesami zachodzącymi w obiektach.

Pierwszy rodzaj powiązań stanowi zasadniczy przedmiot opisu morfologicznego, drugi natomiast jest przedmiotem opisu funkcjonalnego. Tak więc w opisie morfologicznym nie będą nas interesowały związki czasowe występujące między obiektami. Nie jest to równoznaczne z założeniem o istnieniu struktur diachronicznych, tj. takich, które trwają bez zmiany niezależnie od biegu czasu. Możemy jednak przyjąć, że w okresie badania (opisu) systemu jego struktury nie ulegają zasadniczym zmianom.

Zakładamy, że wszystkie systemy rzeczywiste (empiryczne) rozpatrywane w badaniach systemów działania mają struktury synchronistyczne, tj. zmieniające się w czasie zarówno w zależności od czynników rozwojowych systemów, jak i od rozwoju człowieka badającego te systemy, jego sposobu myślenia, narzędzi badawczych itp.

Ze względu na własności sprzężeń między elementami systemu (w tym systemu logistycznego) wyróżniamy następujące rodzaje *sprzężeń*:

- lokalizacyjne, czyli sprzężone są elementy, które muszą pozostawać we wzajemnych relacjach ze względu na reprezentowane cechy systemowe;
- energetyczne, czyli istnieją sprzężenia między elementami, gdy jeden z nich stanowi podstawę do powstania drugiego;

- egzystencjonalne, czyli sprzężone są elementy, których istnienie jako elementów systemów jest określone przez relacje z innymi elementami, co najmniej niedestruktywnie nań wpływającymi;
- koegzystencjonalne, czyli sprzężone są elementy, między którymi istnieją relacje odpowiadające ich potrzebom (np. relacja współdziałania³⁷⁵).

Do pełnego opisu morfologicznego systemu konieczne jest:

- odwzorowanie struktury systemu w postaci grafu płaskiego lub topologicznego;
- określenie stopnia i rzędu grafu, liczby cyklomatycznej, pełnej liczby chromatycznej itp.;
- wykazanie spójności grafu lub określenie prawdopodobieństwa spójności grafu;
- określenie ilości informacji strukturalnej w systemie;
- określenie rodzaju struktury.

Opis funkcjonalny – jest wyrazem ujęcia funkcjonalnego (procesualnego, zdarzeniowego, dynamicznego) systemu, w którym znajdują zastosowanie takie kategorie, jak: czas, stan, zdarzenie, funkcja, proces itp. Opis ten stosuje się podczas rozwiązywania zadań, w których istotne jest uzyskanie odpowiedzi na poniższe pytania:

- jakie funkcje i procesy są realizowane w systemie?
- jakie jest zachowanie się systemu w danych warunkach?
- jaka jest organizacja realizacji procesów (funkcji) przez system?
- jaki powinien być najbardziej pożądanym przebieg procesów w systemie?
- czy struktury systemu odpowiadają realizowanym procesom w sensie przyjętego kryterium efektywności?
- w jaki sposób cechy elementów systemu wpływają na efektywność procesów itp.?

Opis funkcjonalny wyraża dążenie do odwzorowania funkcji i procesów systemu, przestrzenno-czasowej organizacji funkcjonowania systemu oraz jego dynamiki. Celem badań funkcjonalnych jest ustalenie związku przyczynowego, stanów, funkcji i procesów w poszczególnych połączonych ze sobą elementach lub podsystemach danego systemu. Opis funkcjonalny charakteryzuje (cehuje) oddziaływania między procesami zachodzącymi w obiektach. Związki wyrażające te oddziaływania możemy podzielić na:

- współdziałania, czyli powiązania obiektów (ich cech), przy czym mogą one mieć charakter kooperacyjny lub konfliktowy;
- funkcjonalne, zapewniające właściwy przebieg procesów (realizację funkcji);

³⁷⁵ Szerzej w podrozdziale 2.3.

- energetyczne, wyrażające oddziaływania energetyczne (energomaterialne) obiektów;
- informacyjne, wyrażające oddziaływania informacyjne (informacyjno-decyzyjne).

Opis rozwojowy – przyjęto, że dla każdego systemu rzeczywistego podstawowe znaczenie mają trzy cechy systemowe wyrażane przez kategorie: (1) struktura, (2) zachowanie, (3) rozwój.

W świetle dotychczasowych wniosków sformułowanych na gruncie badań systemowych stwierdza się, że rozwój niejako zawiera w sobie dwa pozostałe pojęcia. Zakładamy więc, że rozwój systemu może dotyczyć rozwoju struktury systemu i/lub rozwoju procesów. Opis rozwojowy systemu jest wyrazem ujęcia prognostycznego, w którym korzysta się z takich pojęć, jak: rozwój, ewolucja, postęp i wzrost. Opis ten jest stosowany w rozwiązywaniu zadań, w których istotne znaczenie ma uzyskanie odpowiedzi na pytania:

- w jakim kierunku będą przebiegać zmiany w strukturze systemu i/lub zmiany w strukturze dynamicznej systemu?
- w jaki sposób zmiany strukturalne wpływają na procesy i funkcje systemu?
- w jaki sposób zmiany procesów i funkcji wpływają na struktury systemu?
- jak należy sterować rozwojem systemu, aby zmiany struktury i procesów przebiegały w pożądanym kierunku itp.

Opis rozwojowy charakteryzuje przede wszystkim dążenie do odwzorowania wszystkich zdarzeń wywołujących zmiany oraz przewidywania struktur i procesów, które będą charakteryzować system w przyszłości.

Wszystkie systemy, których struktury, elementy, procesy i funkcje ulegają zmianom w czasie wskutek wzrostu, starzenia się, rozbudowy, ewolucji itp. nazywamy *systemami rozwoju (rozwijającymi się)*. Rozwój systemu będziemy charakteryzować typem dynamiki rozwoju. Wyróżniono następujące typy dynamiki rozwoju:

- postępowy rozwój typu ewolucyjnego, gdy system stopniowo przyjmuje cechy (stany) korzystniejsze niż cechy (stany) pierwotne;
- wsteczny rozwój typu ewolucyjnego, gdy system stopniowo przyjmuje cechy (stany) mniej korzystne (mniej pożądane) niż cechy (stany) pierwotne;
- typu katastroficznego, gdy następuje gwałtowny spadek wartości pozytywnych (korzystnych) cech systemowych;
- typu eksplozywnego, gdy następuje gwałtowny wzrost w systemie i przejście do dominacji pewnych pozytywnych cech systemowych;
- typu funkcjonalnego, gdy występują fluktuacje wartości podstawowych cech systemowych wokół pewnych wartości średnich (każda zmiana w systemie wywołująca jego rozwój ma określone przyczyny i skutki).

Zasadnicze typy przyczyn i skutków rozwoju przedstawiono w tabeli 6.3.

Podstawą opisu rozwojowego systemu jest znajomość jego opisu morfologicznego i funkcjonalnego.

W przypadku konwergencji (zbieżności) rozwój systemu polega na dążeniu do zaniku specjalizacji w systemie, czyli w wyniku rozwoju wszystkie elementy systemu realizują procesy elementarne tego samego typu. W przypadku dywergencji (rozbieżności) rozwój systemu wywołuje zjawisko przeciwne, czyli wszystkie elementy systemu będą realizować procesy różnych typów. Zarówno dywergencja, jak i konwergencja systemów wiąże się ze zmianami ilości informacji funkcjonalnej, lecz w przeciwnych kierunkach.

Tabela 6.3

Klasyfikacja związków przyczynowych

| Skutki | | | Przyczyny | |
|---|---|--|--------------|---------------------------|
| Typ | Podtyp | Odmiana | Wewnętrzne | Zewnętrzne |
| Zmiana energii | | | | Energetyczna |
| Zmiana struktury | Zniszczenie struktury (gwałtowny wzrost entropii) | Egzogeniczna | | Energetyczna |
| | | Endogeniczna | Energetyczny | Realizator |
| | Proces wyrównawczy (stopniowy wzrost entropii) | | Tensyjna | Ewentualnie realizator |
| | Komplikacja struktury (stopniowy spadek entropii) | Egzogeniczna | | Energetyczna informacyjna |
| Endogeniczna (spontaniczne zróżnicowanie, rozwój) | | Interakcyjna Informacyjna lub realizator | Energetyczna | |

Źródło: opracowanie własne.

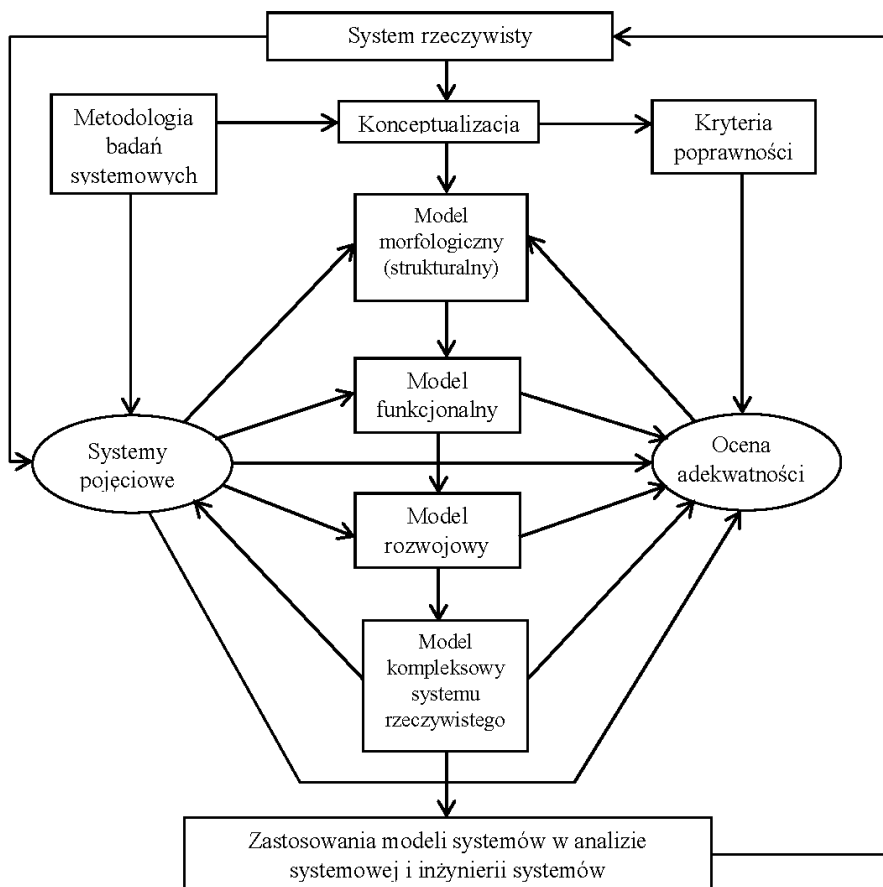
Stwierdzono, że w zależności od pojawiania się potrzeb, rozwój systemu może dotyczyć: (1) tylko procesów organizujących działanie (sterowanie, kierowanie, zarządzanie), (2) tylko procesów roboczych (wykonawcze, ergo-materialne), (3) procesów zarówno jednych, jak i drugich³⁷⁶. Z porównania potrzeb i rozwoju wynikają dwa charakterystyczne przypadki: (1) przypadek rozwoju systemu normalnego w stosunku do potrzeb i (2) przypadek nienadążania rozwoju systemu za potrzebami.

Dla badań rozwoju charakterystyczne jest pojęcie prognozy rozwoju systemu (**model rozwojowy**). Najczęściej uważa się, że prognoza to wynik

³⁷⁶ Zob. R. Staniszewski, *Cybernetyka systemów projektowania*, Warszawa 1981; P. Sienkiewicz, *25 wykładów*. AON, Warszawa 2015.

opartego na podstawach naukowych przewidywania przebiegu i stanu możliwych (prawdopodobnych) zdarzeń (rzeczy, faktów, zjawisk), wyrażony w formie informacji prognostycznej. W opisie rozwojowym będziemy korzystać z tzw. prognoz rozwojowych systemu.

Prognozą rozwojową systemu nazywamy wypowiedź opracowaną na podstawie prospektywnego badania zachowania się systemu, zawierającą miarę zdarzenia losowego opisującego rozwój systemu w określonych warunkach i określonym czasie.



Rys. 6.3. Istotne czynniki kompleksowego modelowania systemów

Źródło: opracowanie własne.

Ilościowe prognozy rozwojowe są wyznaczane na podstawie matematycznych modeli rozwojowych i modeli symulacyjnych, natomiast jakościowe prognozy rozwojowe określa się najczęściej za pomocą technik heurystycznych, wśród których technika ocen ekspertów ma nadal podstawowe znaczenie. Wnioski dotyczące typu rozwoju systemu mogą być opracowywane na podstawie

symulacyjnego badania rozwoju systemu. Uważamy, że w najbliższej przyszłości symulacyjne badania rozwoju systemów będą mieć podstawowe znaczenie dla analiz rozwojowych i badań prognostycznych.

W celu uzyskania pełnego opisu rozwojowego należy: zweryfikować model strukturalny i model funkcjonalny; opracować listę możliwych przyczyn i skutków rozwoju systemu; ustalić podstawowe cechy i charakterystyki rozwoju systemu; określić możliwości sterowania rozwojem; wyznaczyć strukturę rozwojową systemu; zweryfikować model rozwojowy poprzez określenie istotnych czynników kompleksowego modelowania systemów – stopnia pewności prognozy (rys. 6.3).

Kierowanie w systemach aktywnych

Przez pojęcie *aktywności systemu* rozumie się, że system:

- działa we własnym interesie, czyli stara się osiągnąć własne cele;
- ma zdolność prognozowania;
- zna swoje możliwości lepiej niż organ kierujący wyższego poziomu;
- jest informowany o zasadach podejmowania decyzji na wyższych poziomach i korzysta z tej informacji podczas swego działania.

O dowolnym systemie powiemy, że jest aktywny, gdy działa lub jest gotowy do działania, a zwłaszcza do intensywnych wysiłków zmierzających do urzeczywistnienia przedsięwziętych celów. Odpowiada to powszechnie przyjętemu pojęciu aktywności³⁷⁷. Cecha aktywności wynika z własności podmiotu działania i własności obiektu, na którym zostały zlokalizowane cele podmiotu. Oznacza to, że jako system aktywny będzie traktowany dany system działania (organizacja) i system, w którym wywołanie określonych zmian jest celem wyróżnionego w badaniach obiektu. W związku z tym systemy te (co najmniej dwa) będą traktowane jako podsystemy *aktywnego systemu działania* (ASD).

Zgodnie z tezą, że dowolny system jest celowy wtedy i tylko wtedy, gdy jest aktywny, wynika, że celowe działanie zakłada zdolność istoty działającej do przewidywania zarówno przebiegu, jak i skutków działania. Działanie jest celowe, gdy jego kierunek i sposób są wyznaczane przez uprzednio powzięty cel. Istotą celowego zachowania systemu jest jego ukierunkowany przebieg zmierzający do osiągnięcia określonego stanu końcowego. Zachowanie celowe zmierza więc do przekształcenia pewnej sytuacji początkowej w zamierzoną sytuację końcową. Ukierunkowany przebieg zachowania systemu jest związany z antycypacją, zarówno sytuacji końcowej, jak i działania do niej prowadzącego. Antycypowana sytuacja końcowa określona wyróżnionym stanem rzeczy (lub zbiorem stanów) jest celem systemu, natomiast antycypowane działania – programem systemu.

³⁷⁷ Zob. T. Pszczołowski, *Mała encyklopedia prakseologii i teorii organizacji*, Warszawa 1978, P. Sienkiewicz, *Inżynieria systemów*, Warszawa 1983, s. 128.

Załóżmy, że dane są systemy **A** i **B**, przy czym jako interesujący przedmiot analizy przyjmujemy system **A**. Powiemy, że cel systemu **A** jest zlokalizowany na systemie **B**, jeżeli antycypowana przez **A** sytuacja końcowa obejmuje stan (stany), którego osiągnięcie oznacza zmianę potencjału (efektywności potencjalnej) systemu **B**. Każda zmiana oznacza bądź wzrost, bądź spadek wartości potencjału.

Jeżeli działanie systemu **A**, którego cel jest zlokalizowany na systemie **B**, jest skutkiem wcześniejszego działania **B** na **A**, to powiemy, że system **A** charakteryzuje *reaktywność*. Jeżeli natomiast działanie systemu **A**, którego cel jest zlokalizowany na systemie **B**, jest podejmowane bez względu na zachowanie się systemu **B** względem niego, to powiemy, że system **A** charakteryzuje *aktywność sprawcza*.

Specyficzność ASD (*aktywnego systemu działania*) pozwala na wyróżnienie następujących cech kierowania w systemie **A**:

- celem kierowania jest projektowanie struktur, procesów, rozwoju i zachowań (postaw) pozwalających na osiąganie celów zlokalizowanych na systemie **B**, ocenianych zgodnie z przyjętymi kryteriami oceny efektywności ASD;
- zapewnienie odpowiedniego poziomu wrażliwości na działanie systemu **B** i określonego poziomu aktywizacji (gotowości) systemu **A**;
- zapobieganie konfliktom w systemie lub usuwanie ich przyczyn (skutków);
- koordynacja współdziałania w ASD (szczególnie uzgadnianie planów);
- zdolność samoregulacji i uczenia się.

Podstawowa różnica między modelem kierowania w dowolnym systemie a kierowaniem w ASD (zwłaszcza w systemach konfliktowych) polega na silniejszym występowaniu w ASD mechanizmów utrzymujących w stanie wewnętrznej stabilności poszczególne jego podsystemy oraz mechanizmu adaptacyjnego służącego do utrzymania równowagi dynamicznej (w systemach kooperacyjnych) lub uzyskania przewagi (w systemach konfliktowych, jest to widoczne w systemach logistycznych). Ponadto w ASD silniej występować będą sprzeczności:

- między koniecznością kooperacji z innymi podsystemami oraz związaną z tym koniecznością podporządkowania się sterowaniu centralnemu a potrzebą zachowania własnej autonomii (w systemach kooperacyjnych);
- między potrzebą uzyskania przewagi a koniecznością zachowania poczucia bezpieczeństwa – zapewnienia określonego poziomu gotowości (w systemach konfliktowych).

Wymienione wyżej cechy charakteryzują systemy typu „przedsiębiorstwo produkcyjne (usługowe) – rynek (klienci)” lub systemy w pewnych obszarach działalności współpracujące, w innych zaś konkurujące (rywalizujące), kierowane przez jeden ośrodek decyzyjny (np. centrum).

W modelach kierowania systemami aktywnymi są przyjmowane następujące założenia:

- każdy z podsystemów dysponuje subiektywnym opisem ASD, tzn. opisem dokonany z jego punktu widzenia i wyrażającym jego cele działania;
- dla określenia decyzji każdy podsystem powinien mieć pewne hipotezy (formułowane w kategoriach przynależności) o wyborach dokonanych przez partnera (kooperanta);
- interesy podsystemów wyrażone funkcjami celów mogą być ich partnerom (kooperantom, konkurentom) mniej lub bardziej dokładnie znane lub nieznanne.

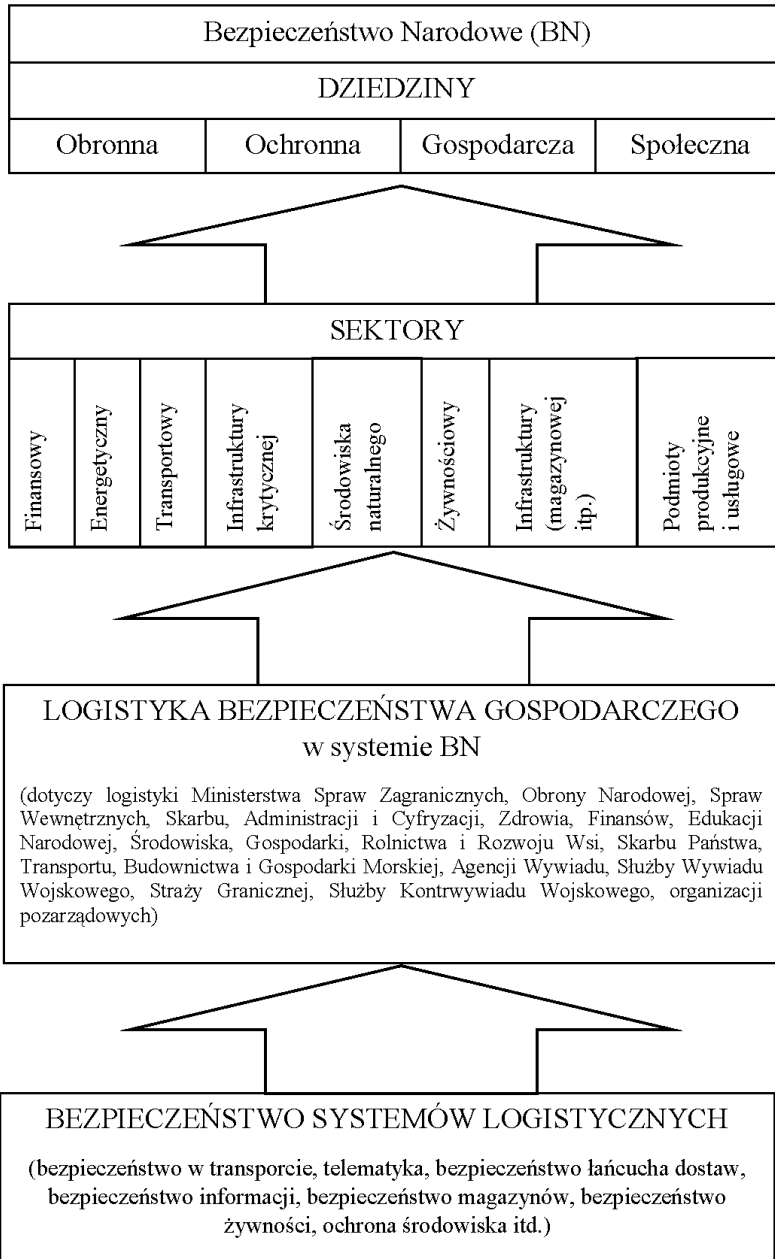
Egzemplifikacja

Bezpieczeństwo gospodarcze to bezpieczeństwo całego systemu gospodarczego oraz wzajemnych relacji (stosunków, sprzężeń) zachodzących między środowiskiem międzynarodowym, państwem i podmiotami prywatnymi. Jest jedną z dziedzin bezpieczeństwa narodowego, ściśle powiązaną z takimi sektorami, jak: finansowy, energetyczny, infrastruktury (przede wszystkim krytycznej infrastruktury państwa), środowiska naturalnego, żywności, podmiotów produkcyjnych i usługowych.

Bezpieczeństwo finansowe jest ściśle związane ze stabilnością sektora finansowego, wielkością długu publicznego oraz wielkością i strukturą rezerw dewizowych kraju itd. Z kolei bezpieczeństwo energetyczne to zapewnienie ciągłości dostaw energii i paliw, dzięki dywersyfikacji dostaw paliw, zwiększanie udziału energii ze źródeł odnawialnych oraz zdolność wydobywcza ze złóż krajowych. Nowoczesna krytyczna infrastruktura państwa jest „systemem systemów” (*system of systems*).

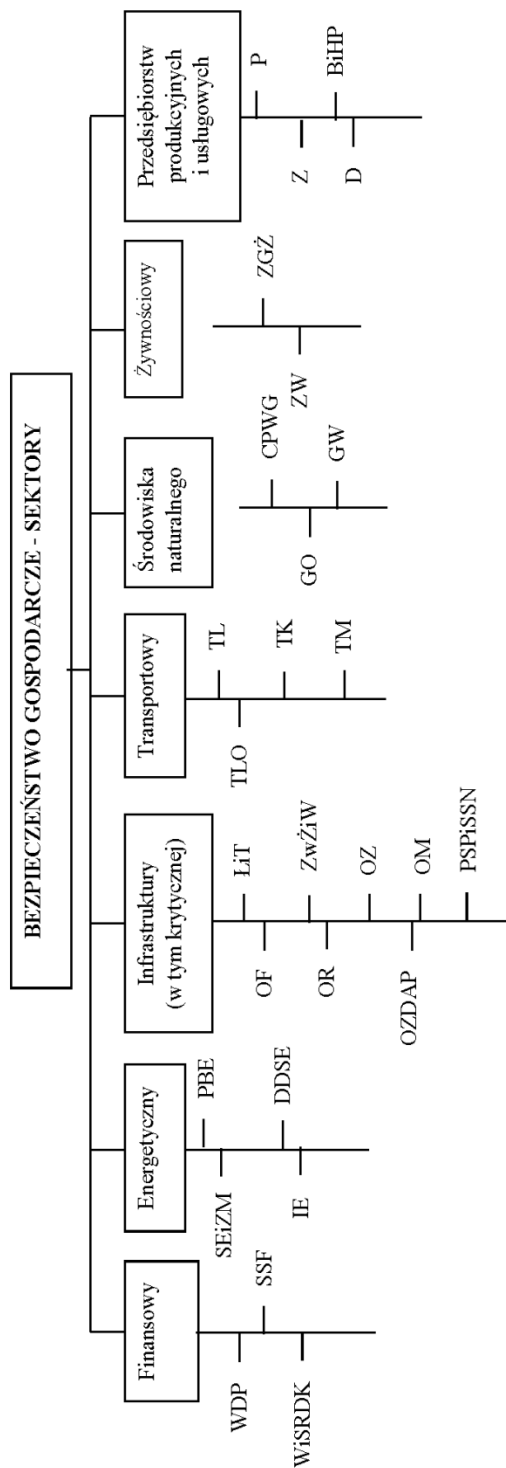
System logistyczny jest systemem stwarzającym warunki do bezpiecznego, ciągłego i efektywnego funkcjonowania dowolnego podmiotu bezpieczeństwa. Systemy logistyczne mają transsektorowy charakter, albowiem funkcjonują w afiliacji z innymi wymiarami bezpieczeństwa (zagroženiami), spełniając funkcje zaspokajania potrzeb materiałowych, energetycznych, informacyjnych itp. określonych podmiotów. Skupiając się na zależnościach przyczynowo-skutkowych należy przyjąć, że jedynie model symulacyjny w rozwiniętym środowisku informatycznym mógłby zapewnić racjonalną konfrontację rzeczywistości z przyjętymi (założonymi) współzależnościami czasowymi między zmiennymi opisującymi relacje między różnymi podmiotami i procesami.

Zlokalizowanie logistyki, jako części zasadniczej w systemie gospodarczym i jednocześnie w dziedzinie bezpieczeństwa, które podobnie jak logistyka stanowi płaszczyznę wspólną dla wielu podmiotów, wskazuje na wielość relacji i sprzężeń zwrotnych pomiędzy elementami poszczególnych podsystemów zarówno systemu gospodarczego (w tym sektorów), jak i systemów bezpieczeństwa, w tym systemu bezpieczeństwa państwa – (rys. 6.4 i 6.5).



Rys. 6.4. System bezpieczeństwa gospodarczego w kontekście bezpieczeństwa systemów logistycznych

Źródło: opracowanie własne.



SSF – stabilność sektora finansowego

WDP – wielkość długu publicznego

WiSRDK – wielkość i struktura rezerw dewizowych kraju

PBE – podmioty bezpieczeństwa energetycznego

SEIZM – surowce energetyczne i zdolność magazynowania

DDSE – dywersyfikacja dostaw surowców energetycznych

IE – infrastruktura energetyczna

LiT – łączność i telekomunikacja

OF – obroty finansowe

ZwŻiW – zaopatrzenie w żywność i wodę

OR – obiekty ratownicze

OZ – ochrona zdrowia

OM – obiekty magazynowe

OZDAP – obiekty zapewniające działanie administracji publicznej

PSPISSN – produkcja, składowanie, przechowywanie i stosowanie substancji niebezpiecznych

TL – transport lądowy

TLO – transport lotniczy

TK – transport kolejowy

TM – transport morski

GO – gospodarka odpadami

GW – gospodarka wodna

CPWG – czystość powietrza, wody, gleby

ZW – zabezpieczenie wody

ZGŻ – zabezpieczenie gospodarki żywnościowej

P – produkcja

BiHP – bezpieczeństwo i higiena pracy

Rys. 6.5. Sektory bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego

Źródło: opracowanie własne na podstawie *Białej Księgi*, Warszawa 2013.

Konieczne jest zatem zastosowanie takiej techniki odwzorowania modelowego, zwanej **modelowaniem**, która jest uniwersalnym sposobem wyrażania tego, „co robimy lub będziemy robić, jak również tego, co było wykonane w przeszłości i co istnieje obecnie”³⁷⁸. Dotyczy to zaawansowanych metod i technik modelowania, które pozwoliłyby na analizę dynamiki (procesów) i statyki (struktur) badanych (modelowanych) systemów (sieci) logistycznych.

Każdy system logistyczny podmiotu bezpieczeństwa realizuje procesy, które ulegają ciągłym zmianom i przeobrażeniom, a ich efekt końcowy czasami nie ma przebiegu wcześniej ustalonego i zaplanowanego ze względu na zmieniające się środowisko, w którym następuje przepływ rzeczowego i informacyjnego, co może oznaczać nieliniowy charakter zależności między atrybutami (cechami systemowymi).

Nie wystarczy więc statyczny opis systemu logistycznego dzięki prezentacji jego struktur wewnętrznych (organizacyjnych, funkcjonalnych). Należy dodatkowo uwzględnić zachodzące dynamiczne zmiany w analizowanym systemie logistycznym i jego otoczeniu, które mają istotny wpływ na przebieg procesów. Zatem odwzorowanie systemu logistycznego podmiotu bezpieczeństwa musi się opierać na powiązaniu opisu statycznego i dynamicznego, użytecznego w projektowaniu logistycznych eksperymentów symulacyjnych.

W modelu systemu logistycznego można wyróżnić:

- obiekt – czyli procesy logistyczne, a ściślej przepływ strumienia rzeczowego i informacyjnego w systemie gospodarczym;
- użytkownika – czyli część rzeczywistości otaczającej obiekt (np. system gospodarczy typu przedsiębiorstwo produkcyjne);
- otoczenie (środowisko) – obiekt i użytkownik są powiązani relacjami z innymi elementami zewnętrznymi, które wpływają (pozytywnie lub negatywnie) na ich zachowanie;
- relacje wewnętrzne i zewnętrzne – zdolność do zapewnienia funkcjonowania obiektu (procesów logistycznych) i użytkownika (np. przedsiębiorstwa) oraz „nawiązywania” kontaktów z otoczeniem (np. z rynkiem dostawców i odbiorców) i wpływania na powstałe tam sytuacje.

Obiekt logistyczny podmiotu bezpieczeństwa posiada wiele istotnych właściwości, takich jak:

- zdolność do stabilnych relacji (powiązań) z otoczeniem (np. zaopatrywanie systemu gospodarczego w niezbędne komponenty, wyroby zgodnie z planem lub reagowania i neutralizacji sytuacji kryzysowych w czasie powodzi, pożaru i innych zagrożeń);

³⁷⁸ Por. R. Dumnicki, A. Kasprzyk, M. Kozłowski, *Analiza i projektowanie obiektowe*, HELION, Gliwice 1998, s. 21.

- zdolność do „nawiązywania kontaktów” z otoczeniem i wpływanie na powstałe tam sytuacje (np. badanie rynku i prognozowanie popytu oraz podaży czy badanie potrzeb związanych z neutralizacją zagrożeń);
- zdolność powiązania obiektu logistycznego relacjami zjawisk związanych z obiektem oraz otoczeniem, dzięki czemu dany obiekt identyfikuje określone zjawiska mające wpływ na efektywność jego działań (np. zaspokojenie podstawowych potrzeb poszkodowanym, pomiar zadowolenia klienta, wydajność procesów logistycznych); powiązania z otoczeniem mogą wynikać z przyczyn wewnętrznych obiektu (np. wielkość zamawianych komponentów zależy od ilości zapotrzebowania klientów na wytwarzane wyroby) lub są wynikiem przyczyn zewnętrznych, które wymuszają lub wręcz ustalają te relacje (np. załamanie rynku, kryzys finansowy, działania konkurencji).

Opis obiektu, ogólnie rzecz biorąc, może dotyczyć trzech jego aspektów³⁷⁹:

- funkcjonowania (procesów rzeczowych), czyli wypełniania zadań przewidzianych przez użytkownika (zapewnienie miejsca i czasu przemieszczanego strumienia rzeczowego, czyli dostarczanie wszystkiego tam, gdzie jest na to zapotrzebowanie w całym systemie produkcyjnym);
- morfologii (struktury), czyli wewnętrznej budowy, składu elementów, powiązań pomiędzy elementami, właściwości elementów itd. (np. podsystemy logistyczne zaopatrzenia, produkcji, dystrybucji, transportu);
- organizacji (procesów informacyjno-decyzyjnych) – w tym ruchu informacji, współdziałania algorytmów sterowania.

Uwzględniając treść realizowanych zadań i podmiotu bezpieczeństwa (w omawianym przykładzie dotyczą one sfery wytwórczej), można zbudować model logistyczny pokazujący przebieg realnych procesów (strumienia rzeczowego oraz towarzyszących informacji), np. przedsiębiorstwa produkcyjnego uwzględniając otoczenie, które może sprzyjać realizowanym działaniom lub nie (rys. 6.6 i 6.7).

W takim modelu można wyodrębnić podsystemy logistyczne (obiekt): zarządzania (PZL), zaopatrywania (PLZ), produkcji (PLP), dystrybucji (PLD), recyklingu (PLR).

Pierwszy z nich jest podsystemem kierującym, natomiast pozostałe są wykonawcze. Funkcjonowanie logistycznego systemu gospodarczego nie byłoby możliwe bez uwzględnienia otoczenia (środowiska) i powiązań (relacji), do których zaliczamy:

- zasilanie zewnętrzne (np. rynek zaopatrzenia – RZ);
- odbiorców dóbr wytwarzanych (np. rynek odbiorców – RO);
- firmy zajmujące się surowcami wtórnymi, utylizacją odpadów (np. rynek recyklingu i zagospodarowania surowców wtórnych – RRiZSW);

³⁷⁹ Por. S. Paszkowski, *Podstawy teorii systemów i analizy systemowej*, WAT, Warszawa 1999, s. 19.

- wpływ otoczenia podmiotu bezpieczeństwa – OPB (otoczenie bliższe: np. strajki, blokady, klęski żywiołowe, konkurencja, regulacje prawne, kondycja ekonomiczna państwa, środowisko społeczno-polityczne, poziom techniki i technologii; otoczenie dalsze: np. globalna gospodarka, infrastruktura, międzynarodowe instytucje, sojusze gospodarcze, globalny rynek finansowy, uwarunkowania prawne, kryzysy finansowe), które można podzielić na takie, o których użytkownik ma informacje i na takie, które są mu niewiadome – tzw. zagrożenia).

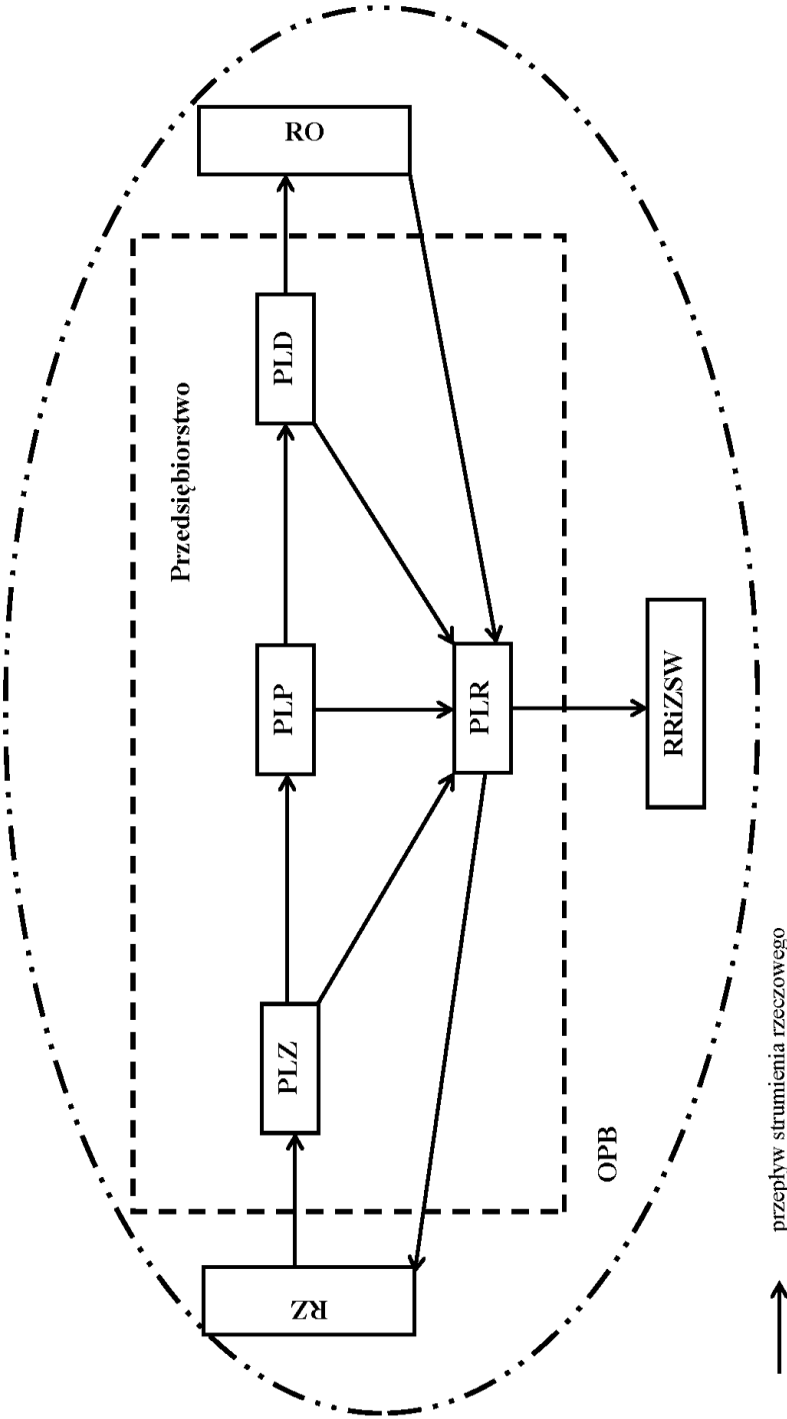
W takim systemie następuje transformacja ilościowa i jakościowa w fazach przepływu strumienia rzeczowego w podsystemie zaopatrzenia, produkcji, dystrybucji i utylizacji (rys. 6.6).

Ważną funkcję w modelu logistycznym systemu gospodarczego spełnia podsystem zarządzania, który zajmuje się planowaniem, koordynowaniem oraz logistyką wykonawczą (związaną z procesami realnymi). Dzięki wymianie informacji między podsystemami logistycznymi przedsiębiorstwa (PZL, PLZ, PLP, PLD, PLR), rynkiem zaopatrzenia i odbiorców oraz otoczeniem podmiotu bezpieczeństwa (OPB) można skutecznie i sprawnie zarządzać logistyką planistyczną i wykonawczą (rys. 6.7). Strumienie informacyjne dotyczą:

- procesów logistycznych realizowanych przez podsystemy wykonawcze w warunkach znanych i pojawiających się nieplanowo, np. w związku ze zdarzeniami kryzysowymi;
- monitorowania zdarzeń wpływających pozytywnie i negatywnie na realizowane procesy logistyczne;
- sprawozdań o stopniu realizacji zadań logistycznych;
- współdziałania między wszystkimi podsystemami logistycznymi systemu gospodarczego;
- relacji między rynkiem zbytu, zaopatrzenia oraz otoczeniem bliższym i dalszym.

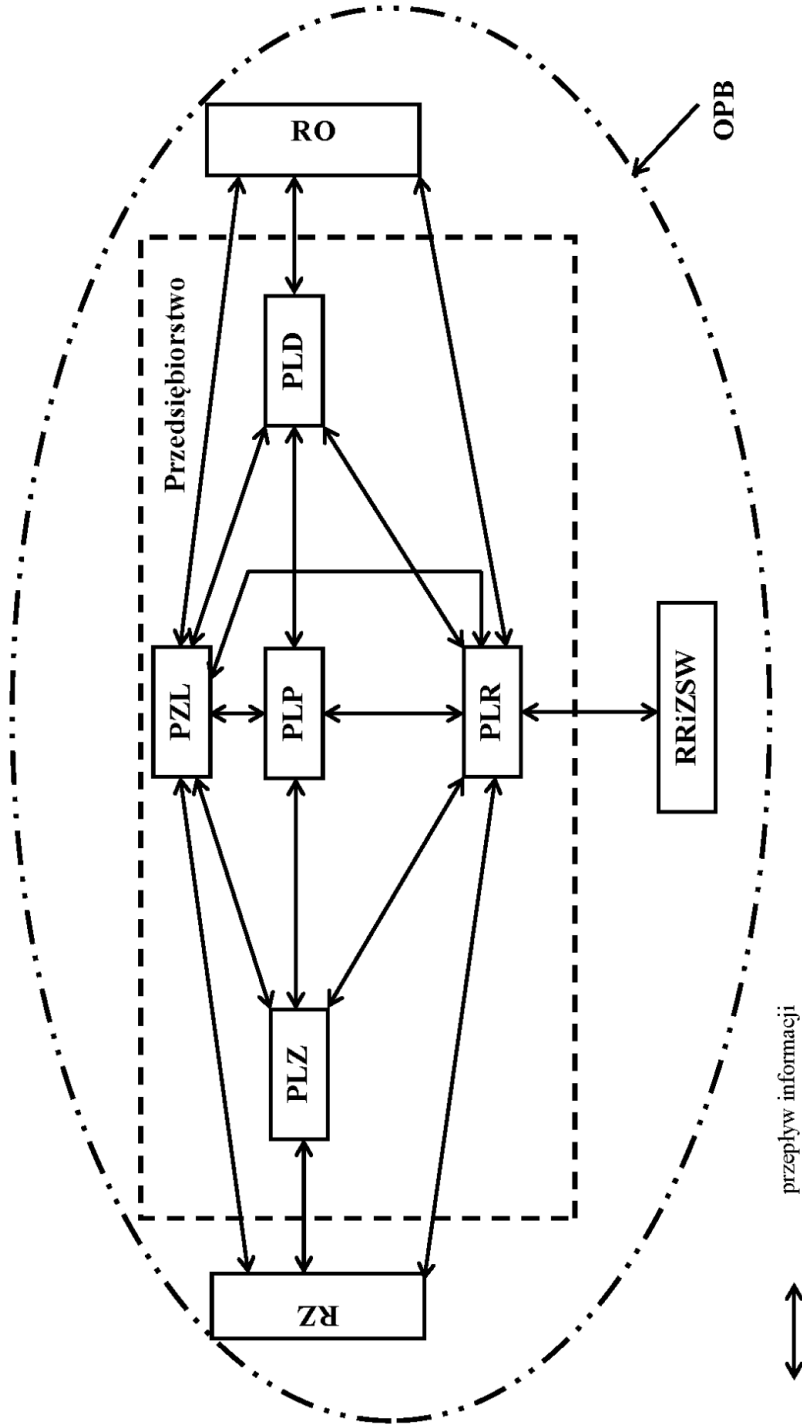
Identyfikacja wielokierunkowych i wielopoziomowych relacji w systemach: gospodarczym i logistycznych w kontekście systemu bezpieczeństwa narodowego oraz sprzężeń zwrotnych (rys. 6.8), które są tworzone w każdym wnętrzu systemu (wyodrębnionego podsystemu) przynosi spostrzeżenie, że oddziaływanie (czynnik) może być zarówno przyczyną, jak i skutkiem. Identyfikacja i rozpoznanie struktury, która narzuca zachowanie systemu, umożliwi efektywne rozpoczęcie transformacji, reorganizacji, poprawy efektywności analizowanego systemu lub innych celów modelowania.

Wpływ logistyki na system bezpieczeństwa narodowego ma charakter zarówno bezpośredni, jak i pośredni. Bezpośredni wpływ wiąże się z działaniami podejmowanymi w warunkach wystąpienia sytuacji kryzysowych i konfliktowych, gdy działania logistyki, niezawodne i skuteczne, zapewniają sprawne „obsłużenie” sytuacji kryzysowej lub konfliktowej w sensie optymalnego przepływu dóbr i ludzi, zagwarantowania adekwatnych sił i środków w określonym czasie.



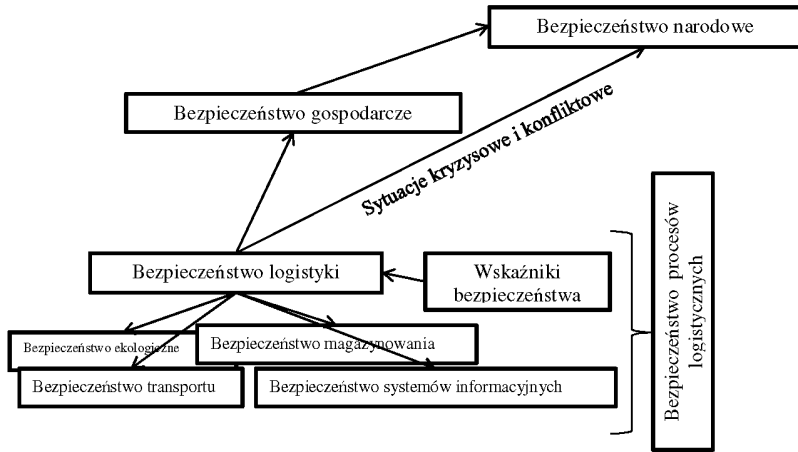
Rys. 6.6. Model logistycznego podmiotu bezpieczeństwa przedsiębiorstwa produkcyjnego – przepływ strumienia rzeczowego

Źródło: opracowanie własne.



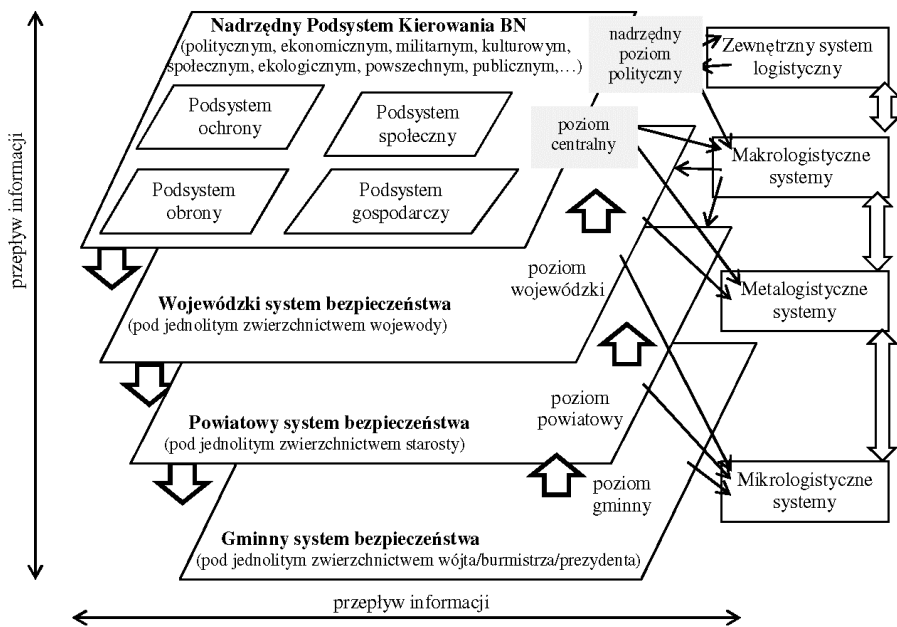
Rys. 6.7. Model logistycznego podmiotu bezpieczeństwa na przykładzie przedsiębiorstwa produkcyjnego – przepływ informacji

Źródło: opracowanie własne.



Rys. 6.8. Relacja bezpieczeństwa logistyki z systemem bezpieczeństwa narodowego

Źródło: opracowanie własne.



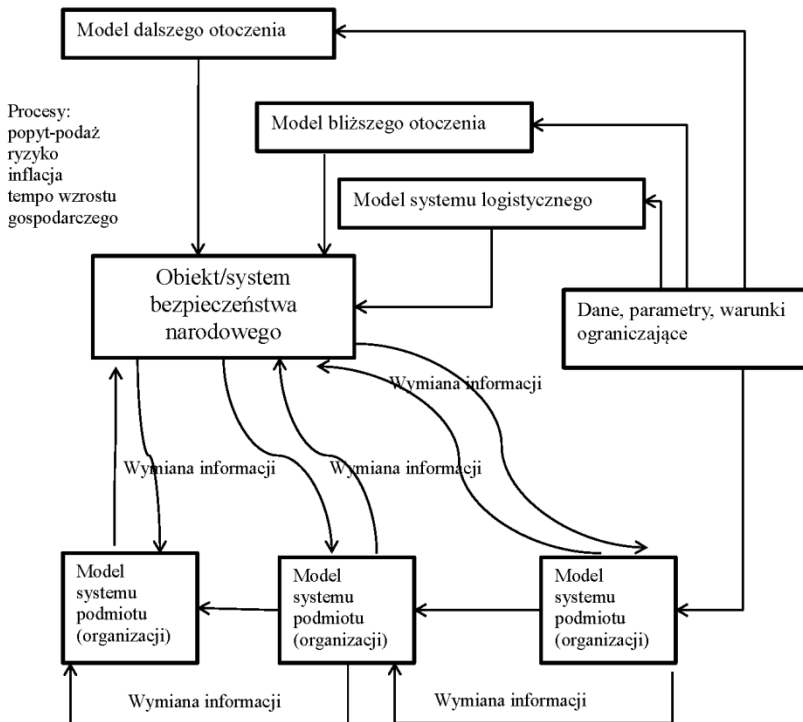
Rys. 6.9. Relacje w ujęciu horyzontalno-wertykalnym systemu bezpieczeństwa narodowego z systemami logistycznymi

Źródło: opracowanie własne.

Wpływ pośredni na poziom bezpieczeństwa narodowego pojawia się wskutek relacji logistyki w systemie gospodarki, w której procesy logistyczne są immanentną częścią wydzielonych sektorów. Gwarantem bezpieczeństwa gospodarczego i bezpieczeństwa narodowego jest bezpieczeństwo systemów (sieci) logistycznych, których bezpieczeństwo powinny być rozpatrywane (badane) w kontekście:

- zawodności bezpieczeństwa systemu zarządzania siecią (np. zakłócenia procesu podejmowania strategicznych decyzji, koordynacji i synchronizacji działań);
- zawodności bezpieczeństwa infrastruktury sieci, przede wszystkim jej technostruktury (transport, komunikacja, łączność);
- zagrożeń społecznych wewnętrznych i zewnętrznych.

Nauka i praktyka zna przykłady modelowania i wykorzystywania modeli wielowymiarowych i wielopłaszczyznowych, jak np. modele symulacyjne gospodarki narodowej³⁸⁰.



Rys. 6.10. Ogólny schemat modelowania zależności pomiędzy modelem systemu logistycznego a systemem (obiekt) bezpieczeństwa narodowego

Źródło: opracowanie własne.

³⁸⁰ *Symulacyjny model gospodarki Polski*, red. nauk. J. Gutenbaum, M. Inkelman, PAN, IBS, Warszawa 1998, s. 88.

Złożone relacje pomiędzy systemami logistycznymi a systemem bezpieczeństwa narodowego zostały uwidocznione na rys. 6.9 i 6.10.

Modele złożonych, dynamicznych, otwartych systemów buduje się w sposób hierarchiczny, opisując części składowe systemu (elementy). Z prostych modeli elementów, uwzględniając wzajemne oddziaływania, buduje się złożony model systemu.

W modelu uwzględnia się tylko wybrane czynniki i tylko w ograniczonym zakresie zmienności. Zakres uwzględnianych zjawisk zależy od dostępnej wiedzy i celu badań symulacyjnych.

6.2. Analiza wyników badań

Wprowadzenie

Współczesne działania logistyczne mają interdyscyplinarny charakter. Wynika to z istoty samej logistyki, którą obecnie w coraz szerszym zakresie wspierają nowoczesne technologie, w szczególności coraz nowszej generacji technologie informacyjno-komunikacyjne ICT (ang. *Information & Communication Technologies*). Jednym z kluczowych zagadnień efektywnego i sprawnego działania współczesnych systemów logistycznych w dynamicznie zmieniającym się środowisku jest zapewnienie pożądanego poziomu bezpieczeństwa w warunkach zakłóceń oraz wewnętrznych i zewnętrznych zagrożeń.

Wrażliwość (podatność) struktur sieci logistycznych współczesnej organizacji na różnorodne zagrożenia może skutkować kryzysem organizacyjnym, zmianami strukturalnymi, a nawet upadłością podmiotów systemów logistycznych (sieci) czy szerzej podmiotów systemu ekonomicznego (gospodarczego), co w konsekwencji może zagrozić bezpieczeństwu narodowemu.

Rosnąca złożoność i długość łańcuchów systemów logistycznych sprawia, że zapewnienie bezpieczeństwa logistycznego jest coraz trudniejsze. O skali tego wyzwania świadczą wyniki badania przeprowadzonego przez firmę Deloitte³⁸¹. Wśród 25 międzynarodowych przedsiębiorstw posiadających globalne sieci dostaw i silnie uzależnionych od reputacji własnej marki stwierdzono, że bezpieczeństwo i jakość nie są kryteriami dominującymi, jakie może dostarczyć operator. Cena ciągle jest najważniejszym kwalifikatorem wyboru usług logistycznych. Zauważyć należy, że podejście, w którym bezpieczeństwo nie jest determinantą działania dotyczy wszystkich aspektów i procesów, nie tylko związanych z bezpieczeństwem systemów logistycznych. Wśród wielu prezentowanych badań z obszaru logistyki wyróżnić można takie, które dotyczą analizy poziomu jakości wdrażanych rozwiązań logistycznych, np. w obsłudze klienta, w których ocenia się poziom satysfakcji, analizuje poziom funkcjonalności magazynu, eksploruje poziom implementacji rozwiązań nowych

³⁸¹ Supply Chain's Last Straw: A Vicious Cycle of Risk, Deloitte 2007.

technologii. Ponadto są tworzone różnego rodzaju rankingi i porównania według wybranych kryteriów.

Natomiast brakuje badań, które podejmowałyby problem oceny poziomu adaptacji rozwiązań zarówno organizacyjno-funkcjonalnych, technicznych, jak i prawnych w zakresie zastosowań systemów bezpieczeństwa w firmach logistycznych. Prezentowane badania wypełniają tę lukę.

Badania naukowe w obszarze bezpieczeństwa systemów, ze względu na rozległość powiązań strukturalno-funkcjonalnych oraz prawnych ograniczeń działających w niej systemów, są niezwykle złożone. Wynika to ze złożoności i różnorodności tych systemów, które charakteryzują się³⁸²:

- wielofunkcyjnością wynikającą z faktu, że ze względu na zasady bezpieczeństwa formułuje się zbiory różnorodnych wymagań, które grupuje się stosownie do obszaru przyszłego, planowanego funkcjonowania systemów;
- złożonością struktury systemów działania (podmiotów bezpieczeństwa, organizacji, instytucji, państwa);
- dużą liczbą podsystemów wchodzących w skład badanych systemów, pozostających w różnych relacjach (stosunkach, sprzężeniach) oraz dużą liczbą wielorakich relacji z bliższym i dalszym otoczeniem;
- specyfiką i dynamiką procesów zachodzących w systemach oraz zewnętrznych oddziaływań (wymuszeń) o charakterze losowym (stochastycznym);
- dużym zasięgiem przestrzennym systemów, brakiem jednoznaczności granic;
- rozproszonym systemem sterowania procesami informacyjno-decyzyjnymi (np. wiele ośrodków decyzyjnych, brak jasnego zakresu odpowiedzialności itp.);
- rozwiniętą, otwartą i rozległą teleinformatyczną infrastrukturą, znajdującą się w stanie permanentnego rozwoju.

Podobny charakter – złożony i interdyscyplinarny mają procesy i systemy (sieci) logistyczne, które odpowiadają za sprawne i efektywne funkcjonowanie wielu systemów istotnych z punktu widzenia bezpieczeństwa państwa. Wraz ze wzrostem złożoności sytuacji, które przychodzi rozwiązywać, wzrasta wpływ czynników losowych, niepewności i wtedy obok skutków pożądanych i zamierzonych, pojawiają się skutki niepożądane zarówno w bliższej, jak i – coraz częściej – dalszej przyszłości³⁸³.

W tym kontekście należy lokalizować problematykę bezpieczeństwa logistyki, bowiem efektem nasilającej się dynamiki zagrożeń są podejmowane działania, skierowane na optymalizację sił i środków w kierunku tworzenia

³⁸² Zob. H. Świeboda, *Zagrożenia informacyjne bezpieczeństwa RP*, Rozprawa doktorska, AON Warszawa 2009, s. 89.

³⁸³ Zob. P. Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania*, Bellona Warszawa 1994, s. 16.

zintegrowanego, kompleksowego systemu bezpieczeństwa narodowego³⁸⁴, którego logistyka jest istotnym jego składnikiem, wykorzystywanym przez system gospodarczy i system zarządzania kryzysowego³⁸⁵. Na progresywność zabezpieczenia logistycznego i technicznego systemu bezpieczeństwa mają być skierowane działania prowadzące do poprawy funkcjonowania systemów w sytuacjach kryzysowych oraz do wspierania obrony w obszarze wzmocnienia zdolności struktur administracyjno-gospodarczych.

W obszarze wzmocnienia zdolności struktur administracyjno-gospodarczych kraju do funkcjonowania w sytuacjach kryzysowych główne działania mają być skierowane na poprawę logistycznego i technicznego zabezpieczenia systemu kierowania³⁸⁶. Wzmocnienie relacji między rozwojem kraju w sensie bezpieczeństwa gospodarczego, w tym podmiotów bezpieczeństwa i logistycznego, a polityką bezpieczeństwa i obronności stworzy podstawę do racjonalnego projektowania zintegrowanego systemu kompleksowego zarządzania bezpieczeństwem narodowym.

Uznając wagę bezpieczeństwa gospodarczego, którą opisują między innymi funkcje przypisane logistyce, przyjęto założenie, że poziom jej bezpieczeństwa jest jednym z istotnych wyznaczników stopnia bezpiecznego rozwoju społeczno-gospodarczego i wpływa na poziom bezpieczeństwa ekonomicznego stanowiącego podstawy zarządzania bezpieczeństwem dla Systemu Bezpieczeństwa Narodowego (SBN). Problemy z tego obszaru obejmują również zagadnienia dotyczące organizacji logistyki na potrzeby zarządzania w sytuacjach kryzysowych.

Celem przeprowadzonych badań była diagnoza i analiza działania warunków organizacyjno-funkcjonalnych, technicznych, prawnych w podmiotach logistycznych, w zakresie zastosowania i wykorzystania możliwości, jakie dają aktualne rozwiązania:

- prawne w zakresie zgodności i przestrzegania procedur zarządzania kryzysowego;
- przestrzegania standardów krajowych i europejskich;
- funkcjonowania w strukturach organizacyjnych komórek odpowiedzialnych za bezpieczeństwo funkcjonowania systemu logistycznego;
- nowoczesnego zarządzania organizacją wymaganego dla zapewnienia wymaganego poziomu bezpieczeństwa, eskalując ku zwiększaniu poziomu bezpieczeństwa systemów logistycznych.

³⁸⁴ Por. *Strategia Rozwoju Sytemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*. Przyjęta uchwałą Rady Ministrów 9 kwietnia 2013 r.; zob. R. Zięba, J. Zajac, *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski*. Ekspertyza na zlecenie Ministerstwa Rozwoju Regionalnego, Warszawa 2010.

³⁸⁵ Regulowany Ustawą o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.

³⁸⁶ Zob. *Strategia Rozwoju*, ..., op. cit., s. 64.

Główny problem zawarto w pytaniu o warunki prawne, organizacyjno-funkcjonalne oraz techniczne, jakie aktualnie są wykorzystywane do wspomaganie zarządzania bezpieczeństwem systemów logistycznych w kontekście bezpieczeństwa gospodarczego.

Tak zaprojektowane i przeprowadzone badania bezpieczeństwa systemów logistycznych w kontekście bezpieczeństwa gospodarczego pozwalają dostrzec ważne kwestie bezpieczeństwa, dla którego odniesieniem jest bezpieczeństwo narodowe. Wyniki dostarczają wskazania do kreowania założeń polityki gospodarczej i bezpieczeństwa w szczególności w kontekście zarządzania ciągłością działania.

Badania ankietowe i rozmowy z ekspertami, ściśle związane z tematyką monografii, miały za zadanie ustosunkować się do wielu problemów oraz przyczynić się do osiągnięcia celu naukowego powiązanego z praktyką. Do zadań tych zostały zaliczone:

- po pierwsze: udzielenie odpowiedzi na pytanie: w jaki sposób należy kształtować poziom systemów bezpieczeństwa oraz kulturę bezpieczeństwa (świadomość zagrożeń i konsekwencji), a także jak identyfikować braki edukacyjne i potrzeby w tym zakresie;
- po drugie: realizacja głównego celu badawczego, którym była identyfikacja stopnia wdrożenia systemów zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych oraz poznanie zasad i form tych systemów, w kontekście zarządzania ciągłością działania, tak istotną z punktu widzenia zapewnienia bezpieczeństwa gospodarczego;
- po trzecie: osiągnięcie celów szczegółowych i aplikacyjnych, które koncentrowały się na aspektach bezpieczeństwa systemów logistycznych w kwestiach identyfikacji znajomości i poziomu wdrożenia narzędzi, procedur prawnych, organizacyjnych, technicznych zarządzania kryzysowego, a także możliwości szkolenia w tym zakresie;
- po czwarte: realizacja głównego problemu badawczego sformułowanego w postaci następującego pytania – w jakim stopniu funkcjonujący system zarządzania bezpieczeństwem systemów logistycznych zapewnia bezpieczną i niezawodną realizację zadań z zakresu bezpieczeństwa narodowego oraz jakie zmiany w systemie będą sprzyjać zapewnieniu bezpieczeństwa w warunkach możliwych i prawdopodobnych zagrożeń państwa?
- po piąte: weryfikacja hipotezy badawczej – z uwagi na fakt rosnącej liczby stwierdzonych naruszeń bezpieczeństwa podkreślono potrzebę zmian w systemie zarządzania bezpieczeństwem logistycznym, z wiodącą rolą instytucjonalnych rozwiązań opartych o przepisy prawa, standardów i ich korelacji z wewnętrznymi uregulowaniami;
- po szóste: określenie słabych i mocnych stron w funkcjonującym systemie zarządzania bezpieczeństwem struktur systemów logistycznych, z uwzględnieniem rozważań zawartych w poprzednich rozdziałach oraz wyników badań empirycznych;

- po siódme: przedstawienie rekomendacji dotyczących zmian w systemie, sprzyjających zapewnieniu bezpieczeństwa w kontekście możliwych i prawdopodobnych zagrożeń w postaci modelu systemu zarządzania bezpieczeństwem systemów logistycznych w kontekście bezpieczeństwa narodowego.

W badaniach posłużono się kwestionariuszem ankietowym (pytania ankietowe zawarto w załączniku) składającym się z metryczki i części pytań merytorycznych (zasadniczych). Posłużono się dwoma rodzajami pytań: zamkniętymi i otwartymi. Przewagę stanowiły pytania zamknięte, w których respondenci byli proszeni o wybór opcji z listy możliwych odpowiedzi.

W metryczce wyróżniono cechy charakteryzujące firmy, takie jak: wielkość firmy (mikro, małe, średnia, duża), formy prawnego zorganizowania (prywatna, państwowa, spółdzielcza, komunalna), rodzaju prowadzonej działalności (usługowa, produkcyjna, usługowo-produkcyjna, konsultingowa, inna), wykorzystywane zasoby kapitałowe (firma z krajowym kapitałem i firma z kapitałem zagranicznym).

Część merytoryczna zawierała 18 pytań, w tym 16 zamkniętych i 2 pytania otwarte, nieobarczone konkretną odpowiedzią (załącznik 3). Celem pytań było uzyskanie odpowiedzi na problemy związane z podstawami prawnymi, organizacyjnymi, technicznymi, procedurami, monitoringiem, systemem zarządzania w sytuacjach krytycznych w logistyce.

W ramach badań zaprojektowano i przeprowadzono pięć pogłębionych wywiadów opartych na pytaniach zawartych w kwestionariuszu ankietowym, które rozszerzono o dodatkowe kwestie związane z bezpieczeństwem logistyki.

W przeprowadzonych badaniach ankietowych istotną kwestią było określenie relacji między udzielanymi odpowiedziami a cechami charakteryzującymi ankietowane firmy, do których oceny wykorzystano w szczególności współczynnik kontyngencji C Pearsona, test niezależności Chi-2. Badanie relacji za pomocą wymienionego modelu matematycznego pozwala wnioskować o problemach występujących w danych grupach podmiotów. Zebrane wyniki pozwalają także na dostrzeżenie nieprawidłowości w funkcjonowaniu badanego systemu oraz umożliwiają weryfikację hipotez roboczych.

W celu określenia siły zależności między uzyskanymi odpowiedziami a wielkością ankietowanych firm wykorzystano współczynnik kontyngencji C Pearsona, który jest oparty na teście niezależności **Chi-2 (inaczej χ^2 albo Ch-kwadrat niezależności)**. Chodzi o sprawdzenie prawdopodobieństwa otrzymania takiego rozkładu liczebności, jaki akurat otrzymaliśmy w badaniu, zakładając, że te cechy są od siebie niezależne.

Wartość testu niezależności Chi-2 jest równa kwadratowi różnicy między zaobserwowaną a oczekiwaną wartością w każdej klasie, podzielonemu przez wartość oczekiwaną dla danej grupy. Wzór na test niezależności ma zatem następującą postać:

$$\chi^2 = \sum_{j=1}^k \frac{(O_j - E_j)^2}{E_j}$$

gdzie: χ^2 – test niezależności Chi-2,

O_j – liczebność otrzymana (ang. *frequency observed*) w każdej kategorii,

E_j – liczebność oczekiwana (ang. *frequency expected*) w każdej kategorii, zgodnie z przewidywaniami wynikającymi z hipotezy zerowej),

$\sum_{j=1}^k$ – suma liczebności w zakresie wszystkich kategorii od j do k,

k – liczba kategorii, na które podzielono badane podmioty.

W przeprowadzonych badaniach istotne było określenie zależności pomiędzy zmiennymi dotyczącymi dwóch czynników – A i B. W przypadku testów wielowymiarowych określa się hipotezę zerową i alternatywną:

H_0 – czynniki A i B są niezbieżne (np. pomiędzy rodzajem wielkości firmy a wybraną odpowiedzią nie zachodzi żaden związek);

H_1 – czynniki A i B są zbieżne (np. pomiędzy rodzajem wielkości firmy a wybraną odpowiedzią zachodzi stały związek).

W badaniu otrzymano dwie grupy zmiennych: A – wielkość firm, B – odpowiedzi.

Podstawę do wyznaczania mierników zależności pomiędzy cechami niemierzalnymi, opartymi na Ch-kwadrat jest tablica korelacyjna.

Przy prowadzeniu analizy danych za pomocą tabel kontyngencji mamy problemy do rozpatrzenia:

- 1) czy zaobserwowane różnice są istotne statystycznie?
- 2) jaka jest siła związku pomiędzy zmiennymi?
- 3) czy relacje są pozorne czy rzeczywiste?

W badaniu z zastosowaniem testu Ch-kwadrat należy:

- wyznaczyć wartości oczekiwane,
- wyznaczyć różnicę pomiędzy tym, co oczekiwane a tym, co zaobserwowane.

Na podstawie otrzymanych wyników wylicza się liczebność oczekiwaną, czyli wartość odpowiadającą liczbie jednostek (n), które powinny znaleźć się w danym przedziale, gdyby były one sobie równe. W badaniu mamy dwie możliwości udzielonych odpowiedzi, stąd wartość oczekiwana wynosi 50% i 50%.

Znając wartości liczebności otrzymanej i oczekiwanej, można obliczyć wartość testu niezależności Chi-2.

Wynik testu niezależności stanowi wartość empiryczną statystyki Chi-2. W celu weryfikacji hipotezy zerowej i alternatywnej niezbędne jest wyznaczenie wartości krytycznej dla testu niezależności Chi-2.

Jeżeli wartość empiryczna Chi-2 jest większa lub równa wartości krytycznej statystyki Chi-2, wówczas cechy pomiędzy badanymi czynnikami są zbieżne,

a szansa pomyłki jest mniejsza lub równa poziomowi istotności (α)³⁸⁷. Poziom istotności został określony na poziomie $\alpha = 0,05$. Jest to wartość standardowo przyjmowana bardzo często w analizach statystycznych, bowiem przyjęcie niskiego poziomu istotności pozwala na ograniczenie błędu.

Poza znajomością poziomu istotności, w celu oszacowania wartości krytycznej, należy wyznaczyć stopień swobody *df* (*degrees of freedom*), który dla testu niezależności Chi-2 oblicza się według wzoru $df = (r - 1) \times (p - 1)$, gdzie *r* i *p* oznaczają liczbę kategorii dla pierwszej i drugiej zmiennej. Na przykład, gdy $r = 4$ (dwie możliwe odpowiedzi dla zmiennej A) oraz $p = 2$ (dwie możliwe odpowiedzi dla zmiennej B). Podstawiając te wartości do wzoru, otrzymujemy liczbę stopni swobody:

$$df = (4 - 1) \times (2 - 1) = 3$$

Znając poziom istotności oraz stopień swobody, wartość krytyczną testu Chi-2 można odczytać z tablic statystycznych (odczyt jest mniej dokładny niż ocena za pomocą np. kalkulatora). Można jednak skorzystać z programu MS Excel, gdzie wartość krytyczną testu niezależności można wyznaczyć za pomocą następującej formuły: ROZKŁAD.CHI.ODW(POZIOM ISTOTNOŚCI; POZIOM SWODODY).

Jeśli wartość ta jest mniejsza od wartości empirycznej statystyki Chi-2, oznacza to, zgodnie z przyjętymi założeniami, że badane cechy są zbieżne.

Wykazana zbieżność cech pozwoli na ocenę związku między dwiema cechami jakościowymi, którą wyznaczano za pomocą współczynnika kontyngencji C Pearsona. Współczynnik ten wskazuje na siłę relacji pomiędzy badanymi czynnikami i przyjmuje dla przyjętych przedziałów określoną interpretację (tabela 6.4).

Tabela 6.4

Wartość współczynnika kontyngencji C Pearsona a siła relacji pomiędzy badanymi czynnikami

| C | Siła relacji pomiędzy badanymi czynnikami |
|---------|---|
| 0-0,2 | bardzo słaby związek między zmiennymi |
| 0,2-0,4 | słaby związek między zmiennymi |
| 0,4-0,6 | umiarkowany związek między zmiennymi |
| 0,6-0,8 | silny związek między zmiennymi |
| 0,8-1,0 | bardzo silny związek między zmiennymi |

Źródło: opracowano na podstawie B. Pułaska-Turyńska, *Statystyka ...*, op. cit., s. 285.

³⁸⁷ B. Pułaska-Turyńska, *Statystyka dla ekonomistów*, Warszawa 2011, s. 285.

Współczynnik C Pearsona jest obliczany według następującego wzoru:

$$C = \sqrt{\frac{\chi^2}{\chi^2 + N}}$$

gdzie: C – współczynnik kontyngencji C Pearsona,
 χ^2 – test niezależności Chi-2,
 N – liczebność próby badawczej.

Badania dotyczące tematyki prezentowanej monografii nie były dotychczas prowadzone w formie, w jakiej je zaprojektowano.

Charakterystyka próby badawczej³⁸⁸

W badaniu uczestniczyły osoby z firm z obszaru logistyki, reprezentujące podmioty bezpieczeństwa zarówno prywatne, państwowe, spółdzielcze, jak i komunalne. Wśród ankietowanych podmiotów były:

- nowoczesne firmy, między innymi z Żnina k/Bydgoszczy, Strykowa k/Łodzi, Mysłowic, Zabierzowa k/Krakowa, Ozorkowa k/Łodzi, Wrocławia, Grójca k/Warszawy, a także z uzyskanych danych z przedsiębiorstw w Niemczech i krajach Skandynawskich, współpracujących z nimi;
- jednostki podległe Ministerstwu Spraw Wewnętrznych i Administracji (Policji, Państwowej Straży Pożarnej);
- podmioty administracji rządowej i samorządowej.

Charakterystyka wybranych firm znajduje się w załączniku 2.

Podstawę badań stanowiła analiza ankiet, które znalazły się w bazie danych jako poprawnie wypełnione. Dane z tego sondowania opracowano komputerowo z wykorzystaniem pakietu Excela. Ich analiza stanowiła podstawę do weryfikacji postawionej na wstępie hipotezy i posłużyła do opracowania części poświęconej modelowi zarządzania bezpieczeństwem systemów logistycznych i gospodarczych w kontekście bezpieczeństwa narodowego.

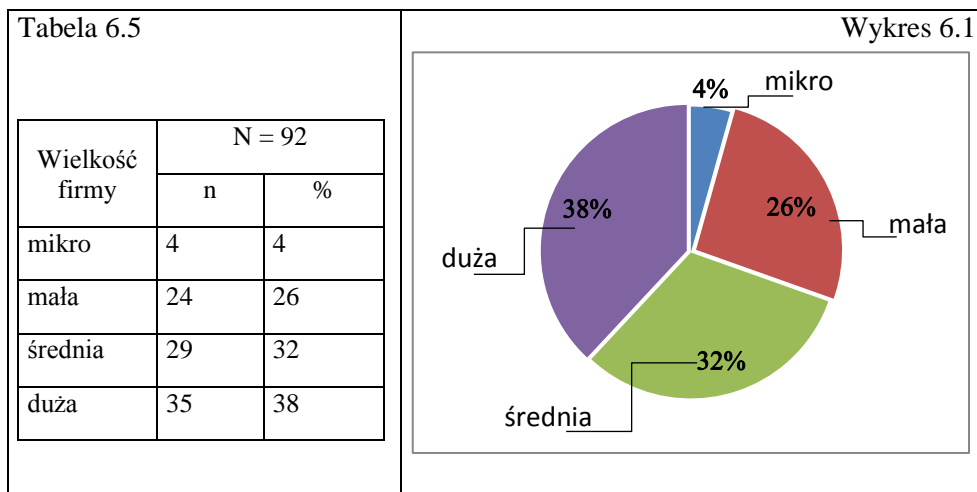
Badania i ich interpretacja

Badanie siły asocjacji między cechami charakteryzującymi grupę badaną a uzyskanymi odpowiedziami potwierdzały założenie o braku zależności cech (słaby i bardzo słaby). Tylko w jednym przypadku wyboru odpowiedzi zachodzi umiarkowana korelacja w kierunku silnego związku. Dotyczy to organizacji produkcji i/lub usług w firmie „na zamówienie” skojarzonych z wielkością firmy, co potwierdził Test χ^2 ($df = 3$, $N = 92$) = 49,24647, $p < 0,05$, $C = 0,590471$. Oznacza to, że wybór opcji organizacji produkcji i/lub usług zależy od wielkości firmy. W tym konkretnym przypadku dotyczy to firm dużych (37%), średnich (25%) i małych (25%).

³⁸⁸ W trakcie analizy metryczki ankiety celowym okazało się, by badania powiązać z pytaniem 15 i 16 kwestionariusza.

Podstawę wyróżnienia podmiotów stanowiła struktura wielkości firm określona ustawą o swobodzie działalności gospodarczej, w której dzieli się podmioty w zależności od rozmiaru. Wyróżnia się przedsiębiorstwa: mikro, małe, średnie i duże. Wśród badanych firm najliczniejszą grupę stanowiły: firmy duże (38%) zatrudniające powyżej 250 pracowników, kolejną grupą firm to firmy średnie (32%) zatrudniające do 250 pracowników i małe (26%) zatrudniające do 50 pracowników. Niewielką grupę spośród badanych firm stanowiły firmy mikro (4%) zatrudniające do 10 pracowników. Zestawienie obrazuje tabela 6.5 i wykres 6.1.

Charakterystyka próby badawczej – struktura wielkości badanych firm³⁸⁹

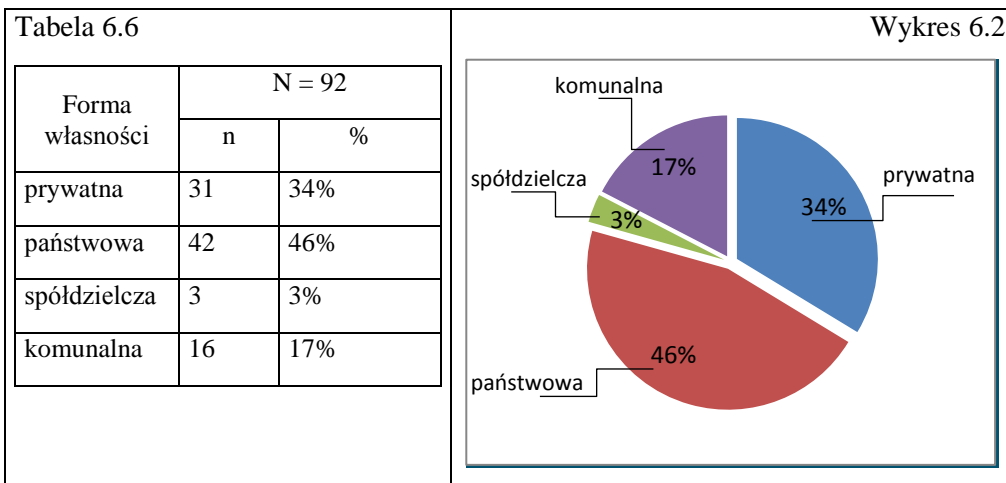


W grupie badanych firm zidentyfikowano cztery formy własności. Najliczniej reprezentowane były firmy (przedsiębiorstwa) będące własnością skarbu państwa, tzw. państwowe (46%), kolejną grupę pod względem ilości stanowiły firmy prywatne (34%), następną grupę tworzyły firmy komunalne (samorządów terytorialnych) – 17% badanych firm i tylko 3% to firmy o spółdzielczej formie własności (tabela 6.6 i wykres 6.2). W sumie podmioty sektora publicznego stanowiły 66% badanej próby.

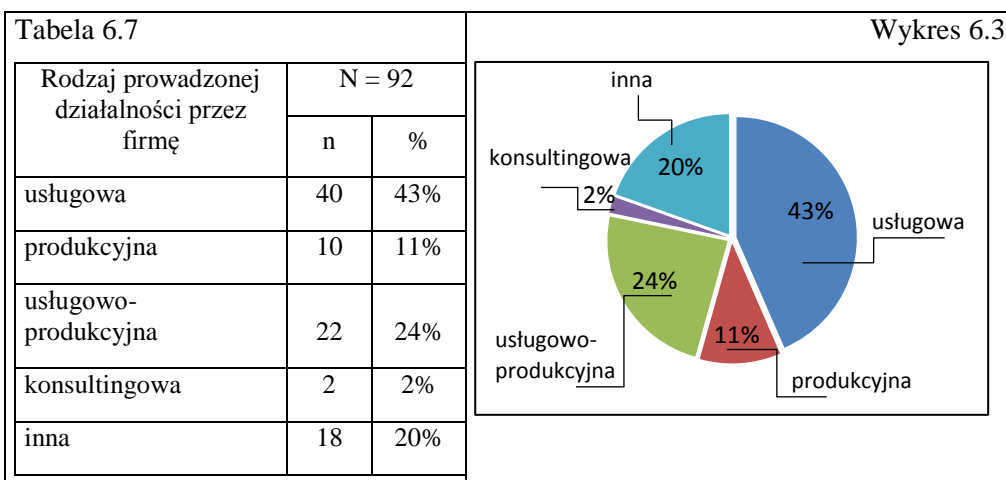
Ze względu na rodzaj prowadzonej działalności wyróżniono firmy usługowe, jako grupę najliczniej reprezentowaną (43%), usługowo-produkcyjne (24%), produkcyjne (11%) oraz konsultingowe stanowiące niewielki odsetek (2%) ogółu badanych podmiotów. Stosunkowo liczną grupę stanowiły firmy wyróżnione jako „inne”, których nie dało się przypisać do żadnej kategorii (20%). Zestawienie obrazuje tabela 6.7 i wykres 6.3.

³⁸⁹ W każdej tabeli użyty symbol „n” oznacza ilość rodzajów (typów) z liczby N – badanych oraz źródłem wszystkich tabel i wykresów są wyniki badań.

Wyróżnienie firm ze względu na formę własności



Rodzaj prowadzonej działalności przez firmy



Jedną z podstawowych kategorii ekonomicznych, wieloznaczną i różnie interpretowaną jest skład, stopień płynności i źródło pochodzenia kapitału. Ze względu na źródła pochodzenia kapitału w badaniach przyjęto kryterium, że firmy finansowane są bądź kapitałem krajowym (własnym), bądź kapitałem obcym. Analiza odpowiedzi pozwoliła stwierdzić, że struktura finansowania działalności badanych firm w 93% była pokrywana własnym kapitałem, a tylko w 7% firmy korzystają z kapitału obcego. Zestawienie obrazuje wykres 6.4 – załącznik 6.1.

Do pytań charakteryzujących grupę badanych firm należą pytania dotyczące sposobu organizacji produkcji i/lub usług, tj. (w ankiecie pytanie 15 oraz 16). Organizacja produkcji i/lub usług w firmach może być realizowana w dwóch wariantach (tabela 6.8):

- 1) na zamówienie dla konkretnego klienta/ usługodawcy lub
- 2) na podstawie prognozowania popytu – na magazyn.

Tabela 6.8

Rozkład odpowiedzi na pytanie o organizację produkcji/usług

| | | | N = 92 | |
|---|---------------|-----|--------|-----|
| | | | n | % |
| Czy organizacja produkcji/usług w Firmie/Instytucji realizowana jest: | Na zamówienie | TAK | 79 | 86% |
| | | NIE | 13 | 14% |
| | Na magazyn | TAK | 31 | 34% |
| | | NIE | 61 | 66% |

Różnica między sposobem organizacji produkcji i/lub usług na „zamówienie” i na „magazyn” wynosi 52%. Wśród badanych firm są podmioty, które realizują procesy produkcji i usług, stosując oba warianty. Firmy te stanowią 20% grupy badawczej (18 podmiotów).

Wybór działań „na zamówienie”, które podejmują firmy w celu organizacji produkcji i/lub usług jest preferowany przede wszystkim w 32% firm dużych, wobec 7% firm tego segmentu, które organizują produkcję w inny sposób. W firmach średnich i małych ¼ podmiotów organizuje produkcję z wykorzystaniem sposobu „na zamówienie”. W segmencie firm mikro 4% organizuje produkcję na zamówienie. Zestawienie obrazuje tabela 6.9.

Tabela 6.9

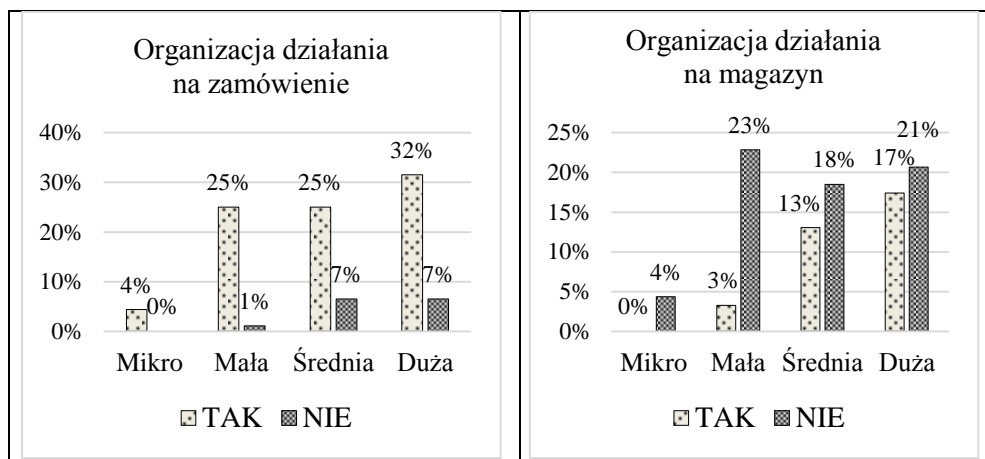
Zestawienie liczebności i odsetka odpowiedzi dla pytania o organizację produkcji i/lub usług w wariantach „na zamówienie” i „na magazyn” w zależności od wielkości firmy

| Wielkość firmy | Organizacja produkcji/usług w Firmie | | | | | | | |
|----------------|--------------------------------------|----|-----|----|-------------------|----|-----|----|
| | Na zamówienie | | | | Na magazyn | | | |
| | Liczebność N = 92 | | | | Liczebność N = 92 | | | |
| | TAK | % | NIE | % | TAK | % | NIE | % |
| Mikro | 4 | 4 | 0 | 0 | 0 | 0 | 4 | 4 |
| Mała | 23 | 25 | 1 | 1 | 3 | 3 | 21 | 23 |
| Średnia | 23 | 25 | 6 | 7 | 12 | 13 | 17 | 18 |
| Duża | 29 | 32 | 6 | 7 | 16 | 17 | 19 | 21 |
| Razem | 79 | 86 | 13 | 14 | 31 | 34 | 61 | 66 |

Analiza odpowiedzi pozwala stwierdzić, że 86% firm (79 podmiotów) działa organizując produkcję i/lub usługi na zamówienie konkretnego klienta/usługobiorcy, natomiast w 34% badanych firm opiera się na wariacie prognozowania popytu (tabela 6.8 i wykres 6.5, który jest w złączniku 6.1).

Wykres 6.6

Odsetek odpowiedzi na pytanie: czy organizacja produkcji /usług w Firmie/Instytucji jest realizowana na zamówienie dla konkretnego klienta/usługodawcy czy „na magazyn” w zależności od wielkości firmy?

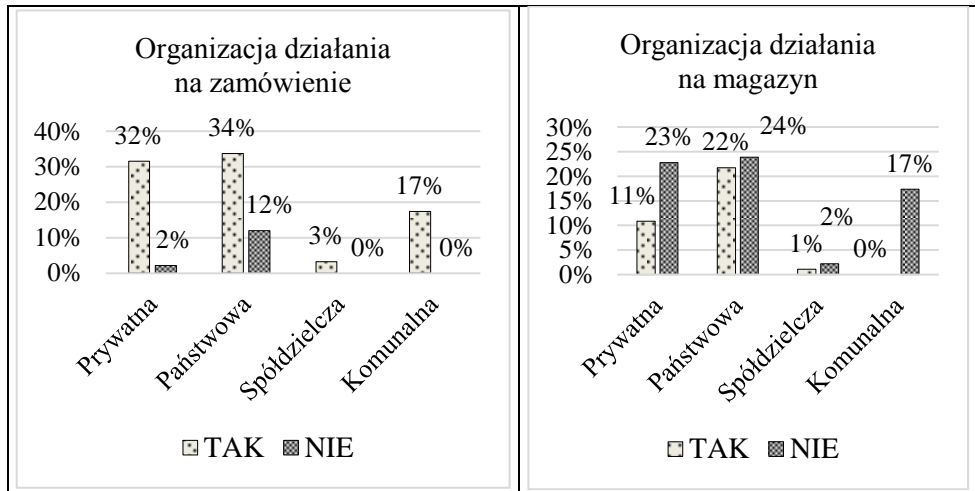


Drugą funkcją zarządzania przepływem dóbr i informacji w procesach produkcji jest forma organizacji produkcji i/lub usług „na magazyn” na podstawie prognozowania popytu. W takiej postaci realizacja organizacji produkcji powoduje, że przedsiębiorstwo dostarcza na rynek produkty standardowe (standaryzacja). Na ostateczną postać produktu klient nie ma wpływu. Jest to produkcja powtarzalna, masowa, wielkoseryjna.

Szczegółowa analiza rozkładu zmiennych wskazała, że według formy realizacji „na magazyn” taka forma jest podstawą organizacji działalności dla 16 podmiotów dużych (17%), 12 podmiotów średniej wielkości (13%), 3 firm małych (3%). W firmach mikro, w badanej próbie przedsiębiorstw, taka podstawa organizacji produkcji i/lub usług nie występuje. Zestawienie obrazuje wykres 6.6.

W przypadku badania zależności między formą własności firmy a sposobami organizacji produkcji i/lub usług forma „na zamówienie” jest stosowana w 34% firm państwowych (31 podmiotów) i 32% firm prywatnych (29 podmiotów), 17% komunalnych (16 podmiotów) oraz w 3% firm spółdzielczych (3 podmioty). Wśród firm komunalnych i spółdzielczych 100% organizuje działania „na zamówienie”. Zestawienie obrazuje wykres 6.7.

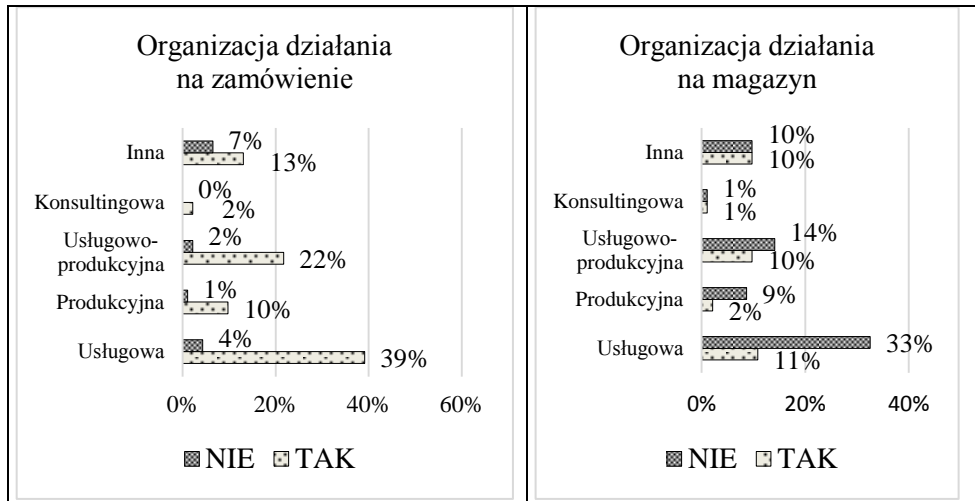
Odsetek firm organizujących procesy produkcji i usług na zamówienie dla konkretnego klienta oraz „na magazyn” w zależności od formy własności firmy



Wśród grupy firm, w których organizację produkcji realizuje się wykorzystując sposób „na magazyn” najliczniej są reprezentowane firmy państwowe: 20 podmiotów, co stanowi 22% ogółu badanych firm. Kolejna grupa to firmy prywatne 10 podmiotów, co stanowi 11% badanych i 1 firma typu spółdzielczego (1% badanych). W firmach komunalnych ta forma organizowania produkcji nie występuje, a wśród firm spółdzielczych stanowi tylko 1%. Zestawienie przedstawia wykres 6.7.

W przypadku badania zależności między profilem działalności firmy a sposobem organizacji produkcji i/lub usług, formę na zamówienie konkretnego klienta (usługobiorcy) realizuje 39% firm o profilu usługowym (36 podmiotów), 22% firm usługowo-produkcyjnych (20 podmiotów), 10% produkcyjnych (9 podmiotów), 2% firm konsultingowych (2 podmioty). Pokażną grupę stanowi 13% firm (12 podmiotów), które nie zostały na tyle zidentyfikowane, aby można było je przypisać do wyróżnionych kategorii odpowiedzi (wykres 8). Analiza rozkładu zmiennych wykazała, że najczęściej tę formę organizacji produkcji na magazyn stosują firmy usługowe (11%), po 10% firmy usługowo-produkcyjne i zakwalifikowane do grupy „inne”, 2% – produkcyjne i 1% – firmy konsultingowe. Zestawienie obrazuje wykres 6.8. Potwierdza się wcześniejsze spostrzeżenie, że firmy chętniej stosują organizację produkcji w oparciu o działania „na zamówienie”.

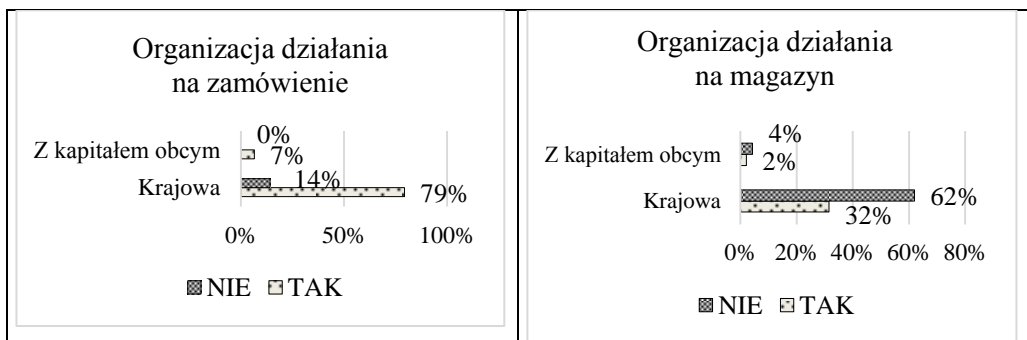
Odsetek firm organizujących procesy produkcji i usług na zamówienie konkretnego klienta oraz w oparciu o „na magazyn” w zależności od rodzaju firmy oraz profilu działalności



Analiza rozkładu zmiennych w tabeli krzyżowej, łącząca sposób organizacji produkcji i/lub usług na zamówienie z formą finansowania działalności, wskazuje, że 79% firm z kapitałem krajowym i 7% firm z kapitałem obcym organizuje produkcję i/lub usługi w oparciu o zamówienia dla konkretnego klienta/usługodawcy. 32% firm z kapitałem krajowym i 2% z kapitałem obcym stosuje metodę „na magazyn” (wykres 6.9).

Wykres 6.9

Odsetek firm organizujących procesy produkcji i usług na zamówienie konkretnego klienta oraz w oparciu o sposób „na magazyn” w zależności od finansowania działalności



Podstawą produkcji i lub usług w firmie czy instytucji może być:

- 1) zaopatrzenie z własnego magazynu, co oznacza, że towary muszą być wcześniej zakupione i znajdują się we własnym magazynie,
- 2) bieżąca realizacja potrzeb, czyli zaspokojenie potrzeby wymaga złożenia zamówienia na wybrany towar.

Tabela 6.10

Rozkład odpowiedzi na pytanie o podstawę produkcji/usług w firmie w zależności od wyboru wariantu

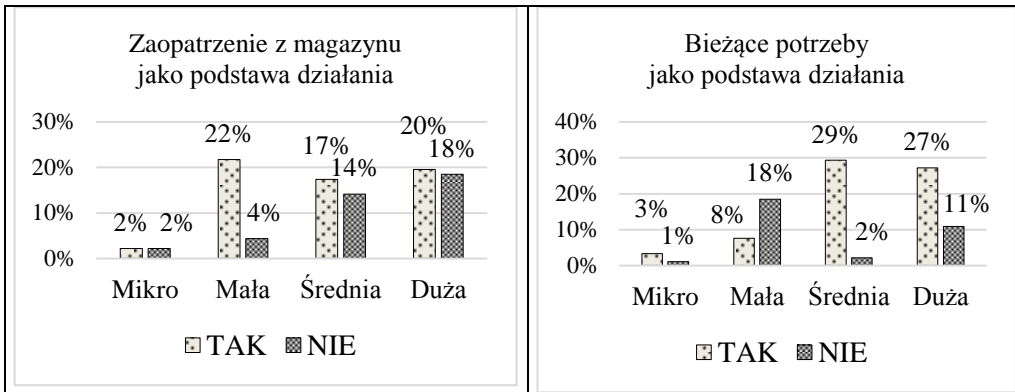
| | | Zaopatrzenie z magazynu | | Bieżąca realizacja potrzeb | |
|-----------------------------------|-----|-------------------------|---------|----------------------------|---------|
| Podstawa produkcji/usług w firmie | TAK | 56 | 61% | 62 | 67% |
| | NIE | 36 | 39% | 30 | 33% |
| Razem | | 92 | 100,00% | 92 | 100,00% |

Firmy korzystają z obu możliwości, organizując działania produkcyjne lub usługowe. Metodę zaopatrzenia z magazynu stosuje 56 podmiotów, co stanowi 61% firm przy 39% firm, które tej metody nie stosują. Natomiast metodę opartą na bieżącej realizacji potrzeb mają wdrożone 62 podmioty, co stanowi 67%, przy czym 33% firm odpowiedziało przecząco. Analiza wskazuje, że wśród badanych firm są takie, które wykorzystują obie metody organizacji podstaw produkcji i/lub usług (tabela 6.10, wykres 6.10, który jest w załączniku 6.1).

Wśród firm wyróżnionych ze względu na wielkość, które metodę zaopatrzenia „z magazynu” stosują jako podstawę organizacji produkcji i/lub usług jest 22% małych firm, 20% dużych 17% średniej wielkości i 2% firm mikro. Zwraca uwagę, że w przypadku firm dużych i średnich duży jest odsetek podmiotów, w których nie stosuje się zaopatrzenia z magazynu jako podstawy działania: 18% duże firmy i 14% firmy średnie (wykres 6.11).

Sposób organizacji podstaw produkcji w oparciu o „bieżące potrzeby”, jako podstawy działania, jest stosowany w przypadku 29% firm średniej wielkości wobec tylko 2%, które tego sposobu nie stosują. Ze sposobu tego korzysta również 27% firm dużych, przy czym duży jest odsetek firm (11%) w tym segmencie, które tego sposobu nie stosują. Sposób ten jest stosowany w 8% firm małych, wobec 18% firm, które podają, że tego sposobu nie stosują, i w 3% firm mikro. Więcej firm z segmentu średnich podmiotów i dużych wybiera sposób realizacji produkcji i/lub usługi korzystając ze sposobu „bieżące potrzeby” (wykres 6.11).

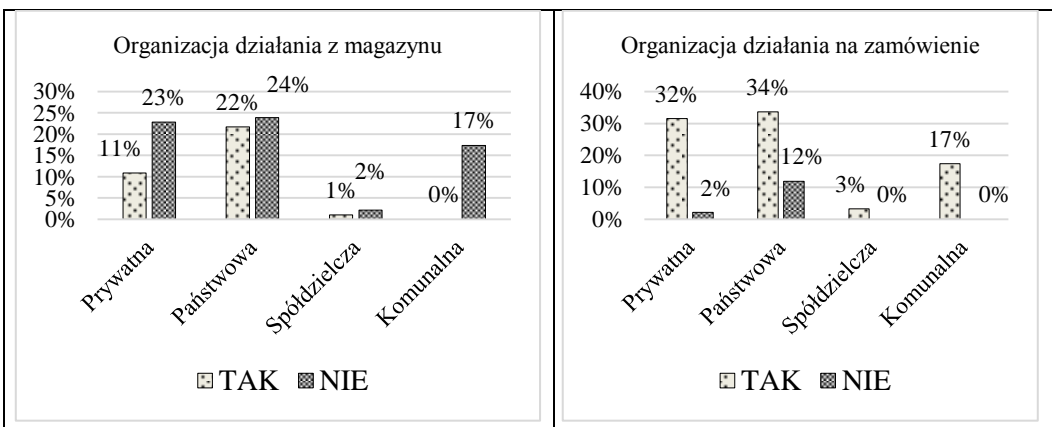
Odsetek firm stosujących zaopatrzenie „z magazynu” jako podstawę organizacji produkcji i/lub usług oraz według bieżącej realizacji potrzeb w zależności od wielkości



Sposób zaopatrywania „z magazynu” najczęściej jest realizowany w firmach państwowych (22%), przy czym 24% nie preferuje zaopatrywania z magazynu, w firmach komunalnych w 17%, w firmach prywatnych ten sposób stosuje 11% firm oraz 1% firm spółdzielczych. Wśród firm komunalnych w badanej próbie 100% organizuje podstawę produkcji w trybie „zaopatrzenie z magazynu” i 1% firm spółdzielczych. W przypadku organizacji „na zamówienie” najwięcej jest firm prywatnych (32%) i państwowych (34%). Zestawienie obrazuje wykres 6.12.

Wykres 6.12

Odsetek firm organizujących produkcję i/lub usługi w oparciu o „na magazyn” oraz sposobu „na zamówienie” w zależności od formy własności

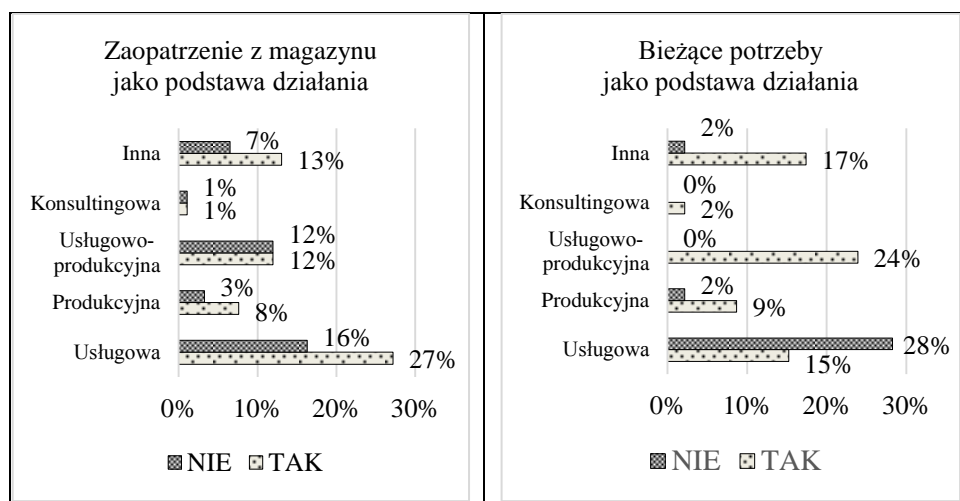


Zaopatrzenie z magazynu najczęściej jest realizowane w 27% w firmach usługowych, usługowo-produkcyjnych w 12%, a produkcyjnych w 8%. Wśród firm „innych” forma zaopatrzenia z magazynu jest stosowana w przypadku 13% firm. W przypadku organizacji „na zamówienie” taki typ produkcji deklaruje najwięcej firm usługowych (28%) i usługowo-produkcyjnych (24%). Zestawienie obrazuje wykres 6.13.

Rozkład odpowiedzi wskazuje, że 57% firm z kapitałem krajowym stosuje „zaopatrzenie z magazynu” wobec 37% firm, które nie stosują tego sposobu. W przypadku firm z kapitałem obcym jest to 4% wobec 2% firm niestosujących.

Wykres 6.13

Odsetek firm stosujących zaopatrzenie „z magazynu” jako podstawę organizacji produkcji i/lub usług w zależności od rodzaju działalności



Wyniki badań merytorycznych (zasadniczych)

Badanie siły asocjacji między cechami charakteryzującymi grupę badaną a uzyskanymi odpowiedziami w większości przypadków potwierdziło założenie o braku zależności cech (słaby i bardzo słaby). Tylko w 2 przypadkach wyboru odpowiedzi zachodzi umiarkowana korelacja w kierunku silnego związku.

Pierwszy jest związany relacją zachodzącą pomiędzy wdrożeniem podstaw prawnych zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych a wielkością firm ankietowanych, co potwierdził Test χ^2 (df = 3, N = 92) = 49,24647, $p < 0,05$, $C = 0,590471$. Oznacza to, że wybór opcji zależy od wielkości firmy. W tym przypadku dotyczy to: 29% firm dużych, 20% firm średniej wielkości, 21% firm małych.

Drugi dotyczy relacji zachodzących pomiędzy wdrożeniem podstaw prawnych zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych a własnością firmy, co potwierdził to Test χ^2 (df = 3,

$N = 92$) = 38,99846, $p < 0,05$ $C = 0,54562$. Oznacza to, że wybór opcji zależy od formy własności firmy. W tym przypadku dotyczy to: 37% firm państwowych (komunalne 17%, prywatne 11%, spółdzielcze 3%).

Pytanie 1

W zakresie bezpieczeństwa systemów logistycznych firmy zapytano o wdrożenie podstaw prawnych zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych.

Wdrożenie podstaw prawnych zarządzania kryzysowego przyczynia się do zapewniania koordynacji przepływów zasobów materialnych, informacji, osób w sytuacjach wystąpienia zdarzeń niepożądanych, w konsekwencji stając się czynnikiem podniesienia poziomu bezpieczeństwa. Ogółem na 92 badane firmy w 63 przypadkach (co stanowi 68% próby) wdrożono podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych, natomiast dla 32% (29 firm) problem pozostaje nierozwiązany (tabela 6.11).

Tabela 6.11

Rozkład odpowiedzi na pytanie: czy wdrożono podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych?

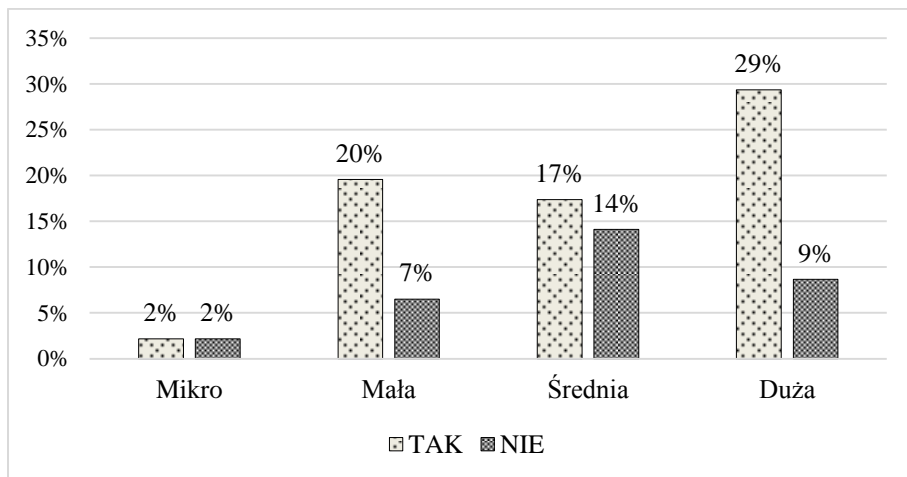
| | | N = 92 | |
|--|-----|--------|---------|
| | | n | % |
| Wdrożenie podstaw prawnych zarządzania kryzysowego | TAK | 63 | 68% |
| | NIE | 29 | 32% |
| Razem | | 92 | 100,00% |

Analiza rozkładu zmiennych w tabeli krzyżowej ujawniła, że w zależności od wielkości firmy zgodność funkcjonowania z aktualnymi regulacjami prawnymi i wewnętrznymi dokumentami organizacyjnymi zapewnia 29% firm dużych, 17% firm średniej wielkości, 20% firm małych i 2% firm mikro. Nie wszystkie firmy zapewniają zgodność funkcjonowania. Wśród grupy firm dużych jest to 9%, średnich 10%, małych 5% i mikro 1% (wykres 6.14).

Największy odsetek wdrożeń w obszarze podstaw prawnych zarządzania kryzysowego mają firmy państwowe (37%). Jest to znaczny odsetek w porównaniu do grupy firm komunalnych, w której 17% ma wdrożone podstawy prawne. W grupie firm prywatnych wdrożenia posiada 11% podmiotów, a w spółdzielczych 3%.

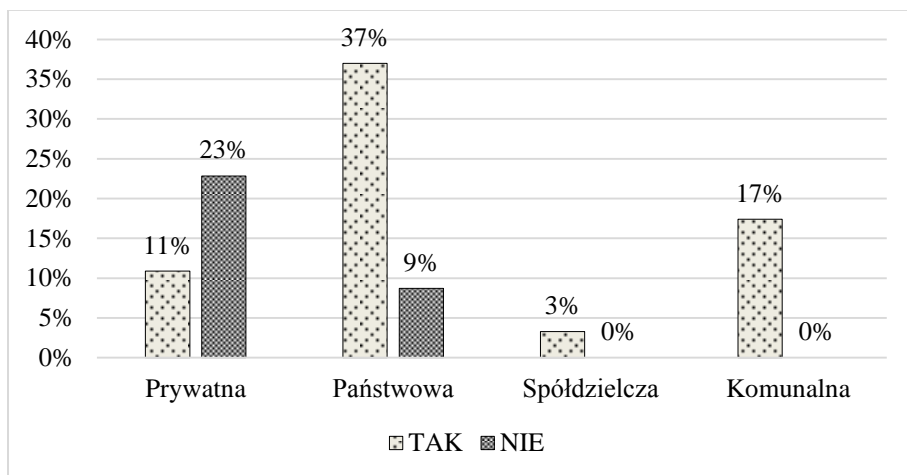
Wykres 6.14

Odsetek firm, które wdrożyły podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych w zależności od wielkości



Wykres 6.15

Odsetek firm, które wdrożyły podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych w zależności od formy własności



Duży jest odsetek firm prywatnych (23%), w których nie ma wdrożonych podstaw prawnych zarządzania kryzysowego, również 9% podmiotów w grupie

firm państwowych nie posiada takiego wdrożenia. W firmach komunalnych i spółdzielczych 100% firm takie wdrożenia posiada (wykres 6.15).

W grupie firm wyróżnionych ze względu na rodzaj prowadzonej działalności, w której wdrożono podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych, najliczniejszą stanowi segment firm usługowych – 33%. Kolejną grupę tworzą firmy zakwalifikowane do kategorii „inne”, w której 17% firm posiada wdrożenia prawnych podstaw zarządzania kryzysowego. W grupie firm usługowo-produkcyjnych jest to 14%, a w grupie firm produkcyjnych jest to tylko 4% podmiotów. W firmach typu konsultingowego 2% posiada wdrożenia, w grupie tej nie ma firm bez wdrożeń. W wyróżnionych grupach rodzajów prowadzonej działalności występuje niewielki odsetek firm, które nie zapewniają wdrożeń z zakresu podstaw zarządzania kryzysowego: firmy usługowe – 11%, usługowo-produkcyjne – 10%, produkcyjne – 7%, inne – 2%, konsultingowe – 1%. Zestawienie obrazuje tabela 6.12.

Tabela 6.12

Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj firmy | N = 92 | | | | Suma |
|----------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Usługowa | 30 | 33% | 10 | 11% | 40 |
| Produkcyjna | 4 | 4% | 6 | 7% | 10 |
| Usługowo-produkcyjna | 13 | 14% | 9 | 10% | 22 |
| Konsultingowa | 0 | 0% | 2 | 2% | 2 |
| Inna | 16 | 17% | 2 | 2% | 18 |
| Razem | 63 | 68% | 29 | 32% | 92 |

Tabela 6.13

Rozkład odpowiedzi związany z finansowaniem działalności

| Sposób finansowania działalności | Wartość otrzymana | | | | Suma |
|----------------------------------|-------------------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Krajowa | 58 | 63% | 28 | 30% | 86 |
| Z kapitałem obcym | 5 | 5% | 1 | 1% | 6 |
| Razem | 63 | 68% | 29 | 32% | |

Badanie zależności wdrożenia podstaw prawnych zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych w zależności od sposobu finansowania działalności wykazało, że wdrożeniem podstaw

prawnych legitymuje się 63% firm z kapitałem krajowym, przy 28% firm, które tych wdrożeń nie mają. W grupie firm z kapitałem obcym 5% posiada wdrożenia, przy 1% firm, które wdrożeń nie posiadają (tabela 6.13).

Pytanie 2

Czy zapewniona jest zgodność funkcjonowania podmiotu z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie kryzysowe?

Wśród badanych firm $\frac{3}{4}$, tj. 75% (69 podmiotów), zapewnia zgodność funkcjonowania podmiotu z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie kryzysowe, jednocześnie $\frac{1}{4}$, tj. 25% firm (23 podmioty), tej zgodności nie zapewnia (tabela 6.14).

Tabela 6.14

Rozkład odpowiedzi na pytanie o zapewnienie zgodności funkcjonowania podmiotu z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie kryzysowe

| | | N = 92 | |
|--|-----|--------|---------|
| | | n | % |
| Zapewnienie zgodności funkcjonowania podmiotu z aktualnymi regulacjami | TAK | 69 | 75% |
| | NIE | 23 | 25% |
| Razem | | 92 | 100,00% |

Szczegółowa analiza rozkładu zmiennych w tabeli krzyżowej ujawniła, że w zależności od wielkości firmy zgodność funkcjonowania z aktualnymi regulacjami prawnymi i wewnętrznymi dokumentami organizacyjnymi zapewnia 29% firm dużych, 20% firm średniej wielkości, 21% firm małych i 3% firm mikro. Wśród wyróżnionych kategorii firm występują firmy, które tej zgodności funkcjonowania nie zapewniają. W grupie firm dużych jest to 9%, w grupie firm średnich to 10%, w małych 5%, i 1% w firmach mikro. Zestawienie rezultatów podano w tabeli 6.15 i wykresie 6.16, który jest w załączniku 6.1.

Szczegółowa analiza rozkładu zmiennych tabeli krzyżowej wykazała, że zgodność funkcjonowania wewnętrznych dokumentów organizacyjnych z aktualnymi regulacjami prawnymi zapewnia 39% firm państwowych wobec 7% firm, które tej zgodności nie zapewniają. Ponadto zgodność jest zapewniona w grupie firm komunalnych (17% podmiotów) i w 3% firm w grupie firm spółdzielczych.

Tabela 6.15

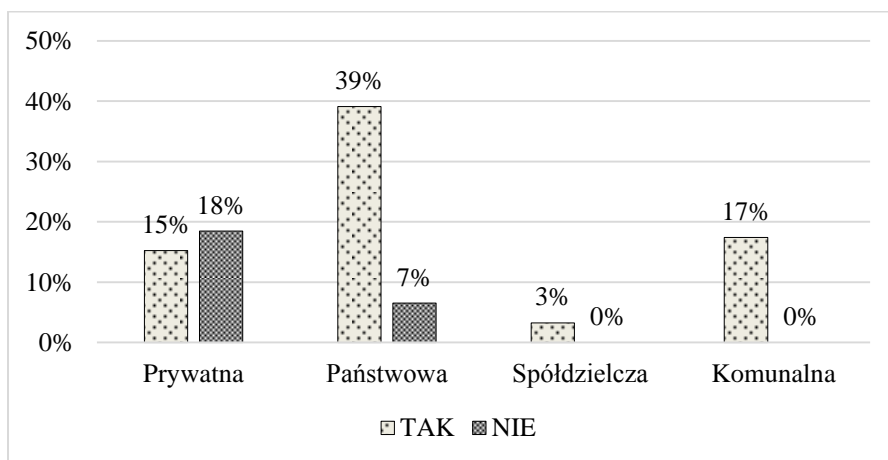
Rozkład odpowiedzi w zależności od wielkości firmy

| Wielkość firmy | Wartość otrzymana | | | | Suma |
|----------------|-------------------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Mikro | 3 | 3% | 1 | 1% | 4 |
| Mała | 19 | 21% | 5 | 5% | 24 |
| Średnia | 20 | 22% | 9 | 10% | 29 |
| Duża | 27 | 29% | 8 | 9% | 35 |
| Razem | 69 | 75% | 23 | 25% | |

Zauważyć należy, że w grupie firm spółdzielczych i komunalnych (w 100% w badanej grupie) jest zapewniona zgodność dokumentacyjna. W grupie firm prywatnych 15% podmiotów zapewnia zgodność, lecz większy jest odsetek (18%) firm, które tej zgodności nie zapewniają. Zestawienie wyników znajduje się na wykresie 6.17 i w tabeli 6.16, która jest w załączniku 6.1.

Wykres 6.17

Odsetek firm, które zapewniają zgodność funkcjonowania z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie w zależności od formy własności



W podziale firm ze względu na rodzaj prowadzonej działalności, najwięcej firm zapewniających zgodność funkcjonowania wewnętrznych dokumentów organizacyjnych z wymaganiami aktualnie obowiązujących prawnych regulacji zapewnia 34% firm usługowych. W grupie firm usługowo-produkcyjnych jest to 17%, a w grupie firm przypisanych do kategorii „inne” 16%. W firmach typu konsultingowego 1% zapewnia zgodność funkcjonowania. W wyróżnionych

grupach rodzajów prowadzonej działalności występuje niewielki odsetek firm, które nie zapewniają zgodności funkcjonowania wewnętrznych dokumentów organizacyjnych z aktualnymi regulacjami prawnymi: (1) firmy usługowe – 10%, (2) usługowo-produkcyjne – 7%, (3) produkcyjne – 4%, (4) inne – 3%, (5) konsultingowe – 1%. Zestawienie zawarto w tabeli 6.17.

Tabela 6.17

Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | | Suma |
|---------------------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Usługowa | 31 | 34% | 9 | 10% | 40 |
| Produkcyjna | 6 | 7% | 4 | 4% | 10 |
| Usługowo-produkcyjna | 16 | 17% | 6 | 7% | 22 |
| Konsultingowa | 1 | 1% | 1 | 1% | 2 |
| Inna | 15 | 16% | 3 | 3% | 18 |
| Razem | 69 | 75% | 23 | 25% | 92 |

Tabela 6.18

Rozkład odpowiedzi w zależności od formy finansowania działalności

| Kryterium wyróżnienia: sposób finansowania działalności | N = 92 | | | |
|---|--------|-----|-----|-----|
| | TAK | % | NIE | % |
| Krajowa | 63 | 68% | 23 | 25% |
| Z kapitałem obcym | 6 | 7% | 0 | 0% |
| Razem | 69 | 75% | 23 | 25% |

Zgodność funkcjonowania wewnętrznych dokumentów z aktualnymi wymaganiami prawnymi jest zapewniona w 68% firm z kapitałem krajowym i w 7% firm z kapitałem obcym. ¼ firm z kapitałem krajowym podaje, że zgodności dokumentacyjnej nie zapewnia (tabela 6.18).

Pytanie 3

Czy identyfikowana i analizowana jest struktura kosztów (strat) zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego?

W ogólnej liczbie odpowiedzi na pytanie o potwierdzenie działań obejmujących identyfikację oraz analizę struktury kosztów zabezpieczeń przed skutkami zagrożeń oraz ich bilansowanie w systemie zarządzania kryzysowego 53 firmy, co stanowi 58% badanych firm, wybrały odpowiedź twierdzącą.

Natomiast 39 firm (42%) nie prowadzi takich działań, nie rozpoznaje kosztów ani ich nie bilansuje (tabela 6.19).

Tabela 6.19

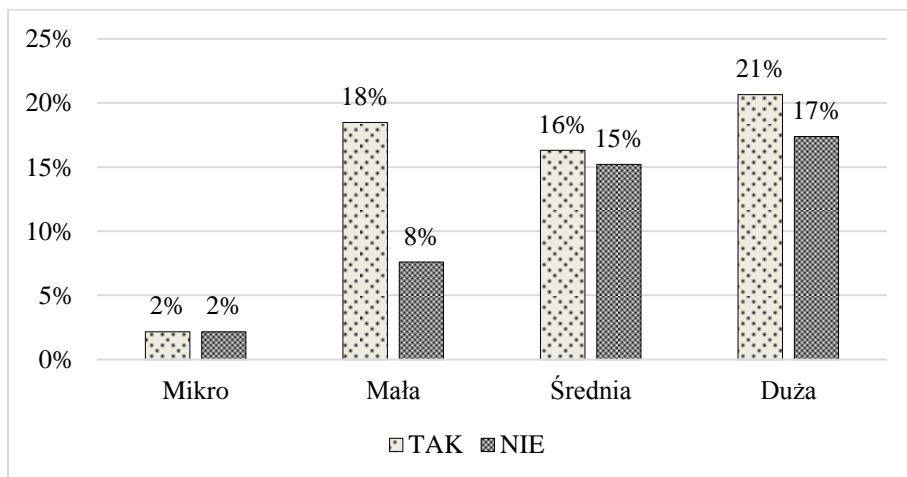
Rozkład odpowiedzi na pytanie 3

| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| Identyfikowanie i analizowanie struktury kosztów zabezpieczeń | TAK | 53 | 58% |
| | NIE | 39 | 42% |
| Razem | | 92 | 100,00% |

W zależności od wielkości firmy, analiza struktury kosztów jest prowadzona w 21% w dużych firmach, w 18% w małych, w 16% średniej wielkości, oraz w 2% w firmach mikro. Zwraca uwagę wysoki odsetek firm, które nie prowadzą analizy struktury kosztów zabezpieczeń. W grupie firm dużych jest to 17%, w grupie firm małych 18%, w średniej wielkości 15% i firmach typu mikro 2%. Zestawienie obrazuje wykres 6.18 i tabela 6.20, która jest w załącznikach 6.1.

Wykres 6.18

Odsetek firm, w których dokonuje się analizy kosztów zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego ze względu na wielkość firmy

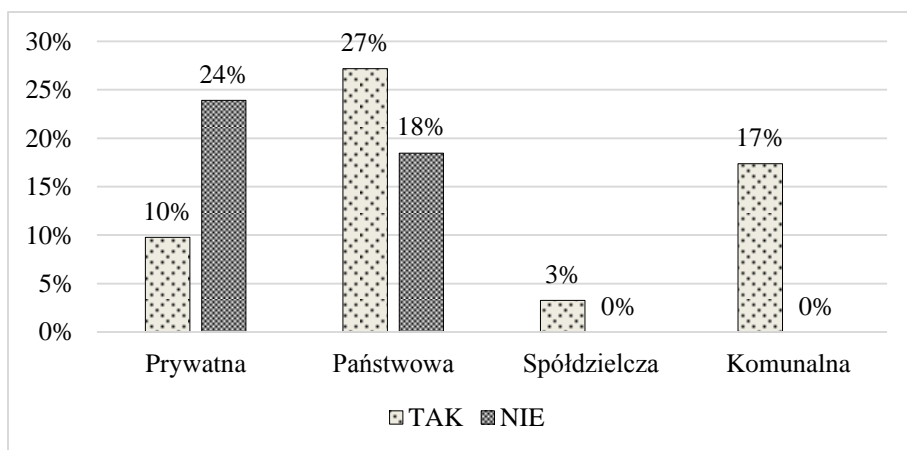


Odsetek firm, które prowadzą identyfikację oraz analizę kosztów zabezpieczenia przed skutkami zagrożeń ze względu na formę własności przedstawia się następująco: 27% firm państwowych, 17% firm komunalnych,

10% firm prywatnych, 3% firm spółdzielczych. Analiza struktury kosztów w firmach spółdzielczych i municypalnych jest prowadzona w 100% badanych firm. Zwraca uwagę duży odsetek firm państwowych (18%) i prywatnych (24%), w których nie prowadzi się analizy. Odsetek firm prywatnych, w których nie prowadzi się analizy kosztów jest o 14% większy od odsetka firm prowadzących takie analizy. Zestawienie obrazuje wykres 6.19.

Wykres 6.19

Odsetek firm, w których dokonuje się analizy kosztów zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego w kontekście formy własności



Badania rozkładu zmiennych wykazały, że analizy struktury kosztów według kryterium rodzaju działalności dokonuje 29% firm usługowych, 12% usługowo-produkcyjnych, 4% produkcyjnych. W firmach konsultingowych badanej grupy podmiotów nie dokonuje się analizy kosztów zabezpieczeń.

Takie analizy są również dokonywane wśród firm logistycznych zakwalifikowanych do grupy „innych”, których rodzaj działalności nie został przyporządkowany do żadnej z wyróżnionych kategorii i wynosi 12% badanej próby. Zwraca uwagę duży odsetek firm, które nie prowadzą analiz kosztów. W grupie firm usługowych jest to 14% i 12% w grupie firm produkcyjno-usługowych. Firmy z grupy produkcyjnych w 7% ogółu badanych firm nie dokonują analiz, również w grupie firm „innych” 8% nie prowadzi analiz i podobnie w 2% firm konsultingowych (tabela 6.21).

Ze względu na rodzaj finansowania działalności, firmy z kapitałem krajowym w 51% podmiotów analizują koszty zabezpieczeń przed skutkami zagrożeń wobec 42% firm, które tego nie wykonują. W grupie firm z kapitałem obcym 7% firm stosuje analizę.

Tabela 6.21

Liczebność obserwowana dla danej grupy oraz rozkład procentowy odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | |
|---------------------------------|--------|-----|-----|-----|
| | TAK | % | NIE | % |
| Usługowa | 27 | 29% | 13 | 14% |
| Produkcyjna | 4 | 4% | 6 | 7% |
| Usługowo-produkcyjna | 11 | 12% | 11 | 12% |
| Konsultingowa | 0 | 0% | 2 | 2% |
| Inna | 11 | 12% | 7 | 8% |
| Razem | 53 | 58% | 39 | 42% |

Pytanie 4

Czy znane (przedsiębiorstwom) są narzędzia wspomagające zarządzanie kryzysowe:

- w planowaniu (projektowaniu) systemów logistycznych?
- w realizacji (we wdrożeniu) systemów logistycznych?

O powodzeniu wdrożeń z zakresu zabezpieczeń przed skutkami realizacji zagrożeń decyduje znajomość narzędzi wspomagających zarządzanie kryzysowe, które powinny obejmować etap planowania (projektowania) systemów logistycznych, jak i fazę realizacji, czyli wdrażania systemów. W badanej próbie odsetek odpowiedzi dotyczących znajomości narzędzi wspomagających zarządzanie kryzysowe obejmujący etap planowania i etap realizacji jest zbliżony i wynosi dla 65% firm (60 podmiotów) w planowaniu, dla 64% (59 podmiotów) w realizacji, w których są znane i stosowane narzędzia wspomagania zarządzania kryzysowego. Zestawienie jest zawarte w tabeli 6.22 i na wykresie 6.20, który jest w załączniku 6.1.

Tabela 6.22

Częstość i odsetek odpowiedzi dla pytania 4

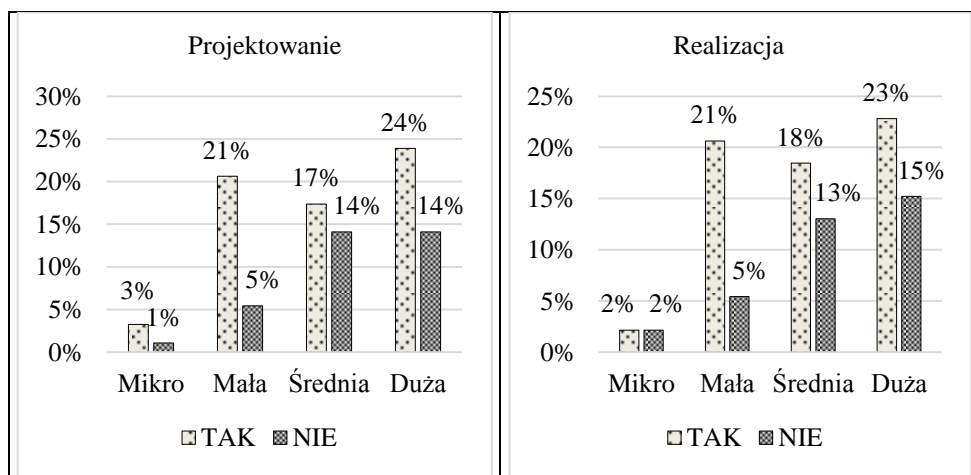
| | | W planowaniu (projektowaniu) systemów logistycznych | | W realizacji (we wdrożeniu) systemów logistycznych | |
|------|----|--|------|--|------|
| | | n | % | n | % |
| | | Znajomość narzędzi wspomagających zarządzanie kryzysowe | TAK | 60 | 65% |
| NIE | 32 | | 35% | 33 | 36% |
| Suma | | 92 | 100% | 92 | 100% |

Zwraca jednak uwagę spora grupa podmiotów, które nie znają narzędzi wspomagających:

- 35% (32 podmioty) w planowaniu,
- 36% (33 podmioty) w realizacji.

Wykres 6.21

Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania oraz etapu realizacji systemów logistycznych w zależności od wielkości firm



W zależności od wielkości firmy, największa znajomość narzędzi wspomagających zarządzanie kryzysowe na etapie projektowania jest w firmach dużych (22 podmioty), co stanowi 24% próby badawczej, 19 w firmach małych (21%), 16 firmach średniej wielkości (17%) i 3 firmach mikro, co stanowi 3% badanych podmiotów. Brak znajomości narzędzi dla fazy planowania wykazało po 14% firm dużych i średniej wielkości i 5% firm małych oraz 1% firm typu mikro (wykres 6.21). W przypadku znajomości narzędzi wspomagających zarządzanie kryzysowe w fazie realizacji systemów logistycznych rozkład odpowiedzi w zależności od wielkości firmy przedstawia się następująco: 23% firm dużych, 23% firm małych, 18% firm średniej wielkości i 2% firm mikro (wykres 6.21). Zwraca uwagę duży odsetek firm podających brak znajomości narzędzi w grupie firm dużych (15%) i średnich (13%) oraz mały odsetek (5%) w grupie firm małych.

Analiza znajomości narzędzi wspomagających zarządzanie kryzysowe dla fazy projektowania systemów logistycznych w zależności od formy własności wykazała, że największa znajomość narzędzi wspomagających zarządzanie

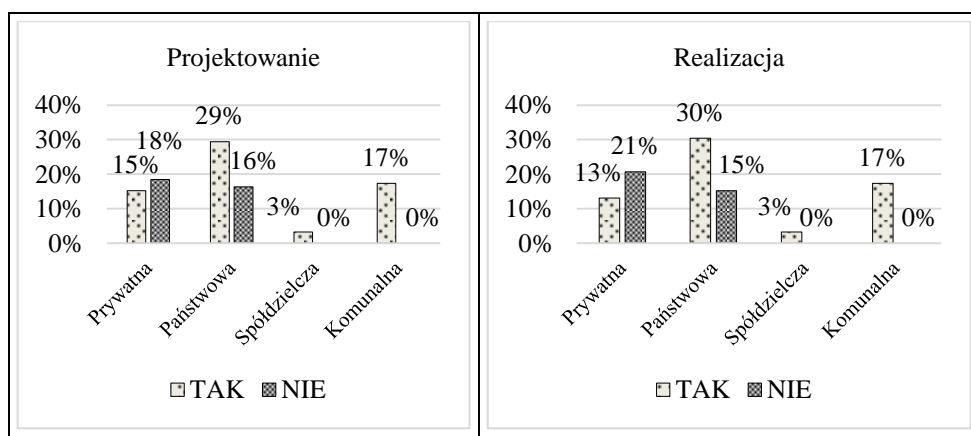
kryzysowe dla etapu projektowania systemów logistycznych dotyczy firm państwowych (29%), komunalnych (17%), prywatnych (15%) i spółdzielczych (3%). Jednak również w tym segmencie firm, w niektórych przypadkach, występuje brak znajomości narzędzi – wśród 16% firm państwowych i 15% prywatnych. Zwraca uwagę fakt, że w badanej próbie w firmach spółdzielczych i komunalnych 100% podmiotów zna narzędzia dla etapu projektowania systemów logistycznych (wykres 6.22).

W zależności od formy własności największa znajomość narzędzi dla fazy realizacji dotyczy firm państwowych (30%), komunalnych (17%), prywatnych (13%), i spółdzielczych (3%). Również w tym segmencie firm, w niektórych przypadkach, występuje brak znajomości narzędzi wśród 15% firm państwowych i 21% prywatnych. Zwraca uwagę fakt, że w badanej próbie w firmach spółdzielczych i komunalnych 100% podmiotów zna narzędzia dla etapu realizacji systemów logistycznych (wykres 6.22).

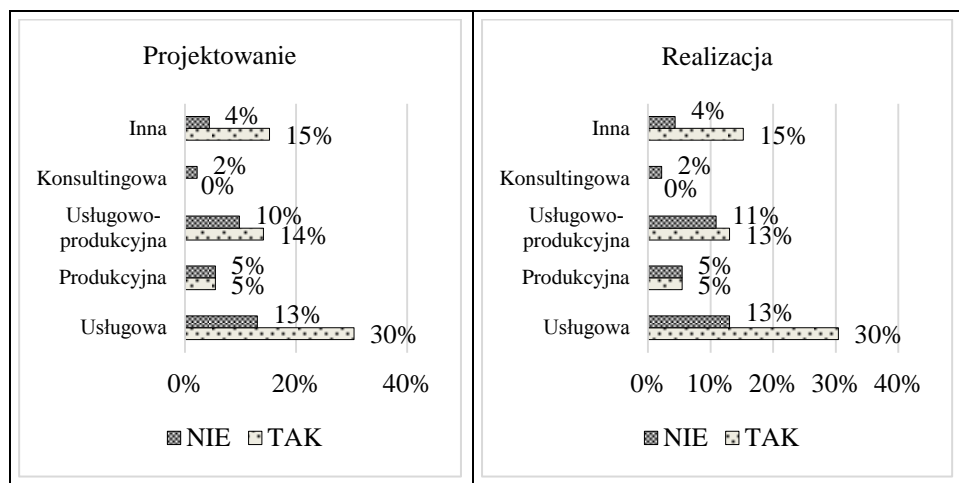
Znajomość narzędzi dla etapu projektowania systemów logistycznych największa jest w firmach typu usługowego: 30% firm posiada wiedzę z tego zakresu, 15% firm jest zakwalifikowanych jako „inne” oraz 14% – firmy z grupy usługowo-produkcyjnych, 5% – firmy produkcyjne i 2% – firmy konsultingowe. W wyróżnionych grupach rodzajów prowadzonej działalności brak znajomości narzędzi podaje: 13% firm usługowych, 10% firm usługowo-produkcyjnych, 5% produkcyjnych, 4% z grupy „inne” i 2% konsultingowe (wykres 6.23).

Wykres 6.22

Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania oraz fazy realizacji systemów logistycznych w zależności od formy własności



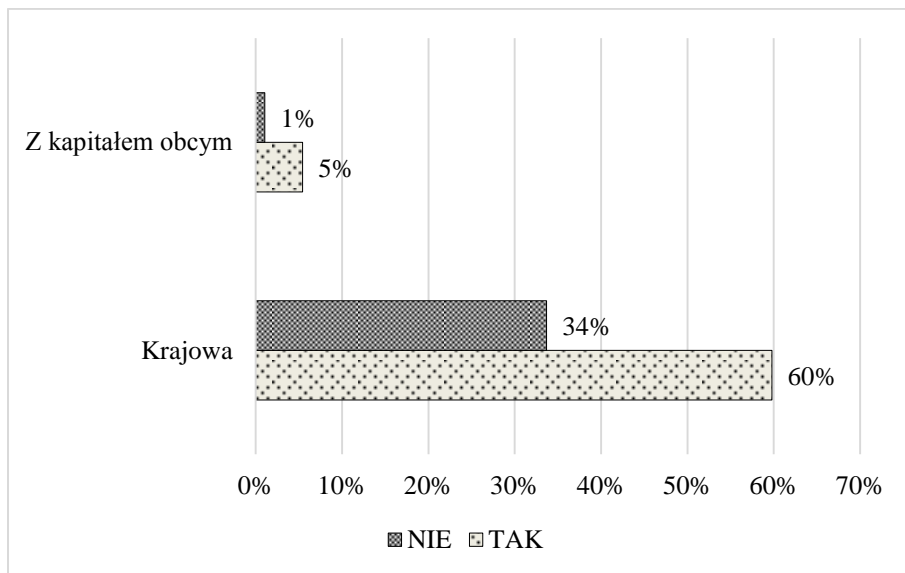
Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania systemów logistycznych oraz etapu realizacji w zależności od rodzaju prowadzonej działalności



Znajomość narzędzi dla etapu realizacji systemów logistycznych największa jest w firmach typu usługowego: 30% firm posiada wiedzę z tego zakresu, 15% firm jest zakwalifikowanych jako „inne” oraz 13% – firmy z grupy usługowo-produkcyjnych i 5% – firmy produkcyjne. W wyróżnionych grupach rodzajów prowadzonej działalności brak znajomości narzędzi podaje: 13% firm usługowych, 11% firm usługowo-produkcyjnych, 5% produkcyjnych, 4% z grupy „inne” i 2% firmy konsultingowe (wykres 6.23).

Korelacja zależności od rodzaju finansowania działalności wskazuje, że 60% firm z kapitałem krajowym i 5% firm z kapitałem obcym zna narzędzia wspomagające zarządzanie kryzysowe w projektowaniu systemów logistycznych. Jednakże 34% firm z kapitałem krajowym i 1% firm z kapitałem obcym nie zna narzędzi. Nieznajomością narzędzi wykazuje się 34% firm z kapitałem krajowym i 1% z kapitałem obcym (wykres 6.24).

Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania systemów logistycznych w zależności od rodzaju finansowania działalności



Pytanie 5

Czy strategia rozwoju Firmy/Instytucji ujmie działania zapewniające bezpieczeństwo planowanych i realizowanych procesów logistycznych?

Badania potwierdzają opinię, że wiele firm w swoich w strategiach ujmie działania, które są gwarantem planowanych i realizowanych procesów logistycznych. Sytuacja ta wynika z presji, jaką wywierają inne podmioty na firmy współpracujące, które legitymując się takim podejściem są traktowane, jako rzetelne i poważne gwarantujące wysoką jakość, bezpieczeństwo, i odpowiedzialność prowadzonej działalności. 76% firm badanej grupy deklaruje posiadanie w strategii zapisu działań, które zapewniają bezpieczeństwo planowanych i realizowanych procesów logistycznych, przy czym spory odsetek (24% badanych podmiotów) ich nie ujmie (tabela 6.23).

Tabela 6.23

Rozkład odpowiedzi dla pytania nr 5

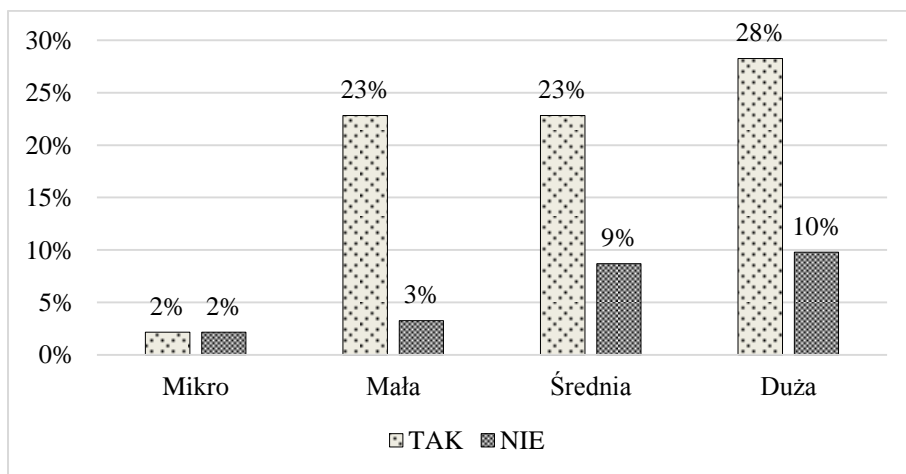
| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| Ujęcie działań zapewniających bezpieczeństwo procesów logistycznych w strategii | TAK | 70 | 76% |
| | NIE | 22 | 24% |
| Razem | | 92 | 100,00% |

Z pogłębionych wywiadów (eksperti dużych firm produkcyjno-usługowych) wynika, że w strategii dla obszaru zabezpieczenia przed skutkami zagrożeń ujmuje się między innymi:

- sposób ochrony marki i reputacji firmy;
- sposób identyfikacji, zarządzania, monitorowania bieżącymi i przyszłymi zagrożeniami mającymi wpływ na funkcjonowanie firmy;
- działania na wypadek nieplanowych zdarzeń (zagrożeń), które paraliżują realizację celów firmy;
- sposoby minimalizowania wpływu incydentów;
- działania minimalizujące czasy przestoju podczas incydentów i skracanie powrotu do stanu pierwotnego;
- sposoby doskonalenia działań, planów, procedur na wypadek sytuacji awaryjnych;
- możliwość szybkiej lokalizacji produktu na rynku i w łańcuchu dostaw w celu zagwarantowania natychmiastowego ich wycofania, w przypadku gdy zagrażają bezpieczeństwu życia i zdrowiu.

Wykres 6.25

Odsetek odpowiedzi na pytanie o ujmowanie działań zapewniających bezpieczeństwo planowanych i realizowanych procesów logistycznych w strategii firmy w zależności od wielkości firmy



Pogłębiona analiza odpowiedzi poszukująca zależności pomiędzy umieszczeniem działań z zakresu zapewniania bezpieczeństwa planowanych i realizowanych procesów logistycznych w strategiach od kryterium wielkości firm, pozwala stwierdzić, że to w 28% dużych firm (26 podmiotów) uzyskano odpowiedzi twierdzące o stosowaniu takich zapisów w strategii. W 23% w firmach średnich i małych (po 21 podmiotów) zadeklarowano twierdzące

odpowiedzi, podobnie jest w 2% firm mikro (2 podmioty) – odpowiedzi twierdzące. Firmy w zależności od wielkości, które nie zapisały w strategii działań zapewniających bezpieczeństwo procesów logistycznych to: 9 podmiotów firm dużych (10%), 8 podmiotów firm średniej wielkości (9%), 3 firmy małe (3%), 2 podmioty mikro (2%). Zestawienie obrazuje wykres 6.25.

Tabela 6.24

Rozkład odpowiedzi w zależności od formy własności firmy

| Forma własności firmy | N = 92 | | | | Suma |
|-----------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Prywatna | 17 | 18% | 14 | 15% | 31 |
| Państwowa | 34 | 37% | 8 | 9% | 42 |
| Spółdzielcza | 3 | 3% | 0 | 0% | 3 |
| Komunalna | 16 | 17% | 0 | 0% | 16 |
| Razem | 70 | 76% | 22 | 24% | 92 |

Najczęściej działania z zakresu zapewniania bezpieczeństwa (planowanych i realizowanych procesów logistycznych) są ujmowane w strategiach firm państwowych – 34 podmioty, co stanowi 37% twierdzących odpowiedzi, prywatnych – 17 podmiotów (18%), komunalnych – 16 podmiotów (17%), i spółdzielczych – 3 podmioty (3%). Przy tym zagadnień tych nie ujmuje 15% podmiotów prywatnych i 9% podmiotów państwowych. Zestawienie jest zawarte w tabeli 6.24. W badanej próbie wśród firm spółdzielczych i komunalnych nie zaobserwowano podmiotów, które nie ujmują działań zapewniających bezpieczeństwo logistyki w strategii.

Ujmowanie procesów zapewniających bezpieczeństwo logistyki w strategii najpowszechniejsze jest w firmach usługowych 33 podmioty (36%), kolejnym podmiotem są firmy usługowo-produkcyjne 14 podmiotów (15%), produkcyjne 7 podmiotów (8%). Liczną grupę, która ujmuje problemy bezpieczeństwa w strategii, stanowią podmioty zgrupowane w kategorii „inne”, które nie zostały dostatecznie rozpoznane i nie przydzielono ich do wyróżnionych kategorii. W grupie tej 16 podmiotów, co stanowi 17%, udzieliło odpowiedzi twierdzących. Wśród firm w ujęciu rodzaju prowadzonej działalności, które nie ujmują problemów bezpieczeństwa w strategii znajduje się 8 firm usługowo-produkcyjnych, co stanowi 9% odpowiedzi i 7 firm usługowych, co stanowi 8% odpowiedzi, 3 firmy produkcyjne (3%), 2 firmy konsultingowe (2%) i 2 firmy „inne”, co również stanowi 2% udzielonych odpowiedzi przeczących. Zestawienie obrazuje tabela 6.25.

Tabela 6.25

Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | | Suma |
|---------------------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Usługowa | 33 | 36% | 7 | 8% | 40 |
| Produkcyjna | 7 | 8% | 3 | 3% | 10 |
| Usługowo-produkcyjna | 14 | 15% | 8 | 9% | 22 |
| Konsultingowa | 0 | 0% | 2 | 2% | 2 |
| Inna | 16 | 17% | 2 | 2% | 18 |
| Razem | 70 | 76% | 22 | 24% | 92 |

Ze względu na sposób finansowania działalności ujmowanie procesów zapewniających bezpieczeństwo logistyki w strategii najczęściej ma miejsce w firmach z kapitałem krajowym – 65 podmiotów, co stanowi 71% odpowiedzi, przy tym 21 podmiotów z kapitałem krajowym (23% udzielonych odpowiedzi) nie zapewnia ujęcia problemów logistyki w strategii. Firmy z kapitałem obcym w badanej próbie stanowią 5 podmiotów (5%) firm, które ujmują problemy bezpieczeństwa logistyki i tylko 1 firma (1%) nie ujmuje (tabela 6.26).

Tabela 6.26

Rozkład odpowiedzi w zależności od sposobu finansowania działalności

| Kryterium wyróżnienia: sposób finansowania działalności | N = 92 | | | |
|---|--------|-----|-----|-----|
| | TAK | % | NIE | % |
| Krajowa | 65 | 71% | 21 | 23% |
| Z kapitałem obcym | 5 | 5% | 1 | 1% |
| Razem | 70 | 76% | 22 | 24% |

Pytanie 6

Czy są opracowane procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji?

Skuteczne zwiększanie bezpieczeństwa firm logistycznych powoduje, że coraz więcej firm, oprócz prowadzenia analiz ryzyka zagrożeń, podejmuje decyzje o wdrażaniu procedur utraty ciągłości działania. Korzyści, jakie wynikają z podjęcia opracowania procedur to między innymi:

- redukcja do minimum wystąpienia zakłóceń, zdarzeń niepożądanych w firmie czy instytucji, dzięki procedurom skutecznej reakcji na sytuacje kryzysowe;
- zapewnienie możliwości odtworzenia zdolności firmy czy instytucji do nieprzerwanego działania lub podjęcia ponownego działania w określonym czasie i przy ustalonym poziomie w sytuacjach kryzysowych;

- podniesienie wiarygodności firmy w kontaktach z klientami, kontrahentami, w oczach inwestorów i udziałowców;
- podniesienie przewagi konkurencyjnej dzięki zapewnieniu ciągłości działania niezależnie od niekorzystnych sytuacji.

Koncepcja zapewniania ciągłości działania podmiotu stanowi kompromis pomiędzy poziomem zabezpieczenia przed zdarzeniami niepożądanymi (sytuacjami kryzysowymi) i kosztami tego zabezpieczenia. Chodzi o identyfikację potencjalnych (możliwych i prawdopodobnych) zagrożeń i prawdopodobieństwa ich wystąpienia. Konsekwencje oszacowuje się uwzględniając czas zawieszenia realizacji procesów produkcyjnych lub usługowych. Szczególną rolę poświęca się zasobom, których dostępność musi być zapewniona w sytuacji kryzysowej, jest warunkiem koniecznym dla utrzymania ciągłości działania lub podjęcia procesów głównych (kluczowych) w jak najkrótszym czasie od wstrzymania.

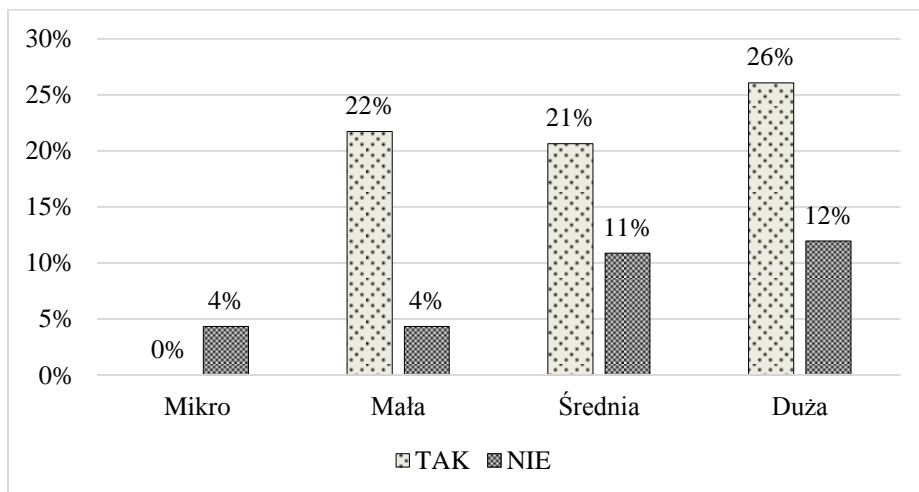
Tabela 6.27

Rozkład odpowiedzi dla pytania nr 6

| | | N = 92 | |
|--|-----|--------|---------|
| | | n | % |
| Opracowanie procedur zarządzania ryzykiem utraty ciągłości działania w firmie/instytucji | TAK | 63 | 68% |
| | NIE | 29 | 32% |
| Razem | | 92 | 100,00% |

Wykres 6.26

Odsetek odpowiedzi na pytanie: czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji w zależności od wielkości firmy?



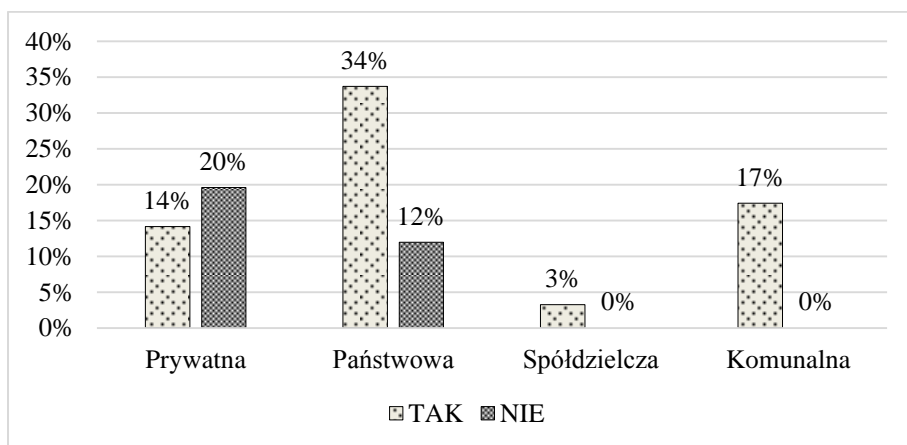
Opracowane procedury zarządzania ryzykiem utraty ciągłości działania funkcjonują w 63 podmiotach, co stanowi 68% badanej grupy. W 29 firmach, tj. 32%, nie wdrożono procedur ciągłości działania (tabela 6.27).

W analizach badających rozkład zmiennych w tabeli krzyżowej, w zależności od wielkości firmy, należy stwierdzić, że najczęściej wdrożeń jest w firmach dużych – 24 podmioty, co stanowi 26% odpowiedzi i odpowiednio w firmach małych – 20 podmiotów, co stanowi 22%, w firmach średnich – 19, co stanowi 21% odpowiedzi potwierdzających wdrożenia procedur. Brak wdrożeń procedur deklarują: 11 firm dużych (12%), 10 podmiotów średniej wielkości (11%), 4 firmy małe i mikro, co stanowi po 4% odpowiedzi przeczących. Wykres 6.26 obrazuje zestawienie liczbowe.

Najliczniej procedury są wdrażane w firmach państwowych – 31 podmiotów, co stanowi 34% badanych podmiotów, wobec 11 podmiotów, co stanowi 12% firm, które, takich wdrożeń nie ma. W firmach komunalnych 16 podmiotów, tj. 17%, ma wdrożone procedury (zaznaczyć należy, że wśród tych firm nie ma podmiotów, które nie miałyby tego rozwiązania). Ponadto wdrożenia ma 13 firm prywatnych, co stanowi 14%. Zwraca uwagę duża liczba firm tego segmentu, które nie posiadają wdrożeń – jest to 18 podmiotów, które stanowią 20% badanej grupy. W badanej grupie firm spółdzielczych i komunalnych rozwiązania są stosowane we wszystkich podmiotach, nie stwierdza się firm, które nie posiadają procedur ciągłości działania. Wykres 6.27 prezentuje zestawienie wyników.

Wykres 6.27

Odsetek odpowiedzi na pytanie: czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji w zależności od formy własności?

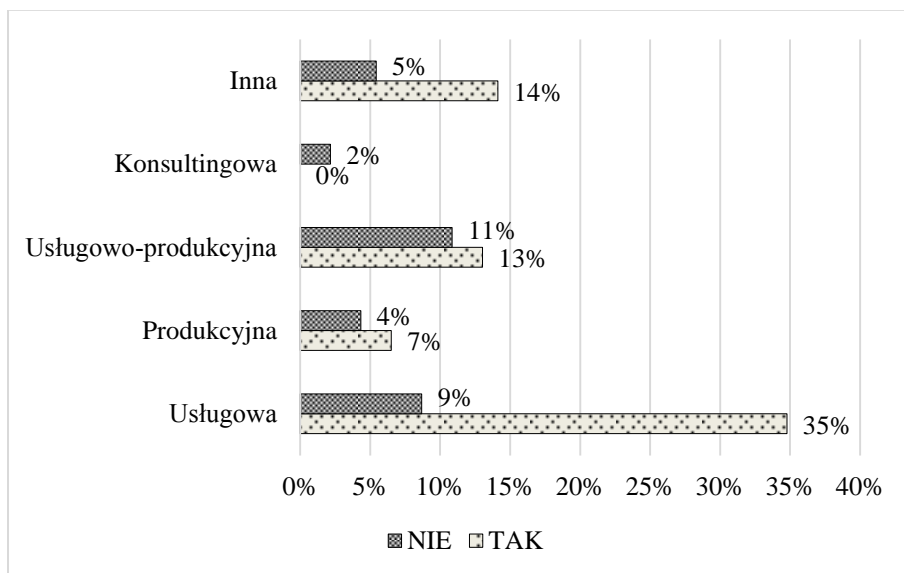


Procedury zarządzania ryzykiem utraty ciągłości działania najliczniej są stosowane w firmach prowadzących działalność usługową: na 32 podmioty, które stanowią 35% badanej grupy, tylko 8 firm, czyli 9% badanych, takich wdrożeń nie posiada. Podobne wielkości wdrożeń procedur mają firmy o charakterze usługowo-produkcyjnym i ujęte w grupie „inne”. W grupie firm usługowo-produkcyjnych 12 podmiotów, tj. 13%, ma wdrożenia, przy czym 10 firm, co stanowi 11%, takich wdrożeń nie ma. W grupie firm produkcyjnych 7% (6 podmiotów) ma wdrożenia, natomiast w 4% firm tych rozwiązań nie ma. Brakuje tych rozwiązań w firmach konsultingowych (wykres 6.28).

Wdrożenia procedur ciągłości działania, analizowane według kryterium sposobu finansowania działalności, występują w przypadku 63% firm z krajowym kapitałem i w 5% firm z kapitałem obcym. Przy tym 30% firm z kapitałem krajowym i 1% z kapitałem obcym nie posiada wdrożonych procedur ciągłości działania.

Wykres 6.28

Odsetek odpowiedzi na pytanie: czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji w zależności od rodzaju prowadzonej działalności?



Pytanie 7

W jakiej formie jest prowadzony monitoring bezpieczeństwa funkcjonowania systemu logistycznego (monitoring fizyczny, wizyjny, mierników efektywności bezpieczeństwa systemu logistycznego)? Mile widziana odpowiedź w 2-3 zdaniach.

W otwartym pytaniu poproszono biorących udział w badaniu o scharakteryzowanie działań podejmowanych w ramach obserwacji (monitoringu) kryteriów wybranych do śledzenia efektywności systemu bezpieczeństwa logistyki.

Na 92 badane podmioty w przypadku 62 firm, co stanowi 67% ogółu odpowiedzi, otrzymano krótkie charakterystyki stosowanych form monitoringu, nie otrzymano natomiast w przypadku 30 podmiotów (33% próby), (tabela 6.28).

Tabela 6.28

Rozkład odpowiedzi na pytanie nr 7

| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| W jakiej formie prowadzony jest monitoring bezpieczeństwa funkcjonowania systemu logistycznego (monitoring fizyczny, wizyjny, mierników efektywności bezpieczeństwa systemu logistycznego)? | TAK | 62 | 67% |
| | NIE | 30 | 33% |
| Razem | | 92 | 100,00% |

Najwięcej informacji na temat prowadzonego monitoringu oraz mierników efektywności bezpieczeństwa systemu logistycznego przekazało 24% firm małych (wobec 2% z brakiem informacji) i 24% firm dużych oraz 17% firm średniej wielkości. W grupie firm dużych i średnich po 14% nie przekazało informacji o posiadanych systemach monitoringu. W grupie badawczej występują 4 firmy mikro, z których dane przekazały 2 (tabela 6.29).

Tabela 6.29

Rozkład odpowiedzi w zależności od wielkości firmy

| Wielkość firmy | N = 92 | | | | Suma |
|----------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Mikro | 2 | 2% | 2 | 2% | 4 |
| Mała | 22 | 24% | 2 | 2% | 24 |
| Średnia | 16 | 17% | 13 | 14% | 29 |
| Duża | 22 | 24% | 13 | 14% | 35 |
| Razem | 62 | 67% | 30 | 33% | 92 |

Analiza rozkładu zmiennych wskazuje, że prowadzenie monitoringu najczęściej jest stosowane w firmach państwowych i wynosi 26%. Uwagę zwraca fakt, że w segmencie tym 20% nie prowadzi monitoringu pod żadną postacią.

W firmach prywatnych monitoring stosuje 21% podmiotów wobec 13%, które monitoringu nie stosują. Natomiast stosowanie monitoringu w segmencie firm spółdzielczych – 3% i komunalnych – 17%, co łącznie stanowi 100% badanej grupy. Wykres 6.29 przedstawia graficzne zestawienie wyników.

Wykres 6.29

Odsetek firm stosujących formy monitoringu w zależności od formy własności firmy

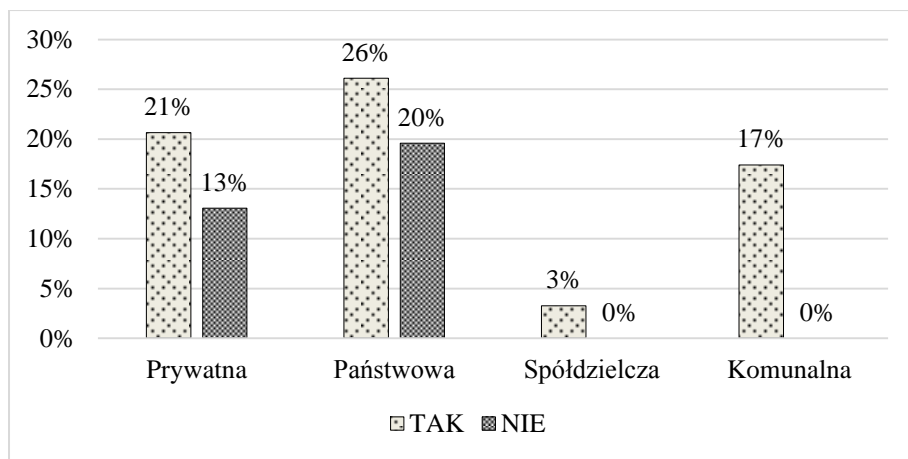


Tabela 6.30

Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | | Suma |
|---------------------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Usługowa | 30 | 33% | 10 | 11% | 40 |
| Produkcyjna | 7 | 8% | 3 | 3% | 10 |
| Usługowo-produkcyjna | 16 | 17% | 6 | 7% | 22 |
| Konsultingowa | 0 | 0% | 2 | 2% | 2 |
| Inna | 9 | 10% | 9 | 10% | 18 |
| Razem | 62 | 67% | 30 | 33% | 92 |

Monitoring systemu logistycznego najczęściej jest stosowany wśród firm prowadzących działalność usługową – jest to 33% próby badawczej. Stanowi to aż 75% firm z tego segmentu podmiotów. Kolejną grupą są firmy usługowo-produkcyjne, z których 17% stosuje monitoring bezpieczeństwa systemów logistyki wobec 7% firm, które monitoringu bezpieczeństwa nie stosują. W segmencie firm produkcyjnych 7% stosuje obserwację bezpieczeństwa

systemów logistycznych wobec 3%, które nie stosują żadnej formy monitoringu. W grupie firm zakwalifikowanych do kategorii „innych” 10% podmiotów stosuje monitoring bezpieczeństwa wobec 10% niestosujących. Można przyjąć, że w grupie tej ½ firm stosuje monitoring i ½ firm nie stosuje obserwacji funkcjonowania systemu bezpieczeństwa systemu logistycznego. W badanej grupie firm segment firm konsultingowych w 2% stosuje obserwację systemu bezpieczeństwa. W grupie tej nie stwierdza się podmiotów, które nie stosują monitoringu bezpieczeństwa systemów logistycznych. Zestawienie przedstawia tabela 6.30.

Analiza rozkładu zmiennych wykazała, że 61% firm finansowanych kapitałem krajowym stosuje monitoring bezpieczeństwa systemów logistyki, przy czym w grupie tej 33% przyznaje się do braku stosowania jakichkolwiek obserwacji bezpieczeństwa systemów logistyki. W grupie firm z kapitałem obcym 7% stosuje monitoring. W tej grupie nie stwierdza się firm niestosujących obserwacji (tabela 6.31).

Tabela 6.31

Rozkład odpowiedzi w zależności od sposobu finansowania działalności

| Sposób finansowania działalności | N = 92 | | Suma |
|----------------------------------|--------|-----|------|
| | TAK | NIE | |
| Krajowa | 56 | 30 | 86 |
| Z kapitałem obcym | 6 | 0 | 6 |
| Razem | 62 | 30 | 92 |

Pytanie 8

Czy znana jest struktura Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego?

Skuteczne zarządzanie firmą wymaga dobrej znajomości podatności na różnego rodzaju zagrożenia zarówno wewnętrzne, jak i zewnętrzne, które mogłyby zakłócić funkcjonowanie systemu logistycznego. Wśród badanych 92 firm 64 podmioty (70%) udzieliły twierdzącej odpowiedzi przyznając, że znają podatności (wrażliwość) swoich struktur na zagrożenia zarówno wewnętrzne, jak i zewnętrzne, które mogą wpływać na zakłócenia funkcjonowania systemu logistycznego. Problem pozostaje nieuregulowany dla 28 podmiotów, tj. 30% firm. Zestawienie wyników zawarto w tabeli 6.32.

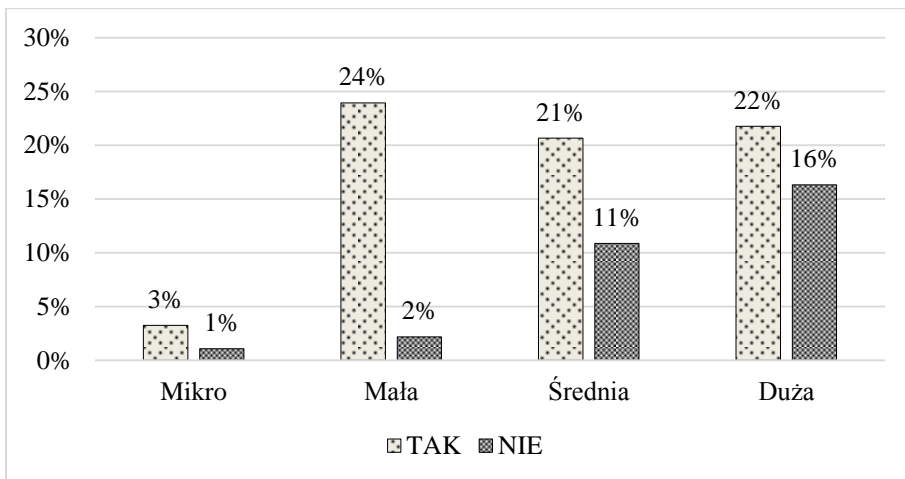
Tabela 6.32

Rozkład odpowiedzi na pytanie nr 8

| | | N = 92 | |
|--|-----|--------|---------|
| | | n | % |
| Znajomość struktury Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego | TAK | 64 | 70% |
| | NIE | 28 | 30% |
| Razem | | 92 | 100,00% |

Wykres 6.30

Odsetek odpowiedzi na pytanie o znajomość struktury Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego w zależności od wielkości firmy



Rozkład zmiennych odpowiedzi twierdzących, w zależności od podziału podmiotów, w którym jako kryterium przyjęto wielkość firmy, jest bardzo zbliżony w analizowanych firmach i jest następujący: zanana jest podatność struktur dla 22 podmiotów firm małych (24%), dla 20 podmiotów dużych firm (22%), 19 przedstawicieli firm średnich (21%). Procent firm, które nie wykazują się znajomością podatności struktur wynosi dla firm dużych 16%, średnich 11%, małych firm 2% i 1% dla firm mikro. Zwraca uwagę fakt, że wśród firm dużych, aż 75% badanej próby nie wykazuje się znajomością podatności struktur na zagrożenia. Podobną sytuację mamy w przypadku firm średniej wielkości, w której 52% badanych podmiotów nie zna podatności struktur. Taki stan rzeczy nasuwa wniosek, że w firmach tych nie prowadzi się ani analiz ryzyka, a tym bardziej w kontekście zarządzania ciągłością działania. Pozytywnie należy

wyróżnić firmy małe, w których znikomy procent podmiotów (2%) nie posiada wiedzy w obszarze podatności własnych struktur na zagrożenia. Wykres 6.30 prezentuje wyniki.

Tabela 6.33

Rozkład odpowiedzi w zależności od formy własności firmy

| Forma własności firmy | N = 92 | | | | Suma n |
|-----------------------|--------|-----|-----|-----|--------|
| | TAK | % | NIE | | |
| Prywatna | 19 | 21% | 12 | 13% | 31 |
| Państwowa | 26 | 28% | 16 | 17% | 42 |
| Spółdzielcza | 3 | 3% | 0 | 0% | 3 |
| Komunalna | 16 | 17% | 0 | 0% | 16 |
| Razem | 64 | 70% | 28 | 30% | 92 |

Tabela 6.34

Rozkład odpowiedzi w relacji do kryterium rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | | Suma |
|---------------------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Usługowa | 32 | 35% | 8 | 9% | 40 |
| Produkcyjna | 8 | 9% | 2 | 2% | 10 |
| Usługowo-produkcyjna | 14 | 15% | 8 | 9% | 22 |
| Konsultingowa | 0 | 0% | 2 | 2% | 2 |
| Inna | 10 | 11% | 8 | 9% | 18 |
| Razem | 64 | 70% | 28 | 30% | 92 |

Znajomość podatności struktur własnej firmy na zagrożenia największa jest wśród firm państwowych, w 28%, tj. w 26 podmiotach uzyskano twierdzącą odpowiedź. Zwraca uwagę stosunkowo duża liczba firm z tego segmentu, które tej wiedzy nie posiada, tj. 16 podmiotów, co stanowi 17% badanych. Znajomość podatności posiada 19 firm prywatnych (21%), przy 12 podmiotach (13%) niemających tej wiedzy. W badanej grupie podmiotów spółdzielczych i komunalnych 100 procent firm zna podatności struktur na zagrożenia (tabela 6.33).

Najlepszą znajomość podatności struktur własnych firm na zagrożenia zarówno wewnętrzne, jak i zewnętrzne deklarują firmy o profilu usługowym – 32 podmioty badanej próby (35%). Nieznajomość w tej grupie deklaruje 8 podmiotów, co stanowi 9% badanej grupy. Spośród firm usługowo-produkcyjnych znajomość podatności zgłosiło 14 podmiotów, tj. 15% próby, natomiast 8 podmiotów (9%) zgłosiło brak znajomości (tabela 6.34).

W grupie firm produkcyjnych 8 podmiotów (9%) deklaruje znajomość podatności struktur i tylko 2 firmy, co stanowi 2%, zgłosiły nieznaną podatności struktur. W grupie firm zakwalifikowanych do kategorii „inne” znajomość deklaruje 10 firm, co stanowi 11% próby badanej, a nieznaną podatności zadeklarowało 8 podmiotów, co stanowi 9% badanej grupy przedsiębiorstw. W grupie firm konsultingowych występują dwa podmioty badawcze, co stanowi 2% firm, które wykazują się nieznaną podatności własnych struktur na zagrożenia. Zestawienie obrazuje wykres 6.31 – załącznik 6.1.

Znajomość podatności struktur własnych firm na zagrożenia w 63% udzielonych odpowiedzi potwierdzają przedstawiciele firm z kapitałem krajowym, przy czym w grupie tej aż 30% nie legitymuje się znajomością podatności na zagrożenia. Firmy z kapitałem obcym w 100% wykazuje się znajomością podatności struktur.

Pytanie 9

Jaki jest stopień samodzielności (autonomiczności) zarządzania bezpieczeństwem systemu logistycznego w Firmie/Instytucji?

- a) pełna samodzielność,
- b) współzarządzanie z innymi podmiotami,
- c) zarządzanie przez podmiot zewnętrzny.

Na 92 odpowiedzi pełną samodzielność zarządzania bezpieczeństwem systemu logistycznego deklarują 34 podmioty, co stanowi 37% odpowiedzi, współzarządzanie z innymi podmiotami zgłosiły 53 firmy, co stanowi 58% badanych. Odpowiedź „c” zarządzanie przez podmiot zewnętrzny wybrało 5 firm, co stanowi 5% odpowiedzi. Zestawienie liczbowe obrazuje tabela 6.35. Najliczniej wybierane jest współzarządzanie z innymi podmiotami, najmniej zarządzanie w formie outsourcingu.

Tabela 6.35

Rozkład odpowiedzi na pytanie 9

| Stopień samodzielności zarządzania bezpieczeństwem systemu logistycznego | N = 92 | |
|--|--------|---------|
| | n | % |
| Pełna samodzielność | 34 | 37% |
| Współzarządzanie z innymi podmiotami | 53 | 58% |
| Zarządzanie przez podmiot zewnętrzny | 5 | 5% |
| Razem | 92 | 100,00% |

Pełną samodzielność zarządzania bezpieczeństwem systemu logistycznego zgłosiło 15% firm średniej wielkości (14 podmiotów próby badawczej), 13%

firm dużych (12 podmiotów), 5% firm małych (5 podmiotów) i 3% firm mikro (3 podmioty). Uwagę zwraca fakt, że w przypadku firm małych i mikro nie występuje zarządzanie przez podmiot zewnętrzny (wariant „c”). Forma zarządzania bezpieczeństwem systemu logistycznego w oparciu o zewnętrzny podmiot dotyczy tylko firm średniej wielkości (3 podmioty, które stanowią 3%) i firm dużych (2 podmioty, tj. 2% firm badanych).

Tabela 6.36

Rozkład odpowiedzi w zależności od wielkości firmy

| Wielkość firmy | N = 92 | | | | | | Suma n |
|----------------|--------|-----|----|-----|---|----|--------|
| | a | % | b | % | c | % | |
| Mikro | 3 | 3% | 1 | 1% | 0 | 0% | 4 |
| Mała | 5 | 5% | 19 | 21% | 0 | 0% | 24 |
| Średnia | 14 | 15% | 12 | 13% | 3 | 3% | 29 |
| Duża | 12 | 13% | 21 | 23% | 2 | 2% | 35 |
| Razem | 34 | 37% | 53 | 58% | 5 | 5% | 92 |

Wariant „b”, w którym zarządzanie bezpieczeństwem systemu logistycznego oparte jest o współzarządzanie z innymi podmiotami występuje we wszystkich typach firm i jest niezależne od ich wielkości. Najliczniej z wariantu tego korzystają firmy duże: 23% (21 podmiotów), 21% firmach w małych (19 podmiotów), 13% firm średniej wielkości (12 podmiotów), 1% w firmach mikro (1 podmiot grupy badawczej). Zestawienie jest przedstawione w tabeli 6.36 i na wykresie 6.32.

Wykres 6.32

Odsetek odpowiedzi wyboru wariantu zarządzania bezpieczeństwem systemu logistycznego w zależności od wielkości firmy

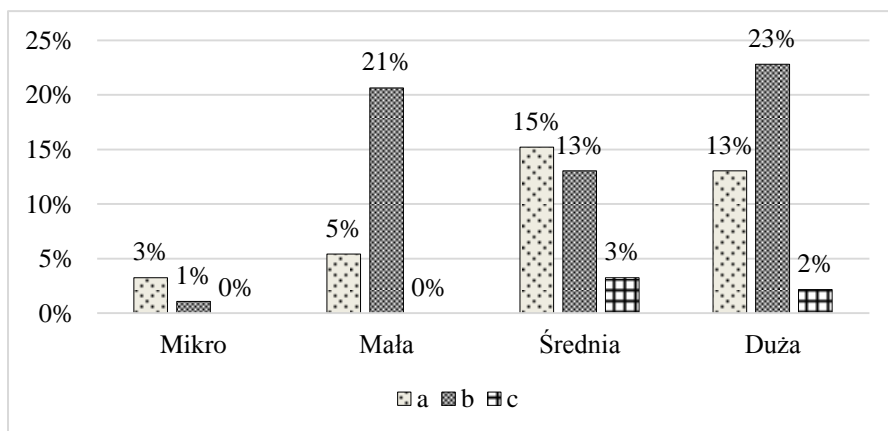


Tabela 6.37

Rozkład odpowiedzi w zależności od formy własności firmy

| Forma własności firmy | N = 92 | | | | | | Suma n |
|-----------------------|--------|-----|----|-----|---|----|--------|
| | a | % | b | % | c | % | |
| Prywatna | 20 | 22% | 9 | 10% | 2 | 2% | 31 |
| Państwowa | 12 | 13% | 27 | 29% | 3 | 3% | 42 |
| Spółdzielcza | 2 | 2% | 1 | 1% | 0 | 0% | 3 |
| Komunalna | 0 | 0% | 16 | 17% | 0 | 0% | 16 |
| Razem | 34 | 37% | 53 | 58% | 5 | 5% | 92 |

Ciekawie przedstawia się rozkład odpowiedzi analizowany z punktu formy własności firmy. Autonomia zarządzania bezpieczeństwem logistyki (wariant „a”) najczęściej jest stosowana w firmach prywatnych (20 podmiotów), co stanowi 22% badanych podmiotów. W grupie firm państwowych jest to 13% (12 podmiotów) i w 2 przypadkach firm spółdzielczych (2%). W firmach komunalnych nie występuje wariant „a” całkowitej samodzielności i wariant „c” zarządzanie zewnętrzne. W firmach typu spółdzielczego również nie występuje wariant „c”. Natomiast we wszystkich firmach bez względu na formę własności występuje wariant „b”, pośrednio oparty o współzarządzanie z innymi podmiotami. Występuje najliczniej w firmach państwowych – 29% (27 podmiotów), w 17% – w firmach komunalnych (16 podmiotów), w których jest jedyną formą zarządzania bezpieczeństwem. Wariant „c” bywa stosowany w firmach prywatnych i państwowych w niewielkim procencie. W firmach prywatnych jest to 2%, a firmach państwowych to 3%. Zestawienie prezentuje tabela 6.37.

W zależności od rodzaju działalności wariant „a” jest stosowany we wszystkich wyróżnionych rodzajach działalności firm. Najliczniej, w 13%, w firmach rodzaju usługowego (12 podmiotów), w 12% w firmach usługowo-produkcyjnych (11 podmiotów), w 7% firm produkcyjnych (6 podmiotów), w 11% firm konsultingowych (1 podmiot grupy badanej). W firmach zakwalifikowanych do kategorii „inne” 4% stosuje autonomiczność (samodzielność) w zarządzaniu bezpieczeństwem logistyki (4 podmioty grupy badanej).

Szeroko stosowany jest wariant „b”, który opiera się na współzarządzaniu bezpieczeństwem systemów logistycznych z innymi podmiotami. Dostrzega się wyraźną przewagę zastosowań tego wariantu nad innymi rozwiązaniami. Stosowany jest w 27% firm o charakterze usługowym (25 podmiotów), w 15% firm zgrupowanych w kategorii „inne” (14 podmiotów), w 10% firm usługowo-produkcyjnych (9 podmiotów) i w 1% w sektorze firm konsultingowych (1 podmiot grupy badanej).

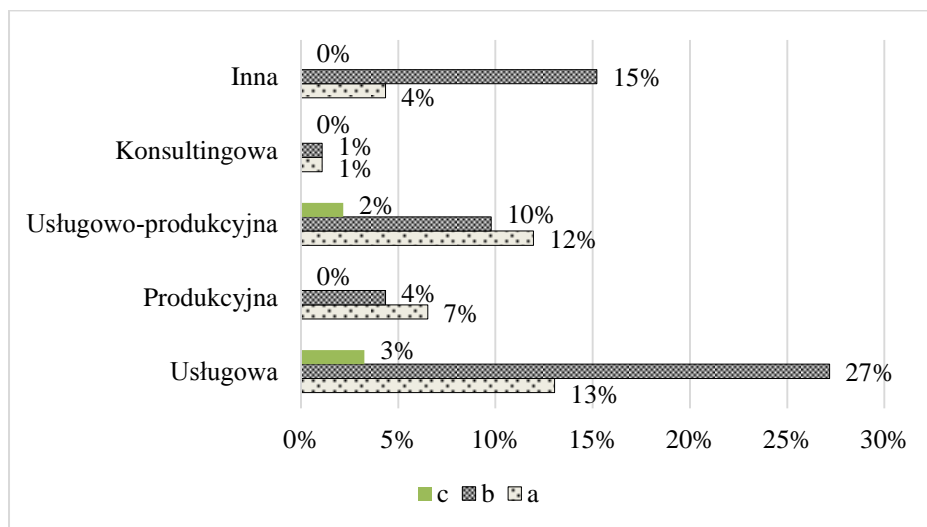
Wariant „c” zarządzania przez podmiot zewnętrzny jest stosowany w firmach usługowych reprezentowanych w badaniu przez 3 podmioty (2%)

oraz usługowo-produkcyjnych reprezentowanych przez 2 podmioty (2%). Wariant „c” nie występuje w firmach o charakterze konsultingowym i firmach przypisanych do kategorii „inna”. Jest najrzadziej wybieraną formą zarządzania bezpieczeństwem systemów logistycznych. Wariant „a” i „b” występuje w firmach zarówno z kapitałem krajowym, jak i zagranicznym. W firmach z kapitałem krajowym bywa ponadto stosowany trzeci wariant „c”, w którym zarządzanie bezpieczeństwem jest zlecane podmiotowi zewnętrznemu. Najliczniej stosowany jest wariant „b” związany ze współzarządzaniem bezpieczeństwem z innymi podmiotami. Zestawienie dla trzech wariantów „a”, „b” i „c” przedstawia wykres 6.33.

W przypadku firm z krajowym kapitałem aż 51 podmiotów (55%) firm stosuje ten wariant, a tylko 2% firm z kapitałem zagranicznym (2 podmioty). W firmach tych niestosowany jest wariant „c” polegający na outsourcingu zarządzania bezpieczeństwem systemów logistycznych.

Wykres 6.33

Odsetek odpowiedzi wyboru wariantu zarządzania bezpieczeństwem systemu logistycznego w zależności od rodzaju prowadzonej działalności



Pytanie 10

Czy w strukturze systemu zarządzania Firmą/Instytucją funkcjonuje komórka (osoba) odpowiedzialna za bezpieczeństwo funkcjonowania systemu logistycznego?

Sprawność zarządzania bezpieczeństwem systemu logistycznego zależy między innymi od wprowadzania instytucjonalnych rozwiązań w firmach, które polegają między innymi na powoływaniu komórek lub wyznaczaniu osób, którym powierza się odpowiedzialność. W praktyce sprowadza się to do tego, czy w istniejącej strukturze firmy funkcjonują komórki bądź osoby odpowie-

działne za ciągłość bezpieczeństwa (co oznacza działania z zakresu organizowania, funkcjonowania, podejmowania decyzji, monitorowania). Funkcjonowanie komórek odpowiedzialnych za bezpieczeństwo systemów wpływa na jakość systemu bezpieczeństwa, chociaż nie jest to jedynym czynnikiem jakości systemu.

W firmach i instytucjach funkcjonują takie rozwiązania. W przypadku badań aż 66 podmiotów (72%) podaje istnienie takich rozwiązań. Istnieje również dość duża grupa podmiotów, w których nie ustanowiono takiej komórki. Jest to 26 podmiotów, co stanowi 28% grupy badawczej. Tabela 6.38 przedstawia wynik badań. Oznacza to brak odpowiedzialnych za pewne procesy nadzorujące system bezpieczeństwa w tych podmiotach.

Tabela 6.38

Rozkład odpowiedzi dla pytania nr 10

| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| Czy w strukturze systemu zarządzania Firmą/Instytucją funkcjonuje komórka (osoba) odpowiedzialna za bezpieczeństwo funkcjonowania systemu logistycznego | TAK | 66 | 72% |
| | NIE | 26 | 28% |
| Razem | | 92 | 100,00% |

Analiza rozkładu zmiennych ujawnia bardzo równomierny rozkład zgłoszonego wyboru. W zależności od wielkości firmy komórka do spraw bezpieczeństwa w jej strukturach występuje: w 25% w przypadku firm dużych (w 23 podmiotach), w 24% w małych firmach (w 22 podmiotach), w 20% w firmach średniej wielkości (w 18 podmiotach) i w 3% w firmach mikro (3 podmioty w grupie badanej). Podmioty, które nie posiadają komórki lub osoby odpowiedzialnej za zarządzanie bezpieczeństwem systemów logistycznych znajdują się w grupie podmiotów firm dużych – 12 podmiotów (13%), firm średniej wielkości – 11 podmiotów (12%) oraz w firmach małych – 2 podmioty (2%) i mikro – 1 podmiot (1%). Zestawienie prezentuje tabela 6.39.

Tabela 6.39

Rozkład odpowiedzi w zależności od wielkości firmy

| Wielkość firmy | N = 92 | | | | Suma n |
|----------------|--------|-----|-----|-----|--------|
| | TAK | % | NIE | % | |
| Mikro | 3 | 3% | 1 | 1% | 4 |
| Mała | 22 | 24% | 2 | 2% | 24 |
| Średnia | 18 | 20% | 11 | 12% | 29 |
| Duża | 23 | 25% | 12 | 13% | 35 |
| Razem | 66 | 72% | 26 | 28% | 92 |

Komórki odpowiedzialne za bezpieczeństwo systemów logistycznych występują w 32% w firmach państwowych (29 podmiotów), w 21% w firmach prywatnych (19 podmiotów), w 17% w firmach komunalnych (16 podmiotów). W firmach typu spółdzielczego 2% posiada komórki do spraw bezpieczeństwa (2 podmioty próby badawczej) wobec 1% firm, które nie posiadają komórek odpowiedzialnych za bezpieczeństwo systemów logistycznych. Podkreślić należy, że firmy municypalne w 100% (w badanej próbce) mają elementy systemu zarządzania bezpieczeństwem systemu logistycznego w postaci komórek za nie odpowiedzialnych. Zestawienie prezentuje tabela 6.40 i wykres 6.34 – załącznik 6.1.

Tabela 6.40

Rozkład odpowiedzi w zależności od formy własności

| Forma własności firmy | N = 92 | | | | Suma n |
|-----------------------|--------|-----|-----|-----|--------|
| | TAK | % | NIE | % | |
| Prywatna | 19 | 21% | 12 | 13% | 31 |
| Państwowa | 29 | 32% | 13 | 14% | 42 |
| Spółdzielcza | 2 | 2% | 1 | 1% | 3 |
| Komunalna | 16 | 17% | 0 | 0% | 16 |
| Razem | 66 | 72% | 26 | 28% | 92 |

Tabela 6.41

Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | | Suma n |
|---------------------------------|--------|-----|-----|-----|--------|
| | TAK | % | NIE | % | |
| Usługowa | 31 | 34% | 9 | 10% | 40 |
| Produkcyjna | 8 | 9% | 2 | 2% | 10 |
| Usługowo-produkcyjna | 12 | 13% | 10 | 11% | 22 |
| Konsultingowa | 0 | 0% | 2 | 2% | 2 |
| Inna | 15 | 16% | 3 | 3% | 18 |
| Razem | 66 | 72% | 26 | 28% | 92 |

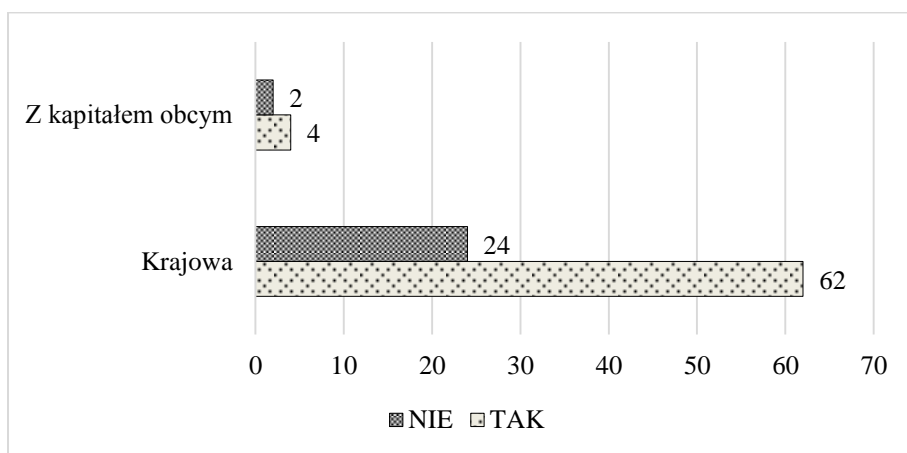
Najliczniejsza grupa firm, w których funkcjonują komórki lub osoby odpowiedzialne za bezpieczeństwo systemu logistycznego została zgłoszona przez firmy usługowe: 31 podmiotów, co stanowi 34% twierdzących odpowiedzi. W przypadku 9 podmiotów (10%) w grupie firm usługowych brakuje takiego rozwiązania. Kolejna grupa to firmy zakwalifikowane do grupy „inne”, w których 15 podmiotów (16%) posiada komórkę lub osobę odpo-

wiedzialną i tylko w 3 podmiotach (3%) brakuje takiego rozwiązania. W grupie firm usługowo-produkcyjnych posiadanie komórki odpowiedzialnej za bezpieczeństwo w strukturach firmy zgłoszono w przypadku 12 podmiotów (13%), przy czym w przypadku 10 firm, co stanowi 11%, takich rozwiązań brakuje. W grupie firm konsultingowych w badaniu nie zgłoszono istnienia takiego rozwiązania. Wynik badań jest przedstawiony w tabeli 6.41 i na wykresie 6.35 – załącznik 6.1.

W badaniu najliczniej są reprezentowane firmy z kapitałem krajowym, stąd oczywiste jest, że najwięcej rozwiązań z powołaniem komórki lub osoby odpowiedzialnej za bezpieczeństwo systemu logistycznego jest w tych firmach. Stanowią one 62% badanych firm (62 podmioty), natomiast takich rozwiązań brakuje w przypadku 24 podmiotów. Firmy z kapitałem obcym stanowią niewielki procent grupy badawczej. Model z powołaniem komórki stosuje 4% badanych firm. Wykres 6.36 przedstawia wyniki badań z tego obszaru.

Wykres 6.36

Częstość odpowiedzi o odpowiedzialność za bezpieczeństwo logistyki w zależności od rodzaju finansowania działalności



Pytanie 11

Jakie procedury zarządzania bezpieczeństwem systemu logistycznego są stosowane w firmie dla etapu:

- planowania (analizy i oceny ryzyka zagrożeń, planowania sił i środków, procedury reagowania, zachowania ciągłości działania)?
- zapobiegania mogącym powstać zagrożeniom (prewencja)?
- reagowania na występujące zakłócenia w funkcjonowaniu systemu logistycznego?
- odbudowy systemu po wystąpieniu zakłóceń częściowych lub całkowitych?

Procedury zarządzania bezpieczeństwem systemu logistycznego wpisują się w fazy zarządzania kryzysowego: zapobiegania, przygotowania, reagowania i odbudowy.

Fazy zapobiegania i przygotowania należą do obszaru profilaktyki (prewencji), przygotowują działania przed pojawianiem się zagrożeń i obejmują m.in. identyfikację i analizę potencjalnych zagrożeń (analiza ryzyka zagrożeń), ograniczanie podatności, ustalenie sił i środków reagowania oraz opracowywanie planów, procedur, instrukcji na wypadek wystąpienia sytuacji kryzysowej.

Fazy reagowania i odbudowy są inicjowane wraz z materializacją zagrożenia i obejmują ograniczanie zniszczeń, neutralizację źródeł zagrożenia, usuwanie skutków, szacowanie strat i odtwarzanie infrastruktury i zasobów.

Tabela 6.42

Rozkład odpowiedzi dla pytania nr 11

| Stosowane procedury zarządzania bezpieczeństwem systemu logistycznego dla etapu: | N = 92 | |
|---|--------|--------|
| | n | % |
| a) planowania (analizy i oceny ryzyka zagrożeń, planowania sił i środków, procedury reagowania, zachowania ciągłości działania) | TAK | 70 76% |
| | NIE | 22 24% |
| b) zapobiegania mogącym powstać zagrożeniom (prewencja) | TAK | 72 78% |
| | NIE | 20 22% |
| c) reagowania na występujące zakłócenia w funkcjonowaniu systemu logistycznego | TAK | 72 78% |
| | NIE | 20 22% |
| d) odbudowy systemu po wystąpieniu zakłóceń częściowych lub całkowitych | TAK | 60 65% |
| | NIE | 32 35% |

Procedury w badanej grupie przedsiębiorstw, w blisko 80% podmiotów dla fazy planowania, zapobiegania i reagowania są stosowane, a to oznacza, że w około ¼ podmiotów brakuje tych procedur. W przypadku etapu odbudowy wdrożonymi procedurami dysponuje 65% podmiotów wobec 35%, w których brakuje stosowania procedur. Zestawienie szczegółowe zawiera tabela 6.42.

W zależności od wielkości firmy w fazie planowania (wariant „a”) procedury zarządzania bezpieczeństwem systemu logistycznego są stosowane odpowiednio (tabela 6.43):

- w firmach dużych – 26 podmiotów (28%), przy 9 podmiotach (10%) niestosujących procedur,
- w firmach średniej wielkości – 21 podmiotów (23%), przy 8 podmiotach, które nie stosują procedur,
- w firmach małych – 20 podmiotów (22%), przy 4% (4 podmioty) niestosujących procedur,

- w firmach mikro – 3 podmioty (3%) stosujące procedury wobec 1% tych procedur niestosujących.

W fazie zapobiegania (wariant „b”) w zależności od wielkości firmy procedury zarządzania bezpieczeństwem systemu logistycznego są stosowane odpowiednio (tabela 6.43):

- w firmach dużych – 29 podmiotów (32%), przy 6 podmiotach (7%) niestosujących procedur,
- w firmach średniej wielkości – 18 podmiotów (20%), przy 11 podmiotach (12%), które nie stosują procedur,
- w firmach małych – 22 podmiotów (24%), przy 2% (2 podmioty) niestosujących procedur,
- w firmach mikro 3 podmioty (3%) stosujące procedury wobec 1% tych procedur niestosujących.

Tabela 6.43

Rozkład odpowiedzi wyboru wariantu w zależności od wielkości firmy

| Wielkość firmy | a | | | | b | | | | c | | | | d | | | |
|----------------|-----|----|-----|----|-----|----|-----|----|-----|----|-----|----|-----|----|-----|----|
| | TAK | % | NIE | % | TAK | % | NIE | % | TAK | % | NIE | % | TAK | % | NIE | % |
| Mikro | 3 | 3 | 1 | 1 | 3 | 3 | 1 | 1 | 3 | 3 | 1 | 1 | 1 | 1 | 3 | 3 |
| Mała | 20 | 22 | 4 | 4 | 22 | 24 | 2 | 2 | 22 | 24 | 2 | 2 | 20 | 22 | 4 | 4 |
| Średnia | 21 | 23 | 8 | 9 | 18 | 20 | 11 | 12 | 23 | 25 | 6 | 7 | 19 | 21 | 10 | 11 |
| Duża | 26 | 28 | 9 | 10 | 29 | 32 | 6 | 7 | 24 | 26 | 11 | 12 | 20 | 22 | 15 | 16 |
| Razem | 70 | 76 | 22 | 24 | 72 | 78 | 20 | 22 | 72 | 78 | 20 | 22 | 60 | 65 | 32 | 35 |

Zwraca uwagę stosunkowo duża liczba podmiotów z grupy firm średnich, w których nie ma zastosowań procedur zarządzania bezpieczeństwem systemów logistycznych dla fazy zapobiegania.

W zależności od wielkości firmy procedury w fazie reagowania (wariant „c”) zarządzania bezpieczeństwem systemu logistycznego są stosowane odpowiednio (tabela 6.43, wykres 6.37):

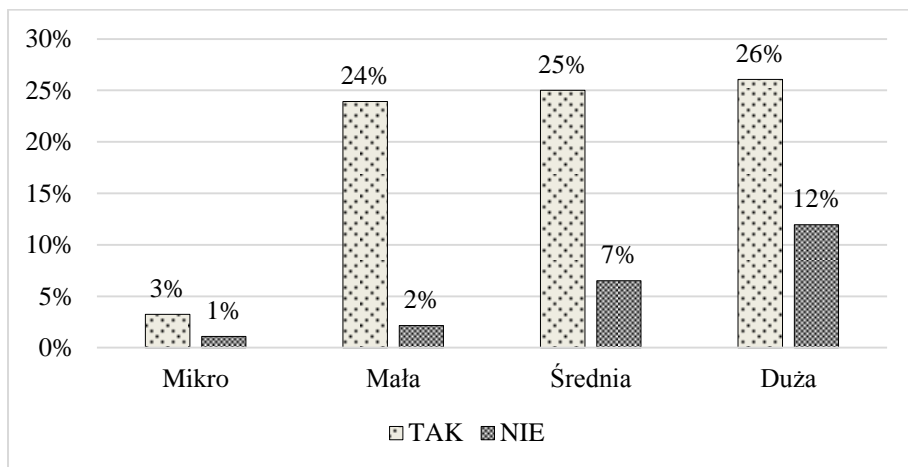
- w firmach dużych – 24 podmioty (26%), przy 11 podmiotach (12%) niestosujących procedur,
- w firmach średniej wielkości – 23 podmioty (25%), przy 6 podmiotach (7%), które nie stosują procedur,
- w firmach małych – 22 podmioty (24%), przy 2% (2 podmioty) niestosujących procedur,

- w firmach mikro – 3 podmioty (3%) stosujące procedury wobec 1% tych procedur niestosujących.

Analiza wskazuje, że występuje stosunkowo niewielki procent firm, w których nie są stosowane procedury zarządzania bezpieczeństwem systemów logistycznych dla tej fazy zarządzania kryzysowego.

Wykres 6.37

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od wielkości firmy

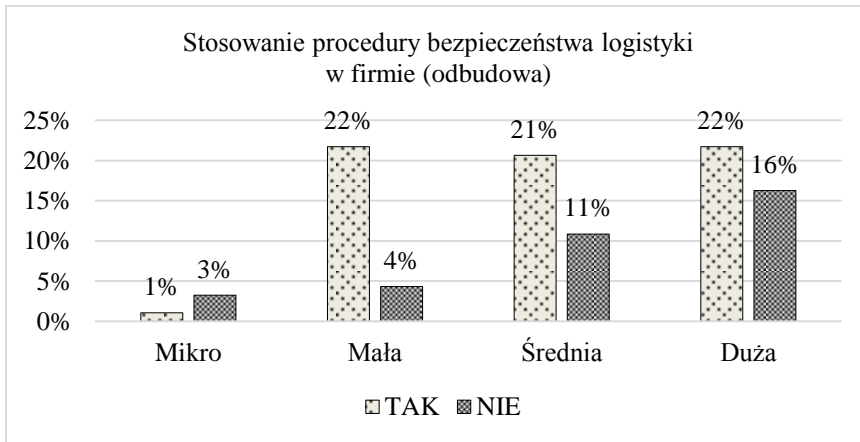


W zależności od wielkości firmy procedury w fazie odbudowy (wariant „d”) zarządzania bezpieczeństwem systemu logistycznego są stosowane odpowiednio (tabela 6.43, wykres 6.38):

- w 22% w firmach dużych (20 podmiotów) wobec 16% (15 podmiotów) firm niestosujących procedur,
- w 21% w firmach średniej wielkości (19 podmiotów), przy 11% firm (10 podmiotów), które nie stosują procedur,
- w 22% w firmach małych (20 podmiotów), przy 4% (4 podmioty) niestosujących procedur,
- w 1% w firmach mikro (1 podmiot) stosujących procedury wobec 3% tych procedur niestosujących.

Zwraca uwagę duża liczba podmiotów niestosujących procedur dla tej fazy zarządzania bezpieczeństwem systemu logistycznego, szczególnie dotyczy to firm dużych i średnich, odpowiednio 16% i 11% braku stosowania procedur (wykres 6.38).

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie odbudowy w zależności od wielkości firmy



Częściej, niż w stosunku pozostałych form własności, procedury w fazie planowania są stosowane w 39% w podmiotach państwowych (35 firm grupy badanej) wobec 7% firm z tej grupy niestosujących procedur zarządzania bezpieczeństwem systemów logistycznych. Procedury dla fazy planowania stosowane są również w 17% firm komunalnych (w 16 podmiotach). W grupie firm komunalnych nie występują firmy, w których nie ma wdrożonych procedur dla tej fazy zarządzania bezpieczeństwem.

Podobnie jest w firmach spółdzielczych. Wdrożone procedury bezpieczeństwa dla fazy planowania występują w 3% podmiotów (w 3 podmiotach grupy badawczej) i nie stwierdza się podmiotów, w których brakuje wdrożonych procedur. 71% firm prywatnych ma wdrożone procedury zarządzania bezpieczeństwem systemu logistycznego dla wszystkich faz zarządzania kryzysowego. W grupie tej tylko 19% podmiotów nie posiada wdrożonych procedur. Firmy państwowe w 100% mają wdrożone procedury dla wszystkich faz zarządzania kryzysowego. Podobna sytuacja jest w przypadku firm spółdzielczych i komunalnych w badanej grupie badawczej.

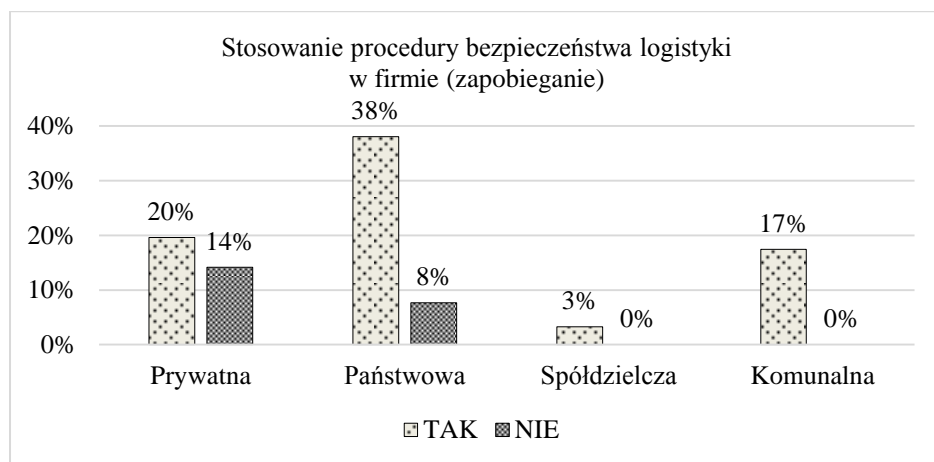
Bardzo zbliżone są rozkłady odpowiedzi otrzymanych od respondentów dla fazy przygotowania i zapobiegania w zakresie stosowania procedur zarządzania bezpieczeństwem systemów logistycznych.

Częściej, niż w stosunku do pozostałych form własności, procedury są stosowane w 38% firm państwowych (35 podmiotów w badanej próbie) wobec 8% firm, które nie stosują procedur (7 podmiotów).

Procedury bezpieczeństwa systemów logistycznych dla fazy zapobiegania zarządzania kryzysowego, stosowane są również w firmach komunalnych w 17% (16 podmiotów). W tej grupie firm brak jest podmiotów, które nie posiadają wdrożeń. Podobnie w firmach spółdzielczych – 3% tej grupy ma wdrożone procedury bezpieczeństwa (w 3 podmiotach badanej grupy) i w tej grupie firm nie stwierdza się firm, w których nie ma wdrożeń. W firmach prywatnych procedury bezpieczeństwa dla fazy zapobiegania są stosowane w 20% firm (18 podmiotów). 14% firm tego segmentu nie posiada procedur bezpieczeństwa systemów logistycznych (13 podmiotów) dla fazy zapobiegania (wykres 6.39).

Wykres 6.39

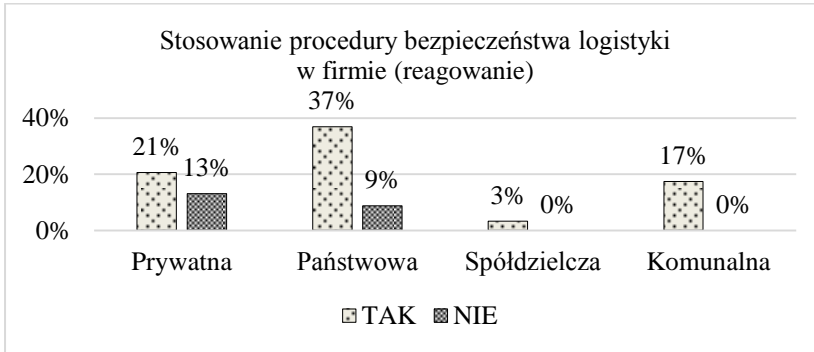
Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie zapobiegania w zależności od formy własności



Dla fazy reagowania procedury bezpieczeństwa są stosowane we wszystkich podmiotach sklasyfikowanych w rodzajach własności firm. Najczęściej procedury są stosowane w podmiotach państwowych (37%) wobec 9% firm niestosujących procedur bezpieczeństwa w tej fazie zarządzania kryzysowego. Drugą grupą są firmy prywatne, w której 21% (19 podmiotów) stosuje procedury wobec 13% (12 podmiotów), w których one nie są stosowane. Procedury stosowane są również w firmach komunalnych w 16 podmiotach (17%), wśród których nie ma firm bez wdrożeń. Podobnie w firmach spółdzielczych – procedury są wdrożone w 3% podmiotów. W tej grupie firm nie stwierdza się podmiotów, w których nie ma wdrożeń (wykres 6.40).

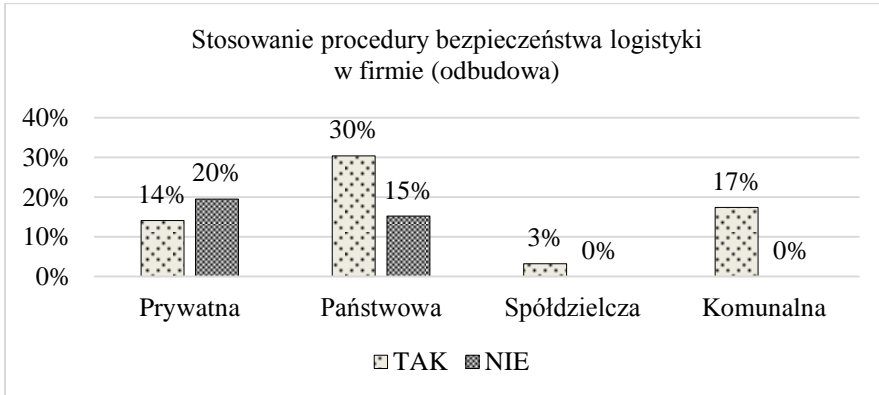
Wykres 6.40

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od formy własności firmy



Wykres 6.41

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie odbudowy w zależności od formy własności firmy



Podobnie jak dla poprzednich faz zarządzania kryzysowego, procedury zarządzania bezpieczeństwem systemu logistycznego dla fazy odbudowy są stosowane w firmach reprezentujących wszystkie formy własności. Najczęściej są stosowane w firmach państwowych: 28 podmiotów (30%) wobec 14 podmiotów (15%) niestosujących procedur. W firmach komunalnych 16 podmiotów, co stanowi 17%, firmach prywatnych 13 podmiotów (14%) wobec 18 podmiotów (20%), które nie stosują procedur. W 3 podmiotach reprezentujących firmy spółdzielcze również stosowane są procedury. Wśród

firm spółdzielczych i komunalnych nie stwierdza się podmiotów, w których nie są stosowane procedury bezpieczeństwa (wykres 6.41).

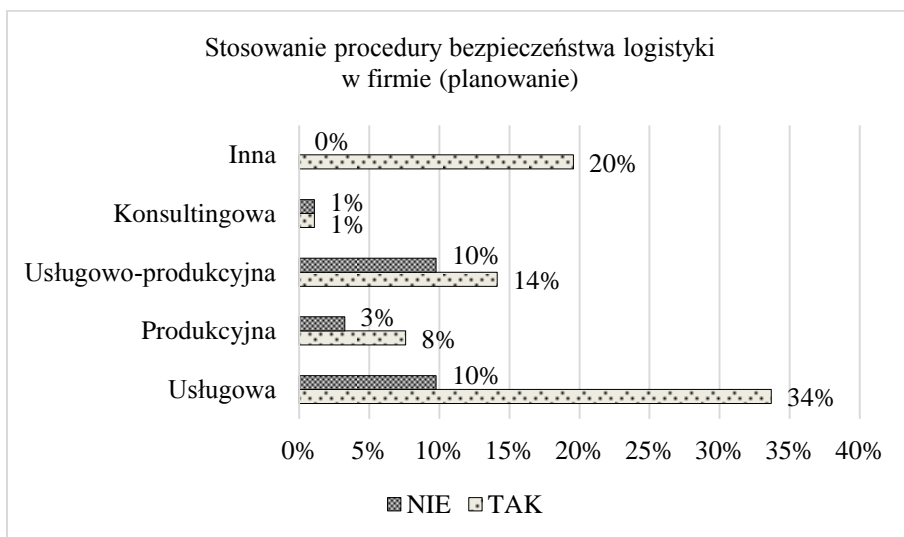
Tabela 6.44

Częstość rozkładu odpowiedzi w zależności od rodzaju prowadzonej działalności w fazie planowania

| Rodzaj prowadzonej działalności | Wariant odpowiedzi | | | | | | | |
|---------------------------------|--------------------|-----|-----|-----|-----|-----|-----|-----|
| | a | | b | | c | | d | |
| | TAK | NIE | TAK | NIE | TAK | NIE | TAK | NIE |
| Usługowa | 31 | 9 | 35 | 5 | 30 | 10 | 28 | 12 |
| Produkcyjna | 7 | 3 | 8 | 2 | 7 | 3 | 5 | 5 |
| Usługowo-produkcyjna | 13 | 9 | 16 | 6 | 17 | 5 | 13 | 9 |
| Konsultingowa | 1 | 1 | 0 | 2 | 0 | 2 | 0 | 2 |
| Inna | 18 | 0 | 13 | 5 | 18 | 0 | 14 | 4 |
| Razem | 70 | 22 | 72 | 20 | 72 | 20 | 60 | 32 |

Wykres 6.42

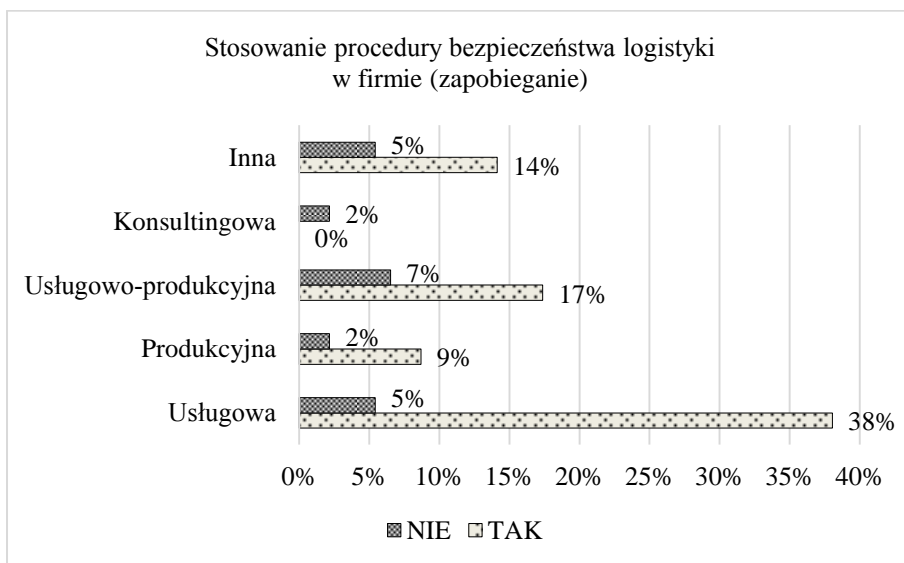
Odsetek odpowiedzi na pytanie o stosowanie procedur zarządzania bezpieczeństwem w fazie planowania w zależności od rodzaju prowadzonej działalności



Procedury zarządzania bezpieczeństwem systemów logistycznych dla fazy planowania najczęściej są stosowane w firmach o charakterze usługowym: w 34% (31 podmiotów) wobec 10% (9 podmiotów), w których procedur się nie stosuje. Kolejną liczną grupę stanowią firmy zakwalifikowane do kategorii „inne”: 20% tej grupy stosuje procedury bezpieczeństwa dla fazy planowania (18 podmiotów). W tej grupie stwierdza się brak podmiotów, które tych procedur nie stosują. Procedury są stosowane w 14% firm usługowo-produkcyjnych, 8% firm produkcyjnych i w 1% firm konsultingowych. Stwierdza się występowanie podmiotów, które nie stosują procedur dla fazy planowania w grupie 10% firm usługowo-produkcyjnych, 3% firm typu produkcyjnego i w 1% firm konsultingowych. Zestawienie prezentuje tabela 6.44 i wykres 6.42.

Wykres 6.43

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie zapobiegania w zależności od rodzaju działalności



Procedury zarządzania bezpieczeństwem systemów logistycznych dla fazy zapobiegania najczęściej są stosowane w firmach o charakterze usługowym: 35 podmiotów (38%) wobec 5 podmiotów (5%), w których procedur dla tej fazy się nie stosuje. Liczną grupę stanowią firmy sektora usługowo-produkcyjnego, w którym dla 16 podmiotów (17%) stosowanie procedur jest praktyką wobec 6 podmiotów (7%) niestosujących procedur.

Kolejną dużą grupę stanowią firmy zakwalifikowane do kategorii „inne”: 13 podmiotów tej grupy, co stanowi 14% grupy badanej, stosuje procedury wobec 5 podmiotów (5%), które tych procedur nie stosują. W grupie firm pro-

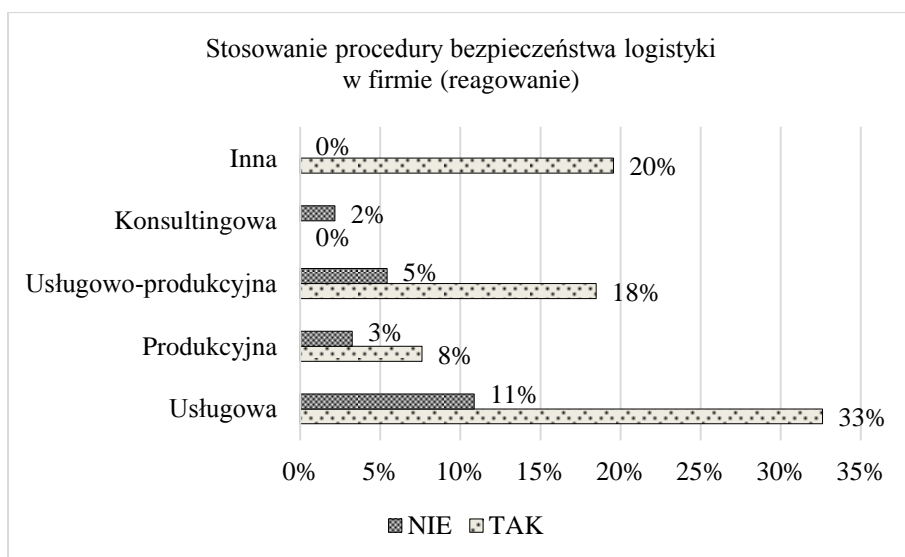
dukcyjnych 8 podmiotów ma wdrożone procedury, co stanowi 9% badanych wobec 2 podmiotów (2%), które nie stosują w tej fazie procedur bezpieczeństwa.

Wśród firm konsultingowych 2% w badanej próbie stwierdziło brak stosowania procedury bezpieczeństwa systemów logistycznych dla fazy zapobiegania, co przedstawiono graficznie na wykresie 6.43.

Procedury zarządzania bezpieczeństwem systemów logistycznych dla fazy reagowania najczęściej są stosowane w firmach o charakterze usługowym: 30 podmiotów (33%) wobec 10 podmiotów (11%), w których procedur dla tej fazy firmy nie stosują. Liczną grupą są firmy sektora usługowo-produkcyjnego, w którym dla 17 podmiotów (18%) stosowanie procedur jest praktyką wobec 5 podmiotów (5%) niestosujących procedur. Kolejną liczną grupę stanowią firmy zakwalifikowane do kategorii „inne”, w której 18 podmiotów tej grupy, co stanowi 20% grupy badanej, stosuje procedury. W grupie tej nie stwierdza się podmiotów, które tych procedur nie stosują. W grupie firm produkcyjnych 7 podmiotów ma wdrożone procedury, co stanowi 8% badanych wobec 3 podmiotów (3%), które nie stosują w tej fazie procedur bezpieczeństwa. Zestawienie prezentuje wykres 6.44. W grupie badanej w firmach konsultingowych nie stwierdza się stosowania procedur bezpieczeństwa.

Wykres 6.44

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od rodzaju prowadzonej działalności

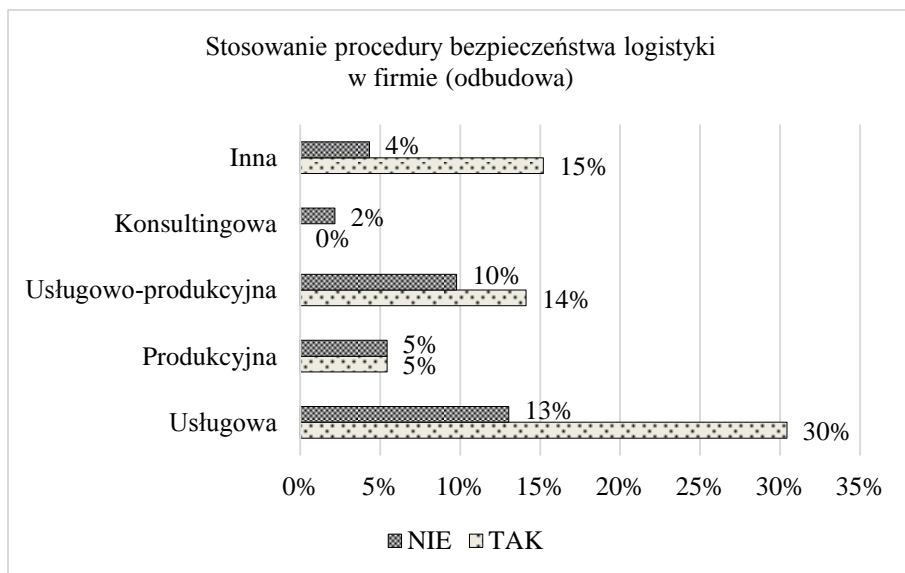


Procedury bezpieczeństwa dla fazy odbudowy są stosowane we wszystkich wyróżnionych rodzajach firm. Podobnie jak w poprzednio analizowanych przykładach najwięcej zastosowań procedur występuje w firmach usługowych –

28 podmiotów (30%) wobec 12 firm (13%), które ich nie stosują. Kolejną grupą są firmy ujęte w grupie firm wyróżnionych jako „inne”. W grupie tej 14 podmiotów (15%) stosuje procedury wobec 4 podmiotów (4%) niestosujących procedur. Kolejną grupę stanowią firmy usługowo-produkcyjne z 13 podmiotami (14%) stosującymi procedury wobec 9 firm (10% ogółu), które procedur nie stosują. Firmy produkcyjne obejmują 5 podmiotów, które stosują procedury bezpieczeństwa i 5 podmiotów niestosujących procedur. Obie wielkości stanowią po 5% ogółu firm. Wyróżnione firmy konsultingowe (2 podmioty) stanowią 2% ogółu i podmioty te zgłosiły, że nie mają wdrożonych procedur bezpieczeństwa dla fazy odbudowy. Zestawienie przedstawia wykres 6.45.

Wykres 6.45

Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od rodzaju prowadzonej działalności



W przypadku zależności od rodzaju finansowania działalności kapitałem krajowym lub obcym odpowiedzi rozkładają się następująco:

Dla fazy planowania: 70% firm z kapitałem krajowym stwierdza, że procedury są w firmach stosowane i 7% – z kapitałem obcym.

Dla fazy zapobiegania: w 72% firm z kapitałem krajowym i w 7% z kapitałem obcym są stosowane procedury zarządzania bezpieczeństwem systemów logistycznych. W 22% badanej grupy, która jest z krajowym kapitałem nie są stosowane procedury bezpieczeństwa.

Dla fazy reagowania stwierdza się, że procedury bezpieczeństwa są stosowane w firmach zarówno z kapitałem krajowym, jak i obcym. Dla 67 podmiotów z krajowym kapitałem (73%), jak i dla 5 z kapitałem obcym (5%) są stosowane procedury zarządzania bezpieczeństwem systemów logistycznych. W 19 firmach z kapitałem krajowym, co stanowi 21% badanej grupy, nie są stosowane procedury bezpieczeństwa. Dla 1% firm z kapitałem obcym w tej fazie również procedury bezpieczeństwa nie są stosowane.

Dla fazy odbudowy procedury są stosowane w firmach zarówno z kapitałem krajowym, jak i obcym. Dla 56 podmiotów z krajowym kapitałem (61%), jak i dla 4 z kapitałem obcym (4%) są stosowane procedury zarządzania bezpieczeństwem systemów logistycznych. W 30 firmach z kapitałem krajowym, co stanowi 33% badanej grupy, nie są stosowane procedury bezpieczeństwa. Dla 2% firm z kapitałem obcym w tej fazie również procedury bezpieczeństwa nie są stosowane.

Pytanie 12

W jakiej formie odbywa się zarządzanie zasobami własnymi (materialne, ludzkie, finansowe, informacyjne) dla zapewnienia wymaganego poziomu bezpieczeństwa funkcjonowania systemu logistycznego:

- a) autonomicznie – jest integralną częścią zarządzania firmą?
- b) jest realizowane przez wyspecjalizowany podmiot zewnętrzny?

Tabela 6.45

Rozkład odpowiedzi dla pytania nr 12

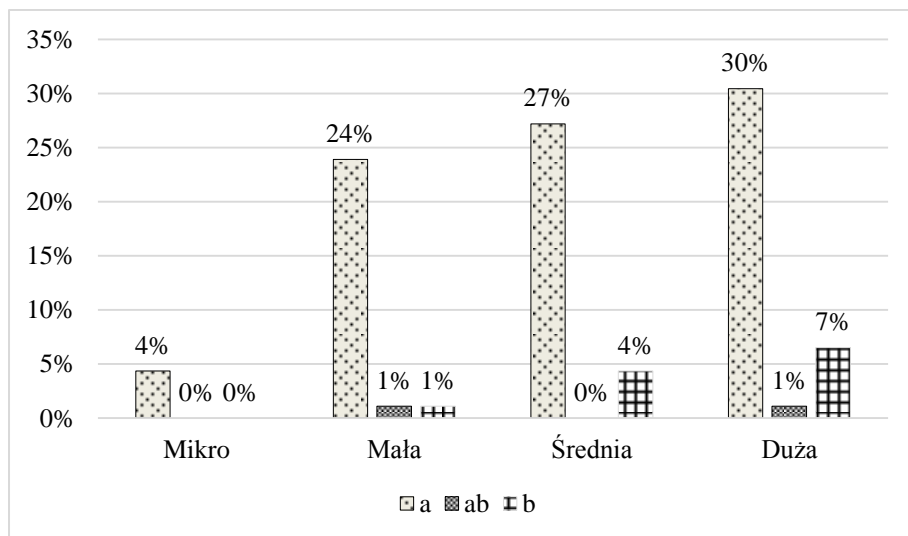
| Sposób zarządzania zasobami własnymi | N = 92 | |
|--|--------|---------|
| | n | % |
| Autonomiczny | 79 | 86% |
| Podmiot zewnętrzny | 11 | 12% |
| Wśród badanych firm 2 podmioty zadeklarowały zarówno pierwszy, jak i drugi sposób zarządzania zasobami | 2 | 2% |
| Razem | 92 | 100,00% |

Sposób pierwszy zarządzania zasobami, który w swej istocie stanowi integralną część zarządzania firmą jest sposobem najpopularniejszym. Stosuje go 86% badanych firm. Drugi sposób, w którym firmy zlecają zarządzanie zasobami wyspecjalizowanym podmiotom zewnętrznym jest realizowane w 12% firm. W przypadku dwóch procent firm (2 podmioty badane) zarządzanie zasobami jest realizowane z wykorzystaniem z obu wariantów – tabela 6.45).

Autonomiczny sposób zarządzania zasobami własnymi jest podstawową procedurą dla 30% firm dużych (18 podmiotów badanej grupy). W grupie firm dużych w 7% jest stosowany również drugi sposób oparty na wyspecjalizowanym podmiocie zewnętrznym (6 firm w grupie badanej). W tej grupie znajduje się 1% firm (1 podmiot), w którym zarządzanie zasobami odbywa się z zastosowaniem obu wariantów. Korzystanie z wariantu mieszanego występuje w grupie firm małych. Zidentyfikowano 1% firm badanych (1 podmiot grupy badanej). Wariant „a”, czyli autonomiczne zarządzanie zasobami, jako jedyny sposób zarządzania, występuje w grupie firm mikro i stanowi 4% ogółu badanych firm. W firmach małych wariant „a” jest podstawą zarządzania zasobami dla 24% podmiotów (22 firmy), a dla firm średniej wielkości stanowi podstawę zarządzania dla 27 podmiotów (25 firm) – wykres 6.46.

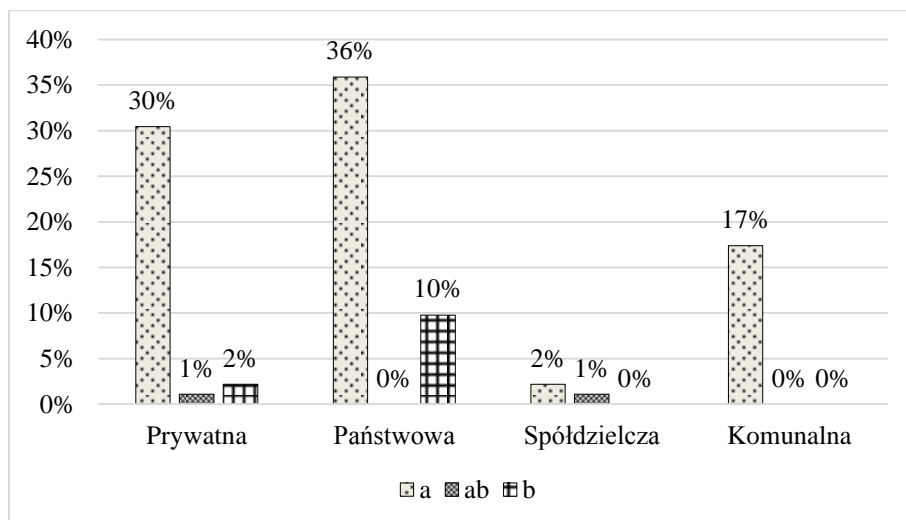
Wykres 6.46

Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy w zależności od wielkości podmiotu



Firmy najliczniej stosują wariant „a”, czyli autonomiczny sposób zarządzania zasobami: firmy państwowe 33 podmioty (36%), firmy prywatne 28 podmiotów (30%), firmy komunalne 16 podmiotów (17%) oraz spółdzielcze 2 (2%). Wśród firm państwowych wyróżnia się drugi sposób zarządzania zasobami dla 9 podmiotów, co stanowi 10%, oraz dla firm prywatnych, w których wstępuje w 2% firm. W grupie firm spółdzielczych i prywatnej wstępuje wariant zidentyfikowany, jako połączenie wariantów „a” i „b” i jest to 1% badanych (wykres 6.47).

Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy
w zależności od formy własności firmy



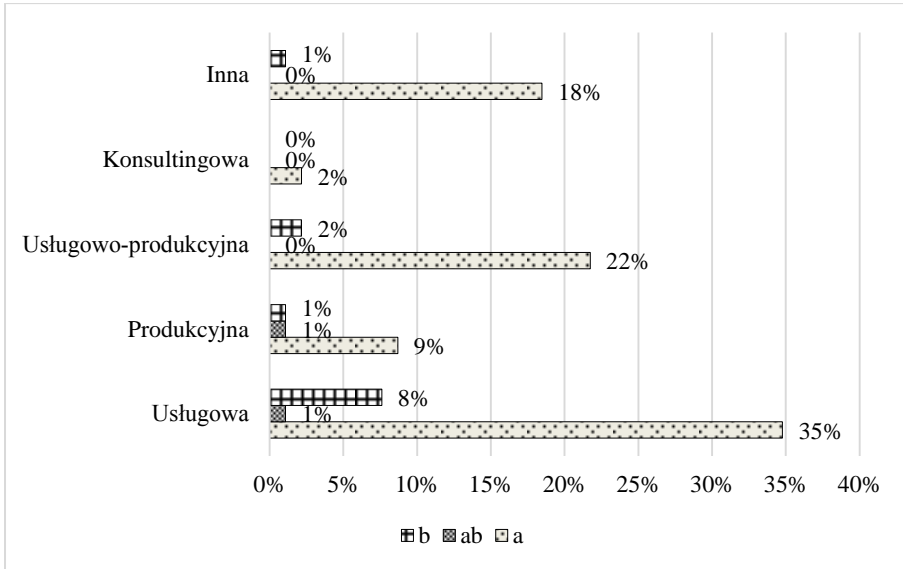
Autonomiczny sposób zarządzania zasobami jest powszechnie stosowany we wszystkich podmiotach bez względu na rodzaj wykonywanej działalności. Najszerszej jednakże stosowany jest w firmach o charakterze usługowym: 32 podmioty (35%), usługowo-produkcyjnych – 20 podmiotów (22%), w firmach przypisanych do kategorii „inne” dla 17 firm stanowi podstawę zarządzania zasobami (18%).

Drugi sposób zarządzania zasobami w oparciu o wyspecjalizowany podmiot zewnętrzny jest zdecydowanie mniej rozpowszechniony. Występuje w 8% firm rodzaju usługowego, 2% usługowo-produkcyjnych, w 1% firm produkcyjnych i 1% firm zakwalifikowanych do kategorii „inne”. Ponadto w przypadku 1% firm rodzaju usługowego i produkcyjnego występuje mieszane zarządzanie zasobami, czyli w jakiejś części jest autonomiczne, a w jakiejś realizowane przez podmiot zewnętrzny (wykres 6.48).

Stwierdza się, że zarządzanie zasobami firmy w podmiotach z kapitałem krajowym w 80% odbywa się w wariantcie pierwszym (autonomicznym), w 12% przy wykorzystaniu wyspecjalizowanego podmiotu zewnętrznego, 1% realizuje wariant mieszany. W przypadku podmiotów z kapitałem obcym 5% zarządzanie realizuje korzystając z wariantu pierwszego, a 1% z wariantu mieszanego (wykres 6.49).

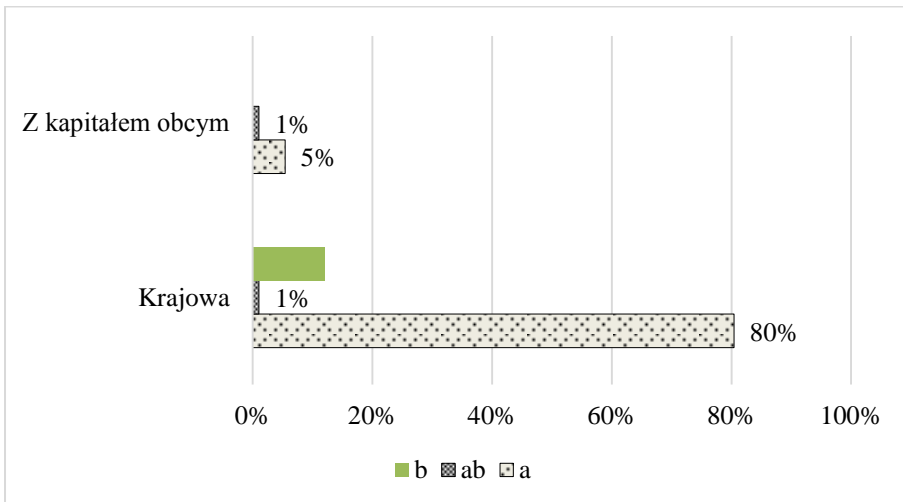
Wykres 6.48

Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy
w zależności od rodzaju prowadzonej działalności



Wykres 6.49

Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy
w zależności od sposobu finansowania działalności



Pytanie 13

Czy zostały wdrożone procedury współdziałania z otoczeniem zewnętrznym w celu efektywnego zarządzania bezpieczeństwem systemu logistycznego?

Warunki, w których współczesne systemy logistyczne realizują swoje cele, tym bardziej gdy dotyczą one zarządzania bezpieczeństwem, zmuszają je do wchodzenia w relacje oparte na współdziałaniu. Dzięki współpracy sprawniej i efektywniej, czyli skuteczniej i ekonomiczniej, podmioty mogą osiągać cele, w tym cele bezpieczeństwa, których spełnienie w pojedynkę byłoby niemożliwe lub trzeba by przeznaczyć znacznie więcej sił i środków. Współdziałanie pozwala bowiem przekraczać granice systemów, a coraz częściej nawet granice sektorów. Gwarancją współdziałania różnych odrębnych organizacji i instytucji na rzecz uzgodnionych celów (bezpieczeństwa) jest dzielenie się informacjami i wiedzą pomiędzy podmiotami współpracującymi, podstawą – wdrożenie procedur regulujących współdziałanie.

W grupie 92 badanych podmiotów logistycznych 65% firm posiada wdrożone procedury współdziałania z otoczeniem wobec 35% firm, które wdrożeń nie posiadają – tabela 6.46.

Tabela 6.46

Rozkład odpowiedzi na pytanie nr 13

| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| Wdrożenie procedur współdziałania z otoczeniem w celu efektywnego zarządzania bezpieczeństwem systemu logistycznego | TAK | 60 | 65% |
| | NIE | 32 | 35% |
| Razem | | 92 | 100,00% |

Dzięki pogłębionym wywiadam uzyskano informacje o działaniach, najczęściej długofalowych, które są podejmowane w celu niwelowania negatywnych skutków funkcjonowania systemów logistycznych. Działania te obejmują między innymi:

- okresowe audyty bezpieczeństwa (fizycznego, teleinformatycznego, ppoż., urządzeń technicznych) przez wyspecjalizowane firmy;
- systematyczne szkolenia personelu przez zewnętrznych specjalistów w uruchamianiu i realizowaniu procedur na wypadek sytuacji nieplanowych;
- ochronę fizyczną przez profesjonalne firmy typu SUFO (Specjalistyczne Uzbrojone Formacje Ochrony) w zakresie ochrony osób i mienia – mają obowiązek współpracy z Policją, Państwową Strażą Pożarną, Strażą Miejską;
- przygotowanie rezerwowej infrastruktury logistycznej (np. magazynowej, transportowej, zasileniowej w wodę, gaz, energię elektryczną);
- zapasy utrzymywane przez inne podmioty gospodarcze.

W zależności od wielkości firmy ilość wdrożeń procedur jest w podobnej wielkości w wyróżnionych typach. Najwięcej jest w firmach małych (24%), przy

bardzo małym odsetku braku wdrożeń (2%). Kolejna grupa to firmy z segmentu dużych (22%), w których jednocześnie jest duża grupa firm, która tych wdrożeń nie posiada (16%). Podobnie jest z firmami średniej wielkości – 20% je posiada wobec 12%, które jej nie posiadają. W zidentyfikowanych firmach mikro nie ma wdrożeń procedur współdziałania z otoczeniem (tabela 6.47).

Tabela 6.47

Częstość odpowiedzi na pytanie o potwierdzenie wdrożenia procedur w zależności od wielkości firmy

| Kategoria wyróżnienia: wielkość firmy | N = 92 | | | |
|---------------------------------------|--------|--------|-----|--------|
| | TAK | % | NIE | % |
| Mikro | 0 | 0% | 4 | 4% |
| Mała | 22 | 24% | 2 | 2% |
| Średnia | 18 | 20% | 11 | 12% |
| Duża | 20 | 22% | 15 | 16% |
| Razem | 60 | 66,00% | 32 | 34,00% |

Procedury wdrożenia współdziałania z otoczeniem są obecne we wszystkich typach własności firm. Najczęściej procedury są wdrażane w firmach państwowych (32%) wobec 14% firm, które wdrożeń nie mają, w 16% firm komunalnych, 13% prywatnych, 3% spółdzielczych. Wśród grupy badanych firm spółdzielczych i komunalnych nie ma podmiotów, w których takie procedury nie byłby wdrożone. Natomiast w grupie firm prywatnych 21% przyznaje się do braku wdrożenia procedur. Zestawienie liczbowe zawiera tabela 6.48 i wykres 6.50 załącznika 6.1.

Tabela 6.48

Rozkład odpowiedzi w zależności od formy własności firmy

| Forma własności firmy | N = 92 | | | | Razem n |
|-----------------------|--------|-----|-----|-----|---------|
| | tak | % | nie | % | |
| Prywatna | 12 | 13% | 19 | 21% | 31 |
| Państwowa | 29 | 32% | 13 | 14% | 42 |
| Spółdzielcza | 3 | 3% | 0 | 0% | 3 |
| Komunalna | 16 | 17% | 0 | 0% | 16 |
| Razem | 60 | 65% | 32 | 35% | 92 |

W zależności od rodzaju prowadzonej działalności najwięcej wdrożeń mają firmy usługowe – 30% badanej grupy przedsiębiorstw. Kolejną grupę firm z wdrożeniami są firmy zgrupowane w kategorii firm „inne” – 16% i usługowo-produkcyjne – 11%, produkcyjne – 7%, 1% – firmy konsultingowe.

W wyróżnionych rodzajach firm egzystują również podmioty, które nie mają wdrożeń procedur współdziałania z otoczeniem. W grupie firm usługowych jest to 13%, podobnie w firmach usługowo-produkcyjnych – 13%, w firmach produkcyjnych – 4%, podobnie w grupie „inne” – 4% i 1% – firmy konsultingowe (tabela 6.49, wykres 6.51 – załącznik 6.1).

Tabela 6.49

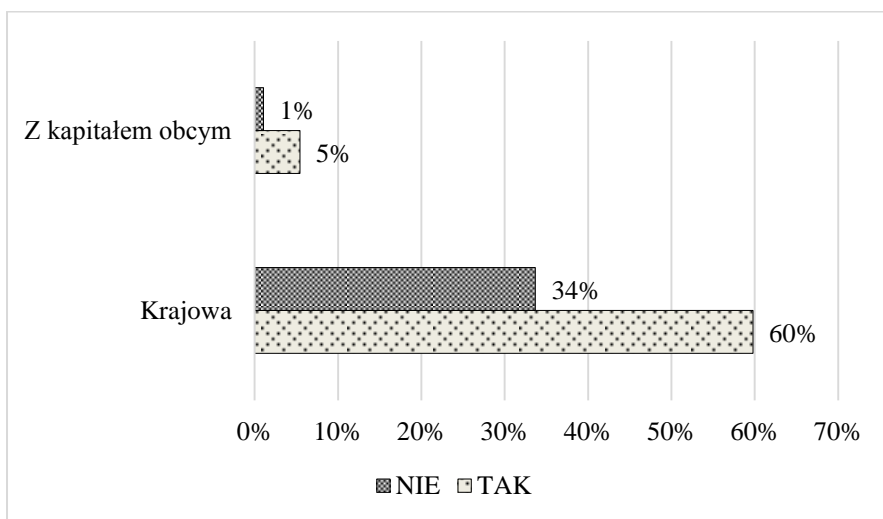
Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 | | | | Suma |
|---------------------------------|--------|-----|-----|-----|------|
| | tak | % | nie | % | |
| Usługowa | 28 | 30% | 12 | 13% | 40 |
| Produkcyjna | 6 | 7% | 4 | 4% | 10 |
| Usługowo-produkcyjna | 10 | 11% | 12 | 13% | 22 |
| Konsultingowa | 1 | 1% | 1 | 1% | 2 |
| Inna | 15 | 16% | 3 | 3% | 18 |
| Razem | 60 | 65% | 32 | 35% | 92 |

W zależności od sposobu finansowania działalności, firmy z kapitałem krajowym w 60% mają wdrożone procedury współdziałania z otoczeniem wobec 34% firm, które tych wdrożeń nie mają. Wśród firm z kapitałem obcym 5% posiada wdrożenia, a 1% nie (wykres 6.52).

Wykres 6.52

Odsetek odpowiedzi na pytanie o wdrożenie procedur współdziałania z otoczeniem w zależności od sposobu finansowania działalności



Pytanie 14

Czy wypracowane procedury oraz wydzielone zasoby zapewniające akceptowalny (przez Firmę i obowiązujące wymagania formalno-prawne) poziom bezpieczeństwa są zgodne z obowiązującymi standardami krajowymi i europejskimi?

W ogólnej liczbie udzielonych odpowiedzi 79% firm posiada wypracowane procedury oraz wydzielone zasoby, które spełniają poziom akceptowalny bezpieczeństwa i są one zgodne z obowiązującymi standardami zarówno krajowymi, jak i zagranicznymi. 21% firm stwierdziło, że nie zapewnia takiej zgodności (tabela 6.50).

Niewielkie różnice występują wśród firm kategoryzowanych ze względu na wielkość w odsetku podmiotów zapewniających zgodność procedur oraz wydzielonych zasobów zapewniających akceptowalny poziom bezpieczeństwa z aktualnymi standardami krajowymi i europejskim. W grupie badanych podmiotów 26% firm dużych, 25% firm małych, 24% firm średniej wielkości zgodność zapewnia.

Tabela 6.50

Rozkład odpowiedzi na pytanie nr 14

| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| Zgodność procedur oraz wydzielonych zasobów przy akceptowalnym poziomie bezpieczeństwa z obowiązującymi standardami krajowymi i europejskim | TAK | 73 | 79% |
| | NIE | 19 | 21% |
| Razem | | 92 | 100,00% |

Zgodności nie zapewnia 12% firm dużych, 8% średniej wielkości i 1% firm małych. Wśród firm mikro nie ma firm, które nie zapewniałyby zgodności procedur wewnętrznych ze standardami (tabela 6.51 i wykres 6.53 – załącznik 6.1).

Tabela 6.51

Rozkład odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskim w zależności od wielkości firmy

| Kategoria wyróżnienia: Wielkość firmy | N = 92 | | | |
|--|--------|-----|-----|-----|
| | TAK | % | NIE | % |
| Mikro | 4 | 4% | 0 | 0% |
| Mała | 23 | 25% | 1 | 1% |
| Średnia | 22 | 24% | 7 | 8% |
| Duża | 24 | 26% | 11 | 12% |
| Razem | 73 | 79% | 19 | 21% |

W kategorii własności firmy zgodność procedur wewnętrznych ze standardami zapewniają w 36% firmy państwowe i 23% prywatne. Kolejną grupę

stanowi 17% firm komunalnych oraz 3% firm spółdzielczych. W grupie firm komunalnych i spółdzielczych 100% firm zapewnia zgodność. Brak zgodności występuje w 11% podmiotów prywatnych i 10% państwowych (tabela 6.52).

Tabela 6.52

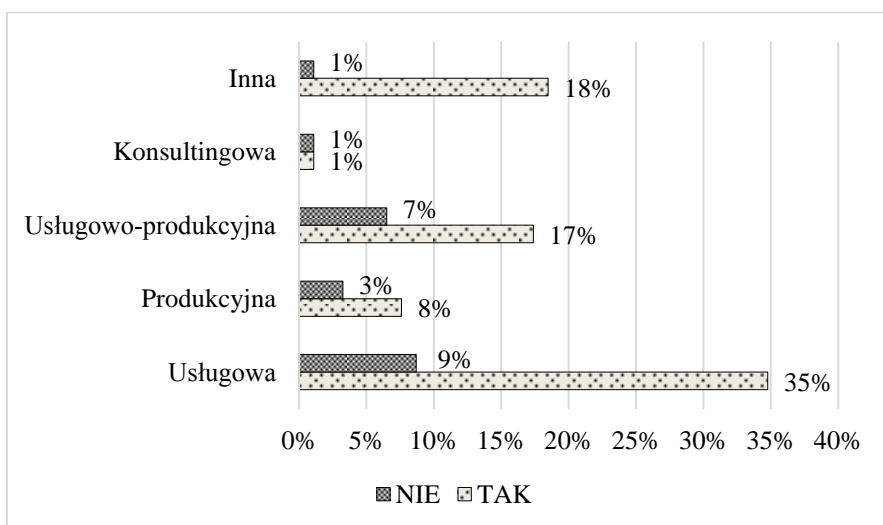
Rozkład odpowiedzi w zależności od formy własności firmy

| Forma własności firmy | N = 92 | | | | Suma n |
|-----------------------|--------|-----|-----|-----|--------|
| | TAK | % | NIE | % | |
| Prywatna | 21 | 23% | 10 | 11% | 31 |
| Państwowa | 33 | 36% | 9 | 10% | 42 |
| Spółdzielcza | 3 | 3% | 0 | 0% | 3 |
| Komunalna | 16 | 17% | 0 | 0% | 16 |
| Razem | 73 | 79% | 19 | 21% | 92 |

Najliczniejszą grupę firm zapewniających zgodność procedur wewnętrznych ze standardami tworzą firmy prowadzące działalność usługową – jest to 35% ogółu badanych podmiotów. W grupie tej tylko 9% firm nie zapewnia zgodności. W grupie firm sklasyfikowanych jako „inne” 18% zapewnia zgodność i tylko 1% jej nie zapewnia. Podobnie jest w grupie firm usługowo-produkcyjnych, w której 17% zgodność zapewnia, wobec 7% firm, które tej zgodności nie zapewniają (wykres 6.54).

Wykres 6.54

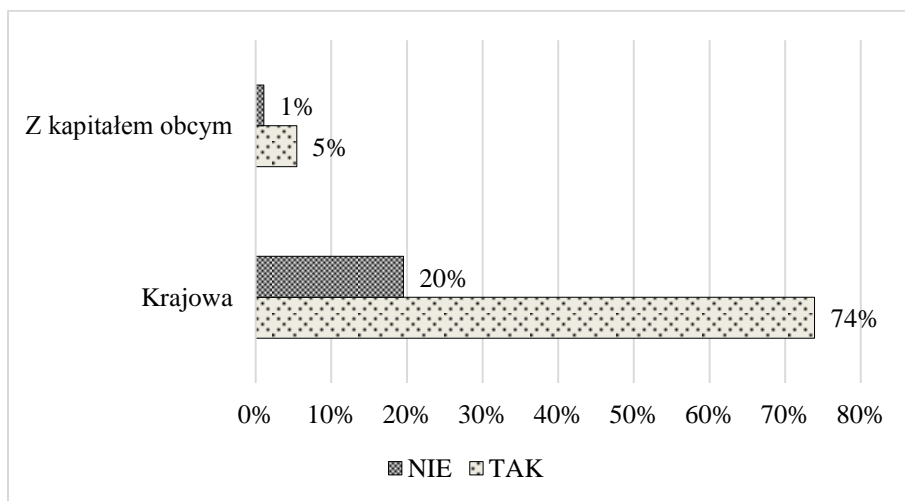
Odsetek odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskimi w zależności od rodzaju prowadzonej działalności



Zgodność procedur zapewniają firmy z kapitałem krajowym w 74%, a z kapitałem obcym w 5%. Firm niezapewniających zgodności w grupie firm finansujących działalność kapitałem krajowym jest 20%, a w grupie firm z kapitałem obcym 1% (wykres 6.55).

Wykres 6.55

Odsetek odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskimi w zależności od sposobu finansowania działalności



Pytanie 17

Proszę podać przykłady praktycznych i konkretnych rozwiązań (organizacyjnych, technicznych i innych) w zakresie zapewnienia bezpieczeństwa systemów logistycznych?

Na 92 badane firmy przykłady praktycznych i konkretnych rozwiązań w zakresie zapewniania bezpieczeństwa systemów logistycznych podało 59% firm. 41% podmiotów udzieliło odmownej odpowiedzi (można jedynie przypuszczać, że powodem był prawdopodobnie brak takich doświadczeń albo ich nieznanostwo) – tabela 6.53.

24% firm z segmentu firm małych i 21% firm dużych oraz 12% firm średniej wielkości i 2% mikro podało przykłady rozwiązań praktykowanych w badanych podmiotach.

W grupie firm, które nie podzieliły się wiedzą ze stosowanych praktyk znalazło się: w grupie firm średnich 20%, w grupie firm dużych 17% i po 2% firmy małe i mikro. W segmencie firm średnich odsetek firm, które nie podały przykładów przewyższa odsetek firm, które podały przykłady rozwiązań (wykres 6.56).

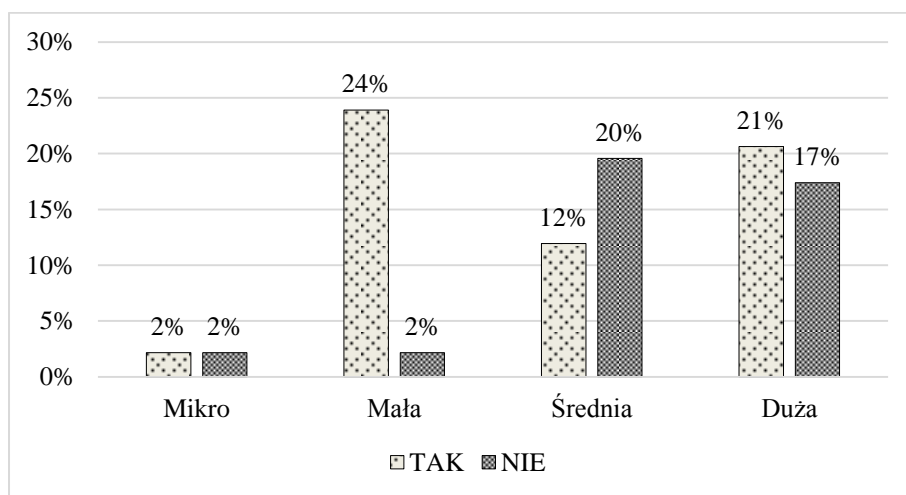
Tabela 6.53

Rozkład odpowiedzi na pytanie nr 17

| | | N = 92 | |
|---|-----|--------|---------|
| | | n | % |
| Praktyczne przykłady rozwiązań w zakresie zapewniania bezpieczeństwa systemów logistycznych | TAK | 54 | 59% |
| | NIE | 38 | 41% |
| Razem | | 92 | 100,00% |

Wykres 6.56

Odsetek odpowiedzi w zależności od wielkości firmy



W firmach wyróżnionych ze względu na rodzaj własności wiedzą praktyczną dotyczącą stosowanych praktyk najchętniej podzieliło się 24% firm państwowych. Kolejną grupę stanowiły firmy komunalne – 17% i prywatne – 15% oraz 2% – firmy typu spółdzielczego. W grupie firm prywatnych zwraca uwagę większy odsetek firm, które nie podały przykładów (18%) w stosunku do tych, które podały. Wśród firm państwowych jest również duży odsetek firm, które nie podały przykładów (tabela 6.54).

W zależności od rodzaju prowadzonej działalności przykłady podało 33% firm usługowych, 13% usługowo-produkcyjnych, 5% firm produkcyjnych oraz 8% firm zgrupowanych w kategorii „inne”. Wśród grupy firm konsultingowych 2% nie podało przykładów (wykres 6.57).

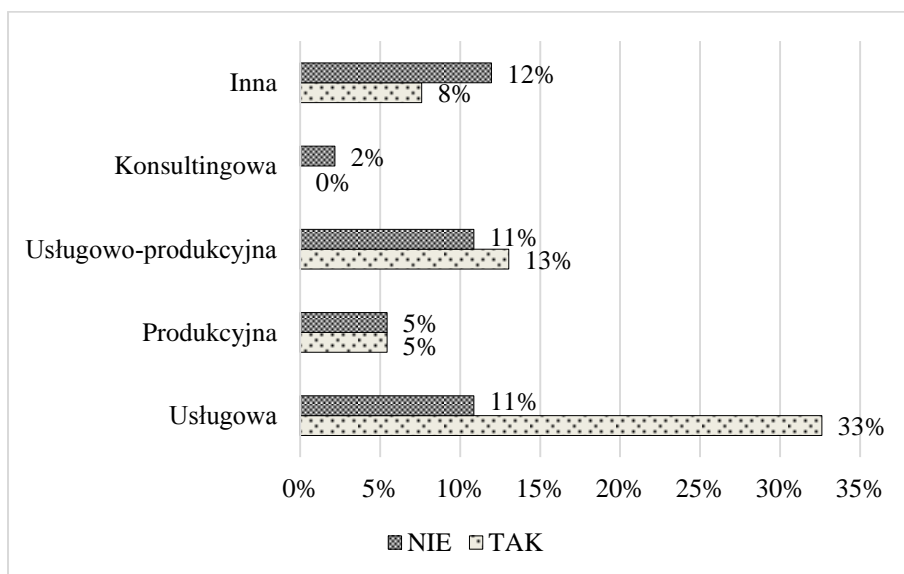
Tabela 6.54

Rozkład odpowiedzi w zależności od formy własności firmy

| Rodzaj własności firmy | N = 92 | | | |
|------------------------|--------|-----|-----|-----|
| | TAK | % | NIE | % |
| Prywatna | 14 | 15% | 17 | 18% |
| Państwowa | 22 | 24% | 20 | 22% |
| Spółdzielcza | 2 | 2% | 1 | 1% |
| Komunalna | 16 | 17% | 0 | 0% |
| Razem | 54 | 59% | 38 | 41% |

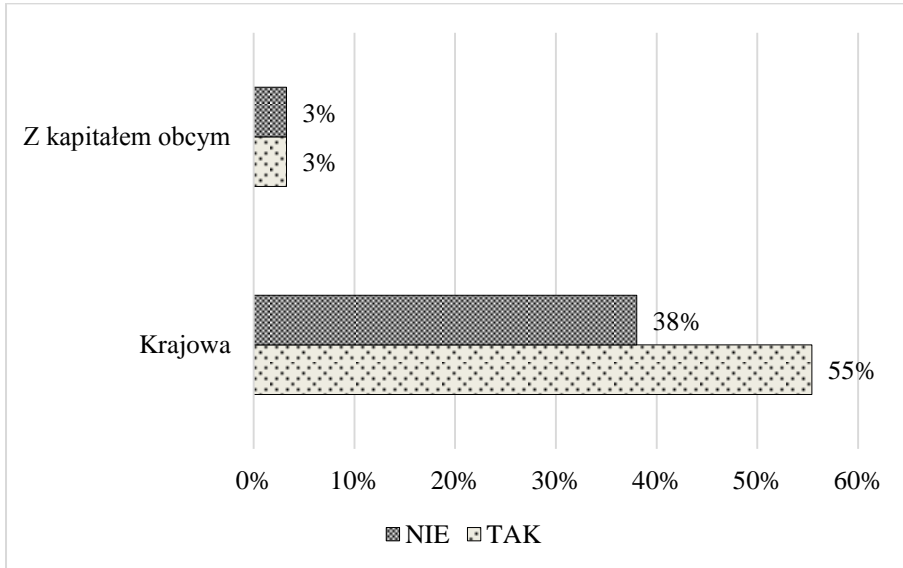
Wykres 6.57

Odsetek odpowiedzi w zależności od rodzaju prowadzonej działalności



W badaniu zależności wyboru odpowiedzi od sposobu finansowania działalności 55% firm finansowanych kapitałem krajowym podało przykłady, ale 38% nie. 3% firm finansowanych kapitałem obcym podało przykłady wobec 3% firm, które tego nie zrobiły (wykres 6.58).

Odsetek odpowiedzi w zależności od sposobu finansowania działalności



Pytanie 18

Czy w firmie prowadzi się szkolenia związane z zarządzaniem bezpieczeństwem systemów logistycznych? Jeśli tak to czy:

- własnymi „siłami”?
- za pomocą wyspecjalizowanych firm zewnętrznych?

Szkolenia powinny być traktowane jako długookresowa inwestycja, która przyniesie wzrost efektywności w kilku obszarach systemu (organizacji, instytucji, logistycznego), np. obniżenie kosztów związanych z bezpieczeństwem, wzrost poziomu bezpieczeństwa, wzrost świadomości. Współczesne szkolenia, obok tradycyjnych form, są uzupełniane narzędziami, które np. umożliwiają symulacje, co ma ogromne znaczenie dla praktyki w zakresie szkoleń zarządzania kryzysowego. W firmach na sprawność i efektywność ma wpływ bezpieczeństwo systemów logistycznych. Firmy, doceniając znaczenie podnoszenia kwalifikacji i kompetencji w obszarze bezpieczeństwa, prowadzą szkolenia. Formy szkoleń są zależne od wielu czynników (np. finansowe, osobowe, celowościowe). O wyborze formy szkolenia decyduje kadra zarządzająca, która formułuje cele do osiągnięcia przez podmiot. W ogólnej liczbie badanych podmiotów wariant „a” własnymi siłami wybrało 60% firm, a 43% podało, że stosuje formę szkolenia „b”, czyli za pomocą wyspecjalizowanych firm zewnętrznych (tabela 6.55).

Tabela 6.55

Rozkład odpowiedzi do pytania nr 18

| Prowadzenie szkoleń związanych z zarządzaniem bezpieczeństwem systemów logistycznych | | N = 92 | |
|--|-----|--------|-----|
| | | n | % |
| Własnymi siłami | TAK | 55 | 60% |
| | NIE | 37 | 40% |
| Za pomocą wyspecjalizowanych firm zewnętrznych | TAK | 40 | 43% |
| | NIE | 52 | 57% |

W grupie firm dużych częściej jest wybierany wariant „a”, czyli prowadzenie szkoleń własnymi siłami. 21% firm segmentu dużych podmiotów wybiera ten wariant, a 14% wariant „b” opierający się o wyspecjalizowane firmy zewnętrzne. Podobnie jest w przypadku firm z grupy średnich z tym, że wariant „a” jest w zdecydowanej przewadze wyborów (17% firm) nad wariantem „b” – 9% firm. Wariant „a” jest dwa razy częściej wybierany niż wariant „b”. W grupie firm małych ilość wybieranych wariantów „a” i „b” jest porównywalna: wariant „a” stanowi 20%, a wariant „b” 21%. Firmy mikro stanowią niewielką grupę w badanej populacji firm. Wybierają zdecydowanie wariant „a”. Zestawienie prezentuje tabela 6.56, wykres 6.59 – załącznik 6.1.

Tabela 6.56

Rozkład odpowiedzi w zależności od wielkości firmy

| Wielkość firmy | N = 92 (wariant a) | | | | N = 92 (wariant b) | | | |
|----------------|--------------------|-----|-----|-----|--------------------|-----|-----|-----|
| | TAK | % | NIE | % | TAK | % | NIE | % |
| Mikro | 2 | 2% | 2 | 2% | 0 | 0% | 4 | 4% |
| Mała | 18 | 20% | 6 | 7% | 19 | 21% | 5 | 5% |
| Średnia | 16 | 17% | 13 | 14% | 8 | 9% | 21 | 23% |
| Duża | 19 | 21% | 16 | 17% | 13 | 14% | 22 | 24% |
| Razem | 55 | 60% | 37 | 40% | 40 | 43% | 52 | 57% |

Odsetek odpowiedzi w przypadku wyboru wariantu „a” i „b” w zależności od formy własności firmy

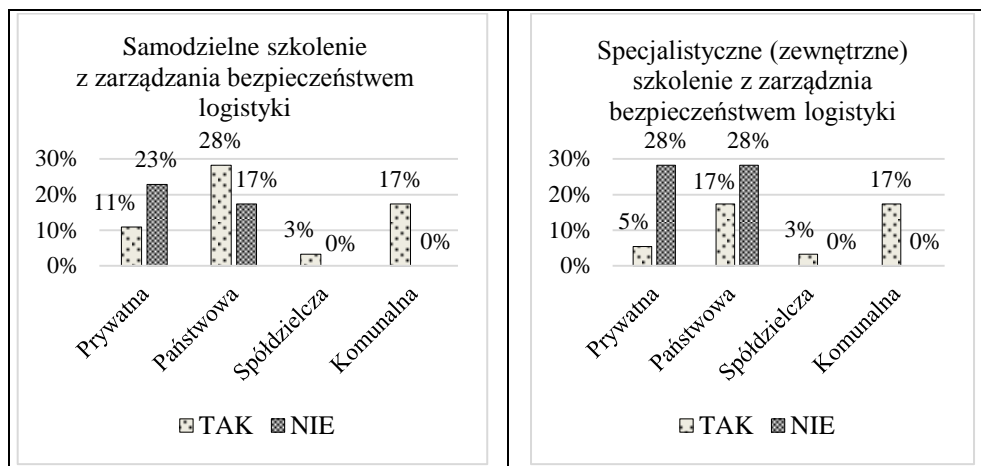


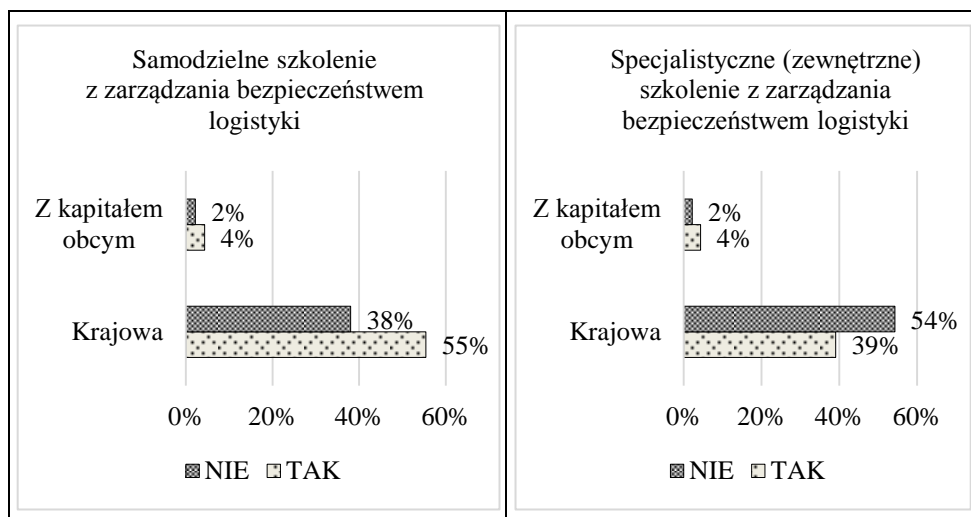
Tabela 6.58

Rozkład wyboru wariantu szkolenia w zależności od rodzaju prowadzonej działalności

| Rodzaj prowadzonej działalności | N = 92 (wariant a) | | | | N = 92 (wariant b) | | | |
|---------------------------------|--------------------|-----|-----|-----|--------------------|-----|-----|-----|
| | TAK | % | NIE | % | TAK | % | NIE | % |
| Usługowa | 29 | 32% | 11 | 12% | 25 | 27% | 15 | 16% |
| Produkcyjna | 5 | 5% | 5 | 5% | 3 | 3% | 7 | 8% |
| Usługowo-produkcyjna | 9 | 10% | 13 | 14% | 4 | 4% | 18 | 20% |
| Konsultingowa | 0 | 0% | 2 | 2% | 0 | 0% | 2 | 2% |
| Inna | 12 | 13% | 6 | 7% | 8 | 9% | 10 | 11% |
| Razem | 55 | 60% | 37 | 40% | 40 | 43% | 52 | 57% |

Wśród firm państwowych 28% podmiotów stosuje szkolenie samodzielne, a 17% firm tego segmentu wybiera wariant „b”. W segmencie firm komunalnych wybór wariantu rozkłada się równomiernie. W badanej grupie 17% firm komunalnych stosuje wariant „a” i 17% wariant „b”.

Odsetek odpowiedzi w przypadku wyboru wariantu „a” i „b” w zależności od sposobu finansowania działalności



W badanej grupie nie stwierdza się firm, w których nie byłyby stosowane szkolenia w zakresie zarządzania bezpieczeństwem systemów logistycznych. Podobnie rozkładają się wybory w grupie firm spółdzielczych, po 3% dla obu wariantów. Grupa firm prywatnych dwa razy częściej stosuje wariant „a” niż wariant „b”. Zestawienie prezentuje wykres 6.60 i tabela 6.57 – załącznik 6.1.

Firmy usługowe stosują oba warianty szkoleń, w podobnym rozkładzie: wariant „a” 32%, a wariant „b” 27%. Nieznacznie przeważa wariant „b”. W grupie firm zakwalifikowanych do kategorii „inne” 13% stosuje wariant „a” szkolenia samodzielne. W tej grupie w 9% firm jest stosowany wariant „b” korzystania z firmy zewnętrznej. W firmach o profilu usługowo-produkcyjnym 10% stosuje wariant „a”, a 4% wariant „b”. W firmach produkcyjnych 5% wybiera wariant „a”, a 3% wariant „b” (tabela 6.58).

W firmach w zależności od sposobu finansowania działalności 55% z kapitałem krajowym i 4% z kapitałem obcym stosuje szkolenia samodzielnie. Szkolenia z wykorzystaniem firm zewnętrznych w grupie firm z kapitałem krajowym stosuje 39% i 4% z kapitałem obcym (wykres 6.61).

6.3. Model zarządzania bezpieczeństwem systemów logistycznych na potrzeby logistyki bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego

Celem modelowania zarządzania bezpieczeństwem systemu logistycznego na potrzeby logistyki bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego (MZBSL) jest skonstruowanie modelu umożliwiającego poznanie zależności w rzeczywistym podmiocie bezpieczeństwa, w którym dokonuje się przemieszczanie strumienia rzeczowego i towarzyszących informacji. Model zarządzania bezpieczeństwem systemu logistycznego oraz prowadzone z nim eksperymenty pozwalają na poznanie tych zależności, tj. osiągnięcie celu modelowania.

Cele, dla których buduje się modele zarządzania bezpieczeństwem systemu logistycznego mogą być:

- 1) poznawcze, jak np. identyfikacja podsystemów logistycznych, określenie związków między wielkościami występującymi w badanym MZBSL oraz określenie przebiegu zmienności tych wielkości wynikających ze skali zagrożeń, które mogą być również przedmiotem (celem) badań;
- 2) praktyczne (użyteczne), które np. dotyczą:
 - opracowania i wdrożenia procedur zarządzania bezpieczeństwem systemu logistycznego z uwzględnieniem samego systemu oraz jego otoczenia bliższego i dalszego;
 - poszukiwania rozwiązań optymalnych, np. dobór procedur, zasobów zapewniających akceptowalny poziom bezpieczeństwa, dobór technologii informatycznych;
 - analizy i oceny wariantu funkcjonowania warunków prawnych i organizacyjnych wspomagających zarządzanie bezpieczeństwem systemu logistycznego;
 - sposobu monitorowania zagrożeń dla systemu logistycznego (pośredni, bezpośredni, z wykorzystaniem najnowszych rozwiązań technicznych lub bez nich);
 - identyfikacji i bilansowania kosztów poniesionych na zabezpieczenie się przed skutkami działań nieplanowych;
 - wyposażenia techniczno-organizacyjnego (potencjału) zarządzania bezpieczeństwem systemu logistycznego;
 - doboru potencjału zarządzania bezpieczeństwem systemu logistycznego w zależności od zagrożeń dla realizowanych procesów logistycznych.

Wielość zagadnień, jakie występują w MZBSL powoduje, że są budowane różne modele w oparciu o wcześniej zaplanowane i przemyślane procedury dla konkretnych etapów. W czasie tych czynności należy uwzględnić, że:

- poszczególne etapy należy traktować systemowo (składowe nie są wyizolowane, są połączone relacjami między sobą i otoczeniem);

- w okresie modelowania występują lub będą występować ograniczenia (np. dostępność danych z monitoringu, wielkość finansów, możliwości pomiarowe, dostępność procedur i algorytmów obliczeniowych, przygotowanie przyszłych użytkowników);
- proces konstruowania MZBSL pozwala na cykliczne powtarzanie czynności, co ułatwia powrót do odpowiedniego etapu konstruowania modelu w przypadku niezgodności wyników z zakładanymi (przyjętymi, sformułowanymi kryteriami, np. z akceptowalnym poziomem czy terminami dostaw).

Modelowanie zarządzania bezpieczeństwem systemu logistycznego powinno być zakończone uzyskaniem określonego wyniku, osiągnięciem założonego, zaplanowanego celu. Zatem w pierwszej fazie, w pierwszym etapie należy zdefiniować cele modelowania, które powinny być podporządkowane konkretnym systemom logistycznym oraz możliwym zagrożeniom.

Wybór kategorii modelu i określenie jego struktury jest etapem polegającym na dokonaniu transformacji z punktu widzenia celów modelowania danych i wiedzy o wybranym systemie logistycznym i zagrożeniach w zbiór zależnych oraz nieantagonistycznych, niekompatybilnych, logicznych relacji.

Wybór kategorii MZBSL jest podyktowany:

- stopniem zgodności z modelowanym zarządzaniem bezpieczeństwem systemu logistycznego, w obszarze bezpieczeństwa, zgodnym z akceptowalnym jego poziomem bezpieczeństwa;
- ergonomicznością i funkcjonalnością użytkownika;
- wielkością posiadanych zasobów.

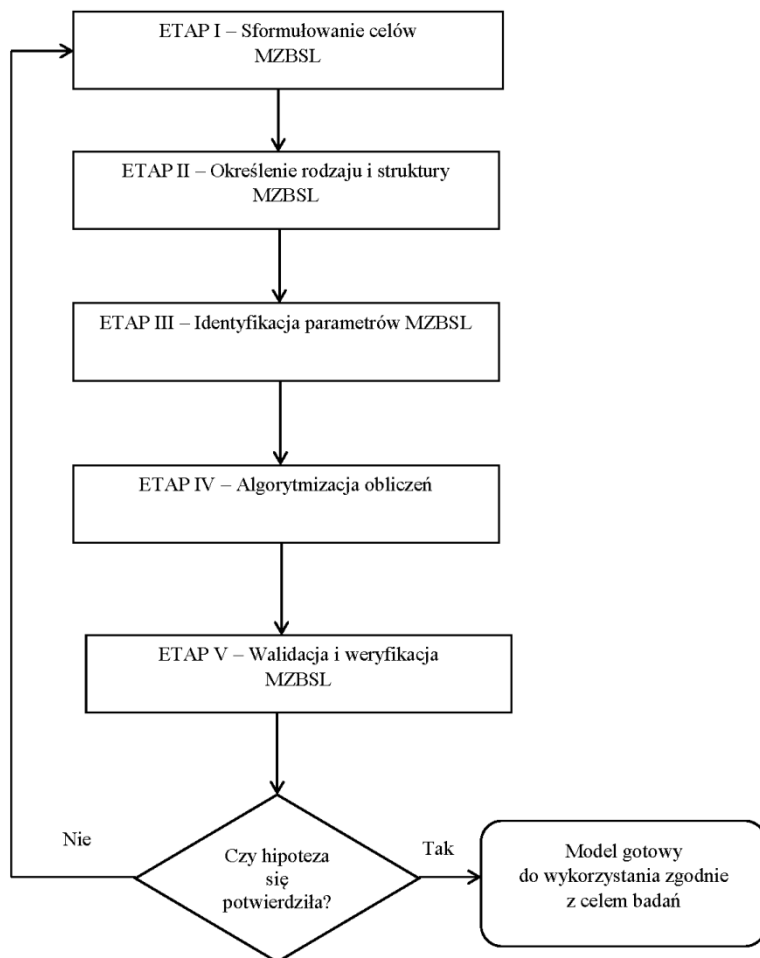
Przedstawione uwarunkowania wymuszają kompromis pomiędzy zaprezentowanymi ograniczeniami. To pozwala na wybór optymalnego MZBSL, który powinien zapewnić równowagę między zaangażowanymi środkami a ewentualnymi stratami w wyniku pojawiania się działań niepożądanych. Bowiern może się okazać, że zaangażujemy więcej środków, niż możemy stracić w wyniku nieplanowych działań związanych np. z sytuacjami kryzysowymi.

Modelowanie jest procesem dochodzenia do twierdzeń według schematu rozumowania hipotetyczno-dedukcyjnego. W tym sensie model może być traktowany jako rozwinięta hipoteza.

Procedurę konstruowania modelu systemu zarządzania bezpieczeństwem systemu logistycznego przedstawiono na rys. 6.11. Składa się ona z sześciu etapów.

Warto podkreślić, że na każdym etapie modelowanie ma dostarczać tylko tyle informacji ile jest w danym momencie potrzebne, pomijając nieistotne szczegóły.

Wymienione etapy są ze sobą powiązane, nie mogą być traktowane niezależnie, a w razie niezgodności wyniku z danymi doświadczalnymi wymagają modyfikowania założeń lub parametrów we właściwym kierunku, aż do uzyskania rozwiązania możliwego do przyjęcia dla określonego celu.



gdzie: MZBSL – model zarządzania bezpieczeństwem systemów logistycznych

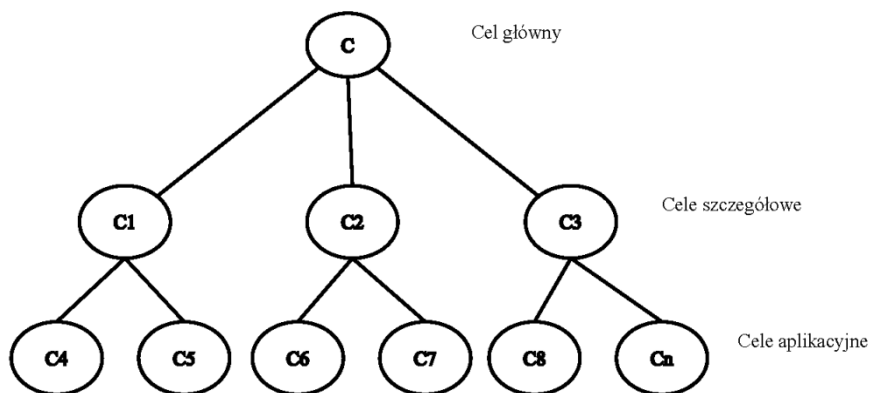
Rys. 6.11. Procedura konstruowania MZBSL (schemat matematycznego modelowania)

Źródło: opracowanie własne.

Etap I – sformułowanie celów modelowania ZBSL obejmuje³⁹⁰:

- określenie celów (rys. 6.12):
 - ✓ głównego (C),
 - ✓ szczegółowych (np. C1, C2, C3),
 - ✓ aplikacyjnych (np. C4, C5, C6, C7, C8, C_n);
- identyfikację i definiowanie informacji początkowej o badanym obiekcie;
- ustalenie dokładności odwzorowania.

³⁹⁰ Por. „Wstęp” monografii.



Rys. 6.12. Hierarchia celów (etap I)

Źródło: opracowanie własne.

Etap II – określa rodzaj i strukturę MZBSL, z uwzględnieniem hipotezy (H) oraz hipotez szczegółowych (H1, H2, H3) i obejmuje:

- ustalenie rodzajów parametrów, od których zależy akceptowalny poziom bezpieczeństwa systemu logistycznego;
- określenie zmiennych decyzyjnych związanych z pojawiającymi się sytuacjami nieplanowanymi, kryzysowymi;
- ustalenie warunków brzegowych³⁹¹, których przekroczenie spowoduje przekroczenie nieakceptowalnego poziomu bezpieczeństwa systemu logistycznego.

Określenie rodzaju i struktury oznacza proces identyfikacji, w którym dokonuje się fragmentacji systemu na podsystemy, elementy, rozpoznaje i diagnozuje relacje pomiędzy elementami, elementami a podsystemami, systemem a otoczeniem, jednocześnie rozpoznaje się typy relacji i opisuje się cechami – argumentami (cecha złożoności systemów), identyfikuje się liczbę połączeń elementów. W przypadku systemu logistycznego mamy do czynienia z socjotechnicznym systemem, a więc powinniśmy uwzględniać system wartości i potrzeb. Bierzemy pod uwagę również zmienność ogólną systemu (system jest dynamiczny), która może dotyczyć możliwości zmian struktury systemu, jak i zmian procesów w systemie (lub podsystemach) w ramach ustalonej pierwotnie struktury.

Kolejną cechą jest określenie stabilności systemu jako zdolności zachowania samego stanu (tożsamości) w obliczu zakłóceń i wymuszeń wewnętrz-

³⁹¹ Warunki brzegowe mogą być określone przez takie parametry, jak: gotowość do świadczenia usług logistycznych, czas realizacji zamówienia, czas oczekiwania między komunikatem zakończeniu procesów roboczych i rozpoczęciem transportu, stopień realizacji składowych: cel-efekt, nakład-efekt, cel-nakład itp.

nych, a także możliwych i prawdopodobnych zdarzeń niepożądanych, często prowadzących do sytuacji kryzysowych. Również konieczne jest określenie zdolności do adaptacji systemu dzięki rozpoznaniu sprzężeń regulujących, przeciwdziałających negatywnym skutkom wywołanym przez otoczenie.

Etap III – identyfikacja parametrów MZBSL obejmuje:

- plan obserwacji, pomiaru, obliczeń i analizy³⁹²;
- przeprowadzenie obserwacji, pomiaru, obliczeń i analizy;
- określenie parametrów modelu.

Do identyfikacji parametrów, które muszą być dobrane zgodnie z założonymi kryteriami, zwykle stosuje się optymalizację pewnej funkcji (np. kosztów). Konieczne jest wyjaśnianie, jakie parametry opisują i charakteryzują działania i operacje w systemie, procesie, zjawisku.

Etap IV – algorytmizacja obliczeń odnosi się do wyznaczania wartości parametrów odwzorowanych w modelu. Jest ciągiem jasno zdefiniowanych czynności (obliczeń), koniecznych do wykonania pewnego rodzaju zadań wcześniej zdefiniowanych i zdiagnozowanych. W przypadku modelowania systemowego jest to wykreowanie (opis, przeprowadzanie) systemu od stanu początkowego do końcowego.

Etap V – walidacja i weryfikacja są to procesy, które służą inspekcji wymagań i celów. Są czynnościami (operacjami, działaniem), które powinno się przeprowadzać we wszystkich fazach modelowania (warto zapamiętać, że obie te czynności zachodzą w wielu różnych momentach i mogą pojawić się w wielu fazach procesu kreowania systemu). Różnice między weryfikacją i walidacją dotyczą przede wszystkim tego, z jakiej perspektywy dokonujemy sprawdzenia (czy technologicznej i typowej dla zespołów budujących system, czy raczej z perspektywy użytkownika końcowego, który nie ma obowiązku rozumieć technicznej strony systemu, którego będzie używał). Reasumując:

- walidacja – powinna odpowiedzieć na pytania: czy zbudowany jest poprawny model? i czy model jest wiernym odwzorowaniem rzeczywistości z perspektywy jego zamierzonych zastosowań?
- weryfikacja – powinna odpowiedzieć na pytania: czy model jest zbudowany w sposób poprawny? i czy implementacja modelu jest zgodna z opisem oraz specyfikacją jego wykonawcy?

Generalnie narzędzia do weryfikacji i walidacji można podzielić na cztery kategorie³⁹³:

³⁹² Obserwacja i pomiar dotyczą podstawowych i istotnych wskaźników i mierników logistycznych, które oceniają: sprawność czynności logistycznych, usługi dostawcze własne i obce, czas przebiegu czynności logistycznych, koszty według różnych podziałów itp.

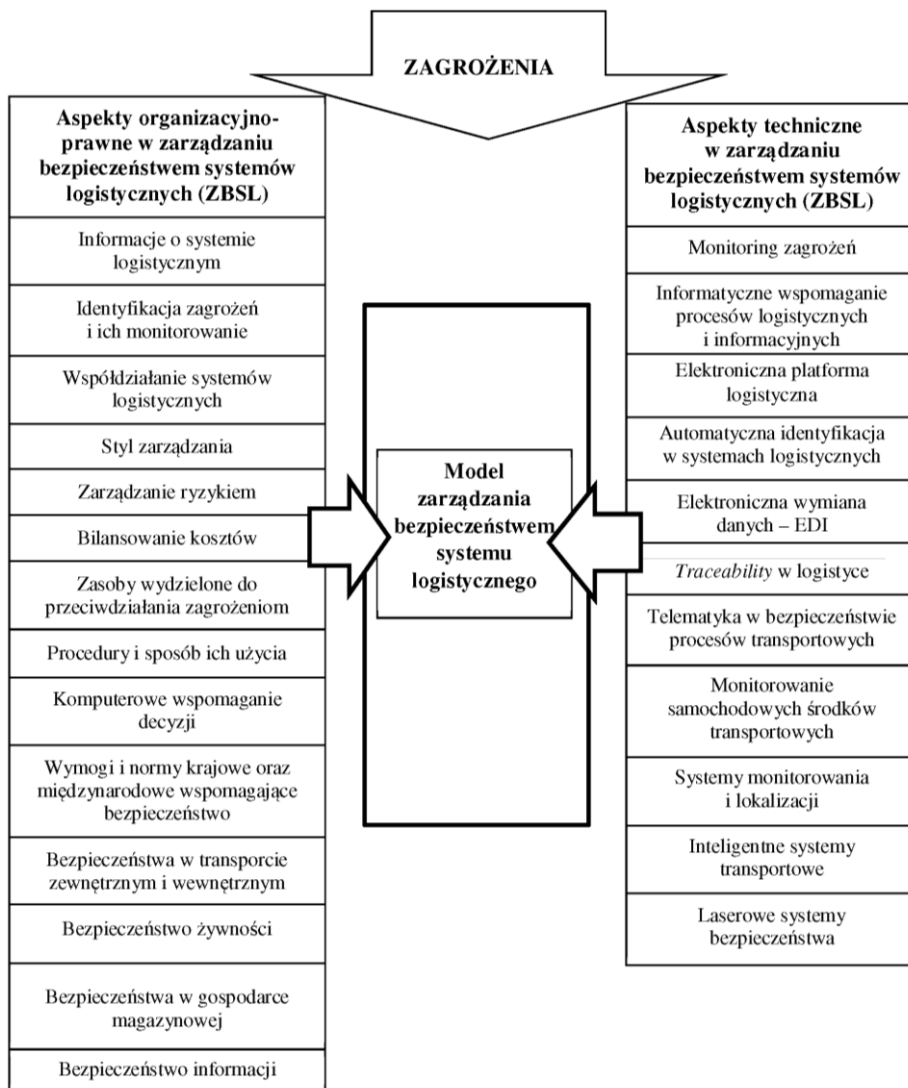
³⁹³ M. Karkula, *Weryfikacja i walidacja dynamicznych modeli symulacyjnych procesów logistycznych*, [w:] *Logistyka* 2012/2, s. 719.

- 1) nieformalne – weryfikacja i walidacja modelu odbywa się bez sformalizowanych narzędzi matematycznych;
- 2) formalne – wykorzystanie technik z tej grupy polega na badaniu poprawności modelu z wykorzystaniem narzędzi matematycznych;
- 3) statyczne – służą do walidacji modelu konceptualnego oraz prawidłowości translacji na model komputerowy, należą do nich analizy przepływu danych, analizy składni i semantyki modelu;
- 4) dynamiczne – wymagają „uruchomienia” modelu i analizy jego dynamicznego zachowania; ta grupa metod jest szczególnie ważna w przypadku walidacji modeli procesów i systemów logistycznych.

Walidacja i weryfikacja modelu symulacyjnego nie są procesami jednostkowymi i nie stanowią wyraźnie wyodrębnionego etapu – należy je traktować jako proces ciągły, zachodzący w trakcie cyklu modelowania. Etap walidacji i weryfikacji modelu jest integralnie związany z każdym z poprzednich etapów konstruowania modelu zarządzania bezpieczeństwem systemu logistycznego. Powinien odbywać się nie tylko po zakończeniu całej procedury, ale w jego wszystkich etapach konstruowania modelu. Przy weryfikacji modelu istotnym elementem jest określenie kryteriów, na bazie których będzie można ocenić, czy warunki zgodności są spełnione, czy nie. Pozytywny wynik oceny kończy proces budowy MZBSL, natomiast wynik negatywny powoduje powrót do wcześniejszych etapów budowy modelu.

Celem tworzenia modelu badawczego jest pozyskanie wiedzy w drodze identyfikacji elementów, relacji łączących elementy wybranych systemów różnych obszarów badawczych oraz poznanie wpływu jaki wywierają na zarządzanie bezpieczeństwem systemów logistycznych. Nieskończenie wiele czynników oddziałuje na obiekty (systemy, podsystemy) i sprawia, że niemożliwe jest zbudowanie modelu z uwzględnieniem wszystkich możliwych oddziaływań wewnętrznych, jak i zewnętrznych. W modelu ograniczamy ilość „połączeń” do tych, których wpływ na zachowanie się obiektu (systemu) jest istotny dla celu prowadzonej analizy.

Zaprezentowany model został przedstawiony w formie modelu ikonicznego, jako graficzna prezentacja analizowanych obszarów badawczych. Ujęcie takie pozwala dostrzec sens wszystkich obserwowanych elementów oraz ułatwia poznanie wewnętrznej organizacji obszarów badawczych. Możliwość wyobrażenia sobie pewnej struktury prowadzonych badań jest podstawowym krokiem w procesie rozwiązywania założonego problemu. Zbudowany model badawczy przedstawia istniejące zależności i relacje pomiędzy poszczególnymi elementami: obszarami badawczymi, zbiorem metod i narzędzi badawczych oraz efektami przeprowadzonych badań.



Rys. 6.13. Model zarządzania bezpieczeństwem systemu logistycznego

Źródło: opracowanie własne.

W czasie modelowania należy pamiętać, że:

- uproszczenie MZBSL może spowodować, że nie osiągniemy założonych rezultatów;
- skomplikowanie spowoduje, że model nie da się wdrożyć w praktyce.

Modelowanie można określić jako próbę wyrażenia za pomocą specjalnej notacji graficznej najważniejszych cech rozwijanego systemu oraz jego otoczenia.

Do zidentyfikowanych obszarów badawczych, omówionych i przeanalizowanych w zarządzaniu bezpieczeństwem systemu logistycznego należą:

- systemy logistyczne organizacji;
- zagrożenia dla systemów logistycznych;
- komputerowe wspomaganie decyzji;
- wymagania norm narodowych w bezpieczeństwie systemów logistycznych;
- technologie informatyczne wspomagające przepływ informacji w systemach logistycznych;
- zagrożenia dla systemów informatycznych;
- zagrożenia dla środowiska;
- zagrożenia dla żywności;
- bezpieczeństwo w transporcie i gospodarce magazynowej.

Charakterystyka poszczególnych obszarów badawczych oraz relacji występujących pomiędzy nimi, ukazana w modelu, stanowi przyczynek do dalszych badań, zmierzających do identyfikacji czynników wpływających na zapewnienie akceptowalnego poziomu bezpieczeństwa systemów logistycznych. Poziom bezpieczeństwa systemu logistycznego wyznacza wiele parametrów, które można opisać w sposób ilościowy i jakościowy, tworząc system mierników prostych i złożonych.

Opracowany model badawczy został przedstawiony na rys. 6.13, który w swojej istocie jest złożony, wielowymiarowy, dynamiczny. Zaprojektowanie takiego systemu jest trudne i tylko szerokie wykorzystanie narzędzi teoretycznych wspartych technologiami informatycznymi oraz wynikami badań prowadzonych na funkcjonujących systemach logistycznych pozwolą zbudować założony model, który uwzględni cele poznawcze i użytkowe.

Wyniki badań zaprezentowane w rozdziale 6.2 pokazały, że w funkcjonujących systemach logistycznych występują niedomagania. I tak np.:

- ponad 30% firm nie posiada wdrożonych podstaw prawnych w obszarze zarządzania bezpieczeństwem systemów logistycznych (tabela 6.11);
- 25% firm nie zapewnia zgodności funkcjonowania podmiotu z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie kryzysowe (tabela 6.14);
- ponad 40% firm nie identyfikuje struktury kosztów (strat) zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego (tabela 6.19), w tym 17% dużych i 15% średnich (wykres 6.18);
- 32% firm nie posiada opracowanych procedur zarządzania ryzykiem utraty ciągłości działania (tabela 6.27), w tym 12% dużych i 11% średnich przedsiębiorstw;
- w 30% nie jest znana struktura firmy pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego (tabela 6.32), w tym w 16% dużych i 11% małych przedsiębiorstw (wykres 6.30);

- w 28% firm nie ma osoby odpowiedzialnej za organizację i funkcjonowanie bezpieczeństwa systemu logistycznego (tabela 6.38), w tym w 13% dużych i 12% małych przedsiębiorstw (wykres 6.39);
- 35% firm nie posiada wdrożonych procedur współdziałania z otoczeniem zewnętrznym w celu efektywnego zarządzania bezpieczeństwem systemu logistycznego.

ZAKOŃCZENIE

Monografia *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne* swoją strukturą, metodologią, obszarem badań, przedmiotem i podmiotem badań w pełni wpisuje się w dyscyplinę nauki o bezpieczeństwie. Dotyczy bezpieczeństwa gospodarczego (jednej z czterech podstawowych dziedzin bezpieczeństwa narodowego³⁹⁴) w takich sektorach, jak: transportowy, infrastruktury (gospodarki magazynowej), środowiska naturalnego, żywnościowego, podmiotów produkcyjnych i usługowych.

W sposób kompleksowy, a jednocześnie syntetyczny są omawiane w opracowaniu związki, zależności i relacje między istotą działań gospodarczych w sferze bezpieczeństwa a ochroną podmiotów oraz materialnych zasobów gospodarczego potencjału bezpieczeństwa narodowego przed zagrożeniami oraz wsparcie działania podsystemów operacyjnych systemu bezpieczeństwa narodowego. Jest to możliwe, między innymi, dzięki instytucjom i podmiotom zmierzającym do wzmocnienia bezpieczeństwa gospodarczego, które swe działania opierają na **logistyce** sprawnej, skutecznej, nowoczesnej, a nade wszystko odpornej na wszelkie zakłócenia i zagrożenia.

Istota monografii sprowadza się do realizacji głównego problemu badawczego poprzez poznanie nieznanych lub mało znanych właściwości, cech badanych obiektów, przedmiotów, zdarzeń, procesów, faktów zapewniających pożądaną poziom bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego w kontekście aspektów logistycznych.

Określenie domen, zagrożeń, warunków prawnych, organizacyjnych, technicznych funkcjonowania bezpieczeństwa systemów logistycznych usprawniających realizację funkcji zarządzania bezpieczeństwem gospodarczym pozwoliło zrealizować cel główny, szczegółowe, aplikacyjne, określone we „Wstępie” opracowania.

Monografia *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne*, poddając analizie uwarunkowania funkcjonalne (pragmatyczne) powoduje, że mamy do czynienia z praktyką społeczną i badaniami stosowanymi. Zaproponowane narzędzia ułatwiają zapobieganie, przygotowanie, reagowanie na zagrożenia procesów logistycznych, a opracowany model zarządzania bezpieczeństwem systemów logistycznych pozwala przyczynić się do likwidacji luk, niedociągnięć i dysfunkcyjności w systemie bezpieczeństwa gospodarczego.

Opracowanie dostarcza rzetelnych danych o zagrożeniach, o stanie bezpieczeństwa ważnych działów gospodarki narodowej i jednocześnie

³⁹⁴ *Biała Księga Bezpieczeństwa Narodowego z 2013 roku*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, s. 19.

w oparciu o wiarygodne informacje zaleca podjęcie działań zaradczych i praktycznych. Owe działania, ściśle związane z bezpieczeństwem, zostały ujęte w trzech kategoriach: przedmiotowym, podmiotowym i funkcjonalnym, co pozwoliło potwierdzić sformułowaną hipotezę: *z uwagi na fakt rosnącej liczby stwierdzonych naruszeń bezpieczeństwa, istnieje potrzeba zmian w systemie zarządzania bezpieczeństwem logistycznym, z wiodącą rolą instytucjonalnych rozwiązań opartych o przepisy prawa, standardów i ich korelacji z wewnętrznymi uregulowaniami*. W zweryfikowaniu hipotezy niezwykle pomocne okazały się wyniki badań zawarte w podrozdziale 6.2, które pokazały niedomagania w zarządzaniu bezpieczeństwem logistycznym na rzecz podmiotów bezpieczeństwa.

W wymiarze podmiotowym są skierowane do ważnych, wybranych sektorów gospodarczych, takich jak: transport (samochodowy, kolejowy), infrastruktura magazynowa, ochrona żywności i środowiska, podmiotów produkcyjnych oraz usługowych. W tym kontekście oznacza to gwarancję funkcjonowania tych, którzy realizują działania w ramach systemów logistycznych.

W wymiarze przedmiotowym to pewność realizowanych zadań w ramach systemów logistycznych przez transport, gospodarkę magazynową. To również zapewnienie bezpieczeństwa żywności oraz ochrona środowiska. Obejmują one realizację i zaspokojenie takich obszarów, jak: przetrwanie, dostosowanie się do nowych warunków, niezależność, wywiązywanie się z nałożonych i oczekiwanych zadań, pewność realizacji przedsięwzięć na rzecz podmiotów bezpieczeństwa.

Funkcjonalny wymiar ujęty jest dwuaspektowo. Z jednej strony to bezpieczeństwo systemów logistycznych gwarantujących pewność i niezawodność przepływu strumienia rzeczowego, usług i informacji w ramach łańcuchów dostaw. Natomiast drugi wymiar to stabilizacja funkcjonowania i rozwój logistyki w określonych organizacjach gospodarczych ze względu na pożądany poziom bezpieczeństwa.

W monografii zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego zostało przedstawione w relacjach i zależnościach związanych z: bezpieczeństwem systemów logistycznych, zagrożeniami, bezpieczeństwem transportu, gospodarką magazynową, bezpieczeństwem żywnościowym, ekologią. Przedstawiona została analiza zagrożeń w transporcie samochodowym, kolejowym, gospodarce magazynowej w formie tabel i wykresów, na których mamy obraz ilości negatywnych zdarzeń i wielkości poniesionych strat, zarówno materialnych, jak i ludzkich (zabitych, rannych). W celu minimalizacji tych zdarzeń, w opracowaniu zostały zaprezentowane rozwiązania organizacyjne, prawne, techniczne.

Szczególnie wiele miejsca poświęcono technologiom wspomagania zarządzania bezpieczeństwem systemów logistycznych, których zastosowanie ma wpływ na sprawność, skuteczność realizowanych procesów gospodarczych

w systemie bezpieczeństwa narodowego, na korzyść podmiotów bezpieczeństwa. Zaprezentowane rozwiązania informatyczne to nie tylko nowoczesność, efektywność, wymierne korzyści organizacyjne, ekonomiczne, ale również bezpieczna logistyka.

Zastosowanie np. telematyki w transporcie to inteligentna droga, inteligentny pojazd, czyli pojazd wyposażony w urządzenia utrzymujące ciągłą, szczególnie bezprzewodową, wymianę informacji z urządzeniami zainstalowanymi przy trasach transportowych oraz inteligentne centrum zarządzania.

Z kolei *traceability* to między innymi możliwość identyfikacji odpowiedzialności, możliwość prześledzenia drogi produktu, od momentu jego powstania z surowców, do momentu, gdy trafi on do ostatniego klienta w łańcuchu dostaw, a jest to szczególnie ważne, gdy mamy do czynienia z produktami szybko zbywalnymi, produktami szybko rotującymi (*FMCG, fast-moving consumer goods*).

Bezpieczny magazyn to ten, w którym wykorzystuje się automatyczną identyfikację (kody kreskowe, elektroniczne oznakowanie produktu) w obrocie zapasami (rezerwami), a także dobre zabezpieczenie fizyczne wsparte elektroniką (np. system sygnalizacji kradzieży, system kontroli dostępu i rejestracji czasu pracy, system kontroli wartowników).

Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego, w aspekcie logistycznym jest niemożliwe bez aktualnej, pełnej, wiarygodnej i bezpiecznej informacji. Przyjęto, że spełnienie warunków pożądanej wysokiej jakości informacji stanowi podstawę efektywnego funkcjonowania systemów zarządzania.

Na szczególną uwagę zasługuje ostatni rozdział monografii, w którym wykorzystano wyniki badań empirycznych. Badania dotyczyły bezpieczeństwa logistyki, w kontekście zarządzania bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego.

Obszarami badawczymi były systemy logistyczne organizacji, zagrożenia dla efektywnego funkcjonowania systemów logistycznych, komputerowe wspomaganie decyzji ze szczególnym uwzględnieniem potrzeb zarządzania kryzysowego, wymagania i normy narodowe w bezpieczeństwie systemów logistycznych, technologie informatyczne wspomagające przepływ informacji w systemach logistycznych, zagrożenia dla systemów informatycznych, bezpieczeństwo w transporcie, żywności, gospodarce magazynowej, ekologii.

Ważną częścią rozważań monografii *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne* jest ujęcie utylitarne. Wskazano, opisano, oceniono główne problemy związane z praktycznym jej wykorzystaniem, poprzez zaakcentowanie istoty problemu w kilku obszarach.

Po pierwsze – bezpieczeństwo gospodarcze w systemie bezpieczeństwa narodowego należy analizować w kontekście wymogów stawianych przez współczesne systemy logistyki. Takie podejście jest wyrazem holistyczno-

systemowego ujęcia problemowych obszarów wiedzy bezpieczeństwa gospodarczego (ekonomicznego) i logistyki w systemie bezpieczeństwa narodowego. Zaprezentowana monografia stanowi kompleksowe połączenie bezpieczeństwa gospodarczego i działań logistycznych w systemie bezpieczeństwa narodowego.

Monografia może być źródłem informacji i wiedzy dla studentów kierunku kształcenia bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, inżynieria bezpieczeństwa i logistyka, słuchaczy studiów podyplomowych, a także dla instytucji zajmujących się bezpieczeństwem oraz organizacji (instytucji) uczestniczących w logistycznym zabezpieczeniu podmiotów bezpieczeństwa.

Po drugie – zaprezentowana metodologia identyfikacji zagrożeń systemów logistycznych, rozpoznania podatności na powstanie sytuacji niebezpiecznych w takich sektorach bezpieczeństwa gospodarczego, jak np. transport (samochodowy i kolejowy), gospodarka magazynowa, żywność, ekologia pozwala na racjonalizację wyboru środków (organizacyjnych, prawnych, technicznych) zapewniających funkcjonowanie (zgodnie z przeznaczeniem) systemu w niebezpiecznym środowisku.

Po trzecie – zaprezentowany model zarządzania bezpieczeństwem systemów logistycznych na potrzeby logistyki bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego został przedstawiony w formie modelu, jako graficzna prezentacja analizowanych obszarów badawczych. Ujęcie takie pozwala dostrzec sens aspektów organizacyjno-prawnych i technicznych w zarządzaniu bezpieczeństwem systemów logistycznych oraz ułatwia poznanie wewnętrznej organizacji obszarów badawczych w kompilacji z zewnętrznym otoczeniem. Charakterystyka poszczególnych obszarów badawczych oraz relacji występujących pomiędzy nimi, ukazana w modelu, stanowi o kierunku dalszych badań zmierzających do identyfikacji czynników wpływających na zapewnienie akceptowalnego poziomu bezpieczeństwa systemów logistycznych.

Po czwarte – z praktycznego punktu widzenia, godne uwagi i zastosowania są wyniki badań przeprowadzonych w obszarze bezpieczeństwa systemów logistycznych, w wybranych podmiotach (organizacjach, firmach) bezpieczeństwa za pomocą kwestionariusza ankiety, który zawierał 18 pytań, w tym 16 zamkniętych i 2 otwarte. Kwestionariusze zostały wysłane do 168 różnych firm, z czego zwrotnie otrzymano 92 (4 z mikro, 24 z małych, 29 ze średnich i 35 z dużych). Dodatkowo, w celu zweryfikowania wyników badań, przeprowadzono pięć rozmów z ekspertami, logistykami dużych firm prywatnych i państwowych, w oparciu o materiały zgromadzone w kwestionariuszu.

W badanych firmach, jak wynika z udzielonych odpowiedzi, największą uwagę przywiązuje się do monitorowania funkcjonowania warunków prawnych i organizacyjnych wspomagających zarządzanie zdarzeniami kryzysowymi w obszarze logistyki.

Wymagania prawne są bezwzględnie realizowane, a niezbędne rozwiązania organizacyjne są sukcesywnie wdrażane w życie. Większość funkcjonujących

rozwiązań, w obszarze bezpieczeństwa systemów logistycznych, jest wynikiem analiz zagrożeń przeprowadzonych przez interdyscyplinarne zespoły pracowników, a niektóre rozwiązania są wynikiem negatywnych zdarzeń, zewnętrznych i wewnętrznych, które wywołały stany czasowych trudności w organizacji (inne niż kryzys). Monitorowaniem zajmują się komórki (osoby) odpowiedzialne za bezpieczeństwo funkcjonowania systemu logistycznego. Wszystkie działania w ramach firmy koordynuje kierownictwo najwyższego szczebla wspomagane przez wewnętrznych i zewnętrznych audytorów (włącznie z korporacyjnymi).

Z rozmów dotyczących bezpieczeństwa systemów logistycznych z ekspertami wynika, że najczęściej uwagi poświęcano zagrożeniom, które wynikają z: makrooczenia organizacji (np. sytuacji gospodarczej w kraju, polityki płacowej, podatkowej, emerytalnej, demograficznej); mikrooczenia organizacji (np. niespójne kryteria wyboru dostawców, brak kontroli nad pracownikami postępującymi nieetycznie – wykradanie danych, informacji, wiedzy, brak dostępności fachowego personelu, brak możliwości pozyskania komponentów do wytwarzania, brak buforowego zapasu); postępowania człowieka – bez złych intencji (niezawodność systemów, błędy w oprogramowaniu, awarie produktów, instalacji, zasilania, serwera, konstrukcji budynków, regałów wysokiego składowania) i związanego ze złymi intencjami (niezadowoleni pracownicy, nieuczciwa konkurencja); katastrof – pożary, huragany, awarie wpływające negatywnie na zdrowie człowieka i środowisko.

W mniejszym stopniu zajmowano się obszarami związanymi z zagrożeniami naturalnymi, włącznie ze zmianami klimatycznymi, wynikającymi np. z lokalizacji magazynu i infrastruktury drogowej lub wynikającymi z niezadowolenia pracowników (np. strajk lub inna forma konfliktu z pracodawcą).

Badania wykazały również, co jest bardzo istotne dla nauki i praktyki, że nie wszystkie podmioty mają wdrożone procedury dotyczące zarządzania bezpieczeństwem systemów logistycznych, a tym samym nie są w stanie zapewnić bezpieczną i niezawodną realizację zadań z zakresu bezpieczeństwa gospodarczego. Argumentami potwierdzającymi to stwierdzenie są liczby wykazane w tabelach i wykresach podrozdziału 6.2, które pokazują, że np. wiele podmiotów nie identyfikuje i analizuje struktury kosztów (strat) zabezpieczenia przed skutkami zagrożeń, brakuje osób (komórek) odpowiedzialnych za bezpieczeństwo funkcjonowania systemu logistycznego, nie prowadzi się odpowiednich szkoleń.

BIBLIOGRAFIA

A. Publikacje zwarte

A Dictionary of the Social Sciences, London 1964.

Arway A., *Supply Chain Security: A Comprehensive Approach*, CRC Press, Boca Raton 2013.

Automatyczna identyfikacja w systemach logistycznych, red. nauk. S. Kwaśniewski, Zajac P., PW, Wrocław 2004.

Ayers J., *Handbook of Supply Chain Management, Second Edition*, Auerbach Publications, Boca Raton 2006.

Banaszak Z., Kłos S., Mleczek J., *Zintegrowane systemy zarządzania*, PWE, Warszawa 2011.

Baraniecka A., *ECR Efficient Consumer Response, Łańcuch dostaw zorientowany na klienta*, IliM, Poznań 2004.

Bezpieczeństwo – ujęcie kompleksowe, red. Z. Grzywna, Wyd. Wyższej Szkoły Zarządzania Marketingowego i Języków Obcych w Katowicach, Katowice 2012.

Bezpieczeństwo ekonomiczne. Teoria i praktyka, red. Z. Kołodziejak, Wyd. Uniwersytetu Łódzkiego, Łódź 1986.

Bezpieczeństwo ekonomiczne. Wyzwania dla zarządzania państwem, red. K. Raczkowski, Ofic. wyd. Wolters Kluwer, Warszawa 2012.

Bezpieczeństwo międzynarodowe. Teoria i praktyka, red. K. Żukrowska, M. Gracik, Wyd. SGH, Warszawa 2006.

Bezpieczeństwo państwa, red. nauk. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza Aspra-Jr, Warszawa 2009.

Bichou K., Bell M., Evans A., *Risk Management in Port Operations, Logistics and Supply Chain Security*, Informa Law from Routledge, London 2007.

Bielecki W.T., *Informatyzacja zarządzania*, PWE, Warszawa 2001.

Boguszewski P., *Globalny raport konkurencyjności 2015-16*, Światowego Forum Gospodarczego, Warszawa, 30 września 2015 r., Departament Stabilności Finansowej.

Bossak J.W., *Systemy gospodarcze a globalna konkurencja*, SGH, Warszawa 2006.

Bozarth C.B., Handfield R.B., *Wprowadzenie do zarządzania operacjami i łańcuchem dostaw*, Helion, Gliwice 2007.

Bragdon C., *Transportation Security*, Butterworth-Heinemann, Oxford 2008.

Brilman J., *Nowoczesne koncepcje i metody zarządzania*, PWE, Warszawa 2002.

Brzeziński M., *Logistyka wojskowa*, Bellona, Warszawa 2005.

Brzeziński M., *Systemy w logistyce*, WAT, Warszawa 2007.

Budnikowski A., *Międzynarodowe stosunki gospodarcze*, PWE, Warszawa 2006.

Burges D., *Cargo Theft, Loss Prevention, and Supply Chain Security*, Elsevier Inc., Burlington 2012.

Christopher M., *Logistyka i zarządzanie łańcuchem dostaw*, Polskie Centrum Doradztwa Logistycznego, Warszawa 2000.

Ciecińska B., Łunarski J., Perłowski R., Stadnicka K., *Systemy zarządzania bezpieczeństwem w przedsiębiorstwie*, PRz, Rzeszów 2006.

Cieślarczyk M., *Psychospołeczne i organizacyjne elementy bezpieczeństwa i obronności*, AON, Warszawa 1998.

Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wyd. Akademii Podlaskiej, Siedlce 2009.

Cook T., *Managing Global Supply Chains: Compliance, Security, and Dealing with Terrorism*, Auerbach Publications, Boca Raton 2008.

Coyle J.J., Bardi E.J., Langly Jr C., *Zarządzanie logistyczne*, PWE, Warszawa, 2002.

Dębczak A., *System zabezpieczenia logistycznego komponentu wojsk lądowych w przyszłych operacjach*, AON, Warszawa 2013.

Dubos R., *Pochwała różnorodności*, Warszawa 1986, s. 197.

Dumnicki R., Kasprzyk A., Kozłowski M., *Analiza i projektowanie obiektowe*, HELION, Gliwice 1998.

Dworecki S., Berny J., *Logistyka racjonalnego działania*, Reprograf, Radom 2005.

Dziurny A., *Model bezpieczeństwa ekonomicznego Rzeczypospolitej Polskiej w warunkach globalizacji i regionalizacji zagrożeń oraz wyzwań cywilizacyjnych*, AON, Warszawa 2012.

Edukacja obronna społeczeństwa, red. B. Wiśniewski, W. Fehler, Wyd. NWSP, Białystok 2006.

Edwards F., Goodrich D., *Introduction to Transportation Security*, CRC Press, Boca Raton 2012.

Ejdys J., Lulewicz A., Obolewicz J., *Zarządzania bezpieczeństwem w przedsiębiorstwie*, PB, Białystok 2008.

Ekonomika bezpieczeństwa państwa średniej wielkości, Teoria i praktyka, red. S. Kurinia i M. Krč, Warszawa-Brno 2000.

Ekonomika obrony, red. W. Stankiewicz, AON, Warszawa 1994.

Ekonomika wojskowa i logistyka wojskowa – podobieństwa i różnice, Materiały z sympozjum, AON, Warszawa 1998.

Encyklopedia naukowa PWE, PWE, Warszawa 1986.

Eßig M., Hülsmann M., Kern E.-M., Klein-Schmeink S., *Supply Chain Safety Management Security and Robustness in Logistics*, Springer, Berlin 2013.

Evangelista P., McKinnon A., Sweeney E., Esposito E., *Supply Chain Innovation for Competing in Highly Dynamic Markets: Challenges and Solutions*, IGI Global, Hershey 2011.

Ficoń K., *Logistyka kryzysowa Procedury Potrzeby Potencjał*, BEL studio, Warszawa 2015.

Ficoń K., *Logistyka ekonomiczna. Procesy logistyczne*, Bel Studio Sp. z o.o., Warszawa 2008.

Ficoń K., *Procesy logistyczne w przedsiębiorstwie*, Impuls Plus Consulting, Gdynia 2001.

Foltys J., *Outsourcing w przedsiębiorstwach sektora MŚP, Scenariusz aplikacyjny*, wydawnictwo UŚ, Katowice 2012.

Frejtag-Mika E., Kołodziejak Z., Putkiewicz W., *Bezpieczeństwo ekonomiczne we współczesnym świecie*, Wyd. Politechniki Radomskiej im. K. Pułaskiego, Radom 1996.

Gawliczek P. *Zagrożenia asymetryczne*, AON, Warszawa 2001.

Glennon John C., *Roadway Safety and Tort Liability*, Lawyer and Judges Publishing Co., 2004.

Greniewski H., *Cybernetyka niematematyczna*, Warszawa 1971.

Grosset R., Mochnaczewski P., Wiatr S., *Zagrożenie i poczucie bezpieczeństwa. Oceny mieszkańców dużych miast*, WSZiP, Warszawa 2009.

Gryz J., *Zarys podstaw teorii bezpieczeństwa*, AON, Warszawa 2010.

Gryz J., *Zarys teorii bezpieczeństwa*, AON, Warszawa 2010.

Handbook for Defining and Setting up a Food Security Information and Early Warning System (FSIEWS), Food And Agriculture Organization Of The United Nations, Rome 2000.

Hitch C.J., McKean R.N., *Ekonomika obrony w erze jądrowej*, Wyd. MON, Warszawa 1965.

Instrumenty zarządzania łańcuchem dostaw, red. nauk. M. Ciesielski. PWE, Warszaw 2009.

Jakubczak R., Flis J. (red.), *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i zagrożenia*, Warszawa 2006.

Janczak A., *ADR w spedycji i magazynie, składowanie i przewóz materiałów niebezpiecznych*, Zacharek – Dom Wydawniczy, Warszawa 2010.

Jaźwiński I., *Determinanty kształtowania polskiego bezpieczeństwa gospodarczego. Wybrane aspekty*, Przegląd Strategiczny 2001.

Jaźwiński I., Ważyńska-Fiok K., *Bezpieczeństwo systemów*, PWN, Warszawa 1993.

Jurkowska-Zeidler A., *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*, Ofic. wyd. Wolters Kluwer, Warszawa 2008.

Kaczmarek T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania. Business continuity management*, Difin, Warszawa 2009.

Kaczmarek T., *Zarządzanie zdywersyfikowanym ryzykiem w świetle badań interdyscyplinarnych*, WSZiM, Warszawa 2003.

Kaeo M., *Tworzenie bezpiecznych sieci*, MIKOM, Warszawa 2000.

Kiperska-Moroń D., Krzyżaniak S., *Logistyka*. Biblioteka Logistyka, Poznań 2009.

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System.* AON, Warszawa 2011.

Klatka K., *Konflikt i gra*, Warszawa 1972.

Klonowski Z.J., *Systemy informatyczne zarządzania przedsiębiorstwem, modele rozwoju i własności funkcjonalne*, Oficyna Wydawnicza PW, Wrocław 2004.

Kody kreskowe i inne globalne standardy w biznesie, red. nauk. E. Hałas, ILiM, Poznań 2012.

Kołodziński E., *Model Podstawowej Jednostki Organizacyjnej Systemu Bezpieczeństwa Kraju*, www.ptib.pl, 10.08.2014.

Kołodziński E., *Istota inżynierii systemów zarządzania bezpieczeństwem*, <http://www.uwm.edu.pl>.

Komorowski J., *Cele przedsiębiorstwa a rozwój gospodarczy. Ujęcie behawioralne*, SGH, Warszawa 2012.

Kompendium wiedzy o logistyce, red. nauk. E. Gołemska, Wydawnictwo Naukowe PWN, Warszawa Poznań, 2001.

Konieczny J., *Podstawy eksploatacji urzędzeń*, Warszaw 1975.

Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Wyd. Muza S.A., Warszawa 2002.

Kopczewski M., Tobolski M., Pasek D., *Bezpieczeństwo w transporcie materiałów niebezpiecznych*, [w:] *Logistyka 2013/6*.

Korzeń Z., *Ekologistyka*, Biblioteka Logistyka, Poznań 2001.

Koźmiński A., Piotrkowski W., *Zarządzanie, Teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa 1996.

Księżopolski K.M., *Bezpieczeństwo ekonomiczne*, Dom Wyd. ELIPSA, Warszawa 2011.

Księżopolski K.M., *Ekonomiczne zagrożenia bezpieczeństwa państw. Metody i środki przeciwdziałania*, Wyd. Kolor Plus, Warszawa 2004.

Kurasiński Z., Pawlisiak M., *Logistyka profesjonalnej armii*, WAT, Warszawa 2013.

Kurek S., Kurek S.T., Stachowiak Z., *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej*, AON, Warszawa 2004.

Leksykon pokoju, Krajowa Agencja Wydawnicza, Warszawa 1987.

Liderman K., *Podręcznik administratora bezpieczeństwo teleinformatyczne*, MIKOM, 2003.

Logistyka dystrybucji, pod red. K. Rutkowskiego, Difin, Warszawa 2001.

Logistyka w biznesie, red. nauk. M Ciesielski, PWE, Warszawa 2006.

Logistyka w przedsiębiorstwie, przewodnik do ćwiczeń, red. G. Radziejowska, Gliwice 2001.

Lotko A., *Zarządzanie relacjami z klientem*, Politechnika Radomska, Radom 2003.

Majewski J., *Informatyka dla logistyki*, ILiM, Poznań 2002.

McDonald T., *Iowa's Traffic Safety Analysis Manual*, Iowa Department of Transportation, Iowa 2012.

Michałowski S., *Bezpieczeństwo ekonomiczne w stosunkach wschód-zachód*, PISM, Warszawa 1990.

Międzynarodowa Konwencja o Bezpieczeństwie Życia na Morzu, 1974, Gdańsk 2002, Polski Rejestr Statków.

Mokrzyszczak H., *Logistyka podstawy procesów logistycznych*, WIG, Białystok 1998.

Molková T., *Hodnocení kvality v dopravním a přepravním procesu*, DF JP Pardubice 2009.

Myczkowski S., *Człowiek. Przyroda. Cywilizacja. Kształtowanie zasobów przyrody oraz ochrona biosfery*, PWN, Warszawa 1976.

Najder J., *Transport międzynarodowy*, PWE, Warszawa 2012.

Nauczyciele i mistrzowie ekonomii i logistyki – Wacław Stankiewicz. Tom I – Ekonomia instytucjonalna wobec problemów bezpieczeństwa i obronności, red. A. Dziurny i S.T. Kurek, AON, Warszawa 2015.

Nowak E., *Logistyka w sytuacjach kryzysowych*, AON, Warszawa 2005.

Nowak E., *Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych*, AON, Warszawa 2007.

Olszewski T., *Geografia rolnictwa Polski*, PWE, Warszawa 1985.

Paszkowski S., *Podstawy teorii systemów i analizy systemowej*, WAT, Warszawa 1999.

Paul T.V., Norrin M. Ripsman, *Globalization and the National Security State*, Oxford University Press, Oxford 2010.

Piasecki S., *Teoria organizacji w świetle analizy systemowej jako teoria języka problemowo zorientowanego*, [w:] Prace IBS PAN, Warszawa 1982.

Pisz I., Łapuńko I., *Zarządzanie projektami w logistyce*, Difin, Warszawa 2015.

Pisz I., Sęk T., Zielecki W., *Logistyka w przedsiębiorstwie*, PWE, Warszawa 2013.

Podręcznik zarządzania cyklem projektu, Ministerstwo Gospodarki i Pracy, Warszawa 2004.

Podstawy bezpieczeństwa współczesnego państwa (podmiotu). Implikacje, red. J. Pawłowski, AON, Warszawa 2015.

Podstawy zarządzania operacyjnego, pod red. Z. Jasińskiego, Oficyna Ekonomiczna, Kraków 2005.

Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2006.

Polcikiewicz Z., *Teoria bezpieczeństwa*. WSOWL, Wrocław 2012.

Pszczołowski T., *Mała encyklopedia prakseologii i teorii organizacji*, Warszawa 1978.

Pułaska-Turyńska B., *Statystyka dla ekonomistów*, Warszawa 2011.

Pyza D., *Modelowanie systemów przewozowych w zastosowaniu do projektowania obsługi transportowej podmiotów gospodarczych*, PW, Warszawa 2012.

Rączkowski B., *BHP w praktyce*, ODiDK, Gdańsk 2010.

Rączkowski K., *Zarządzanie wiedzą w administracji celnej w systemie bezpieczeństwa ekonomiczno-społecznego*, Wyd. Difin, Warszawa 2010.

Rushton A., Croucher P., Baker P., *Handbook of Logistics and Distribution Management (4th Edition)*, Kogan Page Publishers.

Rutkowski C., *Bezpieczeństwo i obronność: strategie – koncepcje – doktryny*, AON, Warszawa 1995.

Samuelson P.A., Nordhaus W.D., *Ekonomia 2*, PWN, Warszawa 1998.

Schetina E., Green K., Carlson J., *Bezpieczeństwo w sieci*, HELLION, Gliwice 2002.

Sheffi Y., *Supply chain management under the threat of international terrorism*, International journal of logistics management, Emerald Group Publishing, Bingley 2001.

Sienkiewicz P., *25 wykładów*, AON, Warszawa 2015.

Sienkiewicz P., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, AON, Warszawa 2008.

Sienkiewicz P., *Analiza systemowa, Podstawy i zastosowania*, Bellona Warszawa 1994.

Sienkiewicz P., *Inżynieria systemów kierowania*, PWE Warszawa 1998.

Sienkiewicz P., *Inżynieria systemów*, Warszawa 1983.

Sienkiewicz P., *Podstawy teorii systemów*, AON, Warszawa 1993.

Skowronek Cz., Sarjusz-Wolski Z., *Logistyka w przedsiębiorstwie*, PWE, Warszawa 2008.

Śladkowski S., *Bezpieczeństwo ekologiczne Rzeczypospolitej Polskiej*, Akademia Obrony Narodowej, Warszawa 2004.

Słownik języka polskiego, red. M. Szymczak, PWN, Warszawa 1978, t. 1 i 3.

Słownik terminologii logistycznej, red. nauk. M. Fertsch, ILiM, Poznań 2006.

Słownik terminów z zakresu bezpieczeństwa narodowego, AON, Warszawa 2002.

Słownik wyrazów obcych, PWN, Warszawa 2001.

Słownik wyrazów obcych, red. J. Tokarski, PWN, Warszawa 1980.

Słownika terminów z zakresu psychologii dowodzenia i zarządzania, AON, Warszawa 2000.

Sokołowski G., *Traceability – bezpieczeństwo i śledzenie przepływu produktów w łańcuchach dostaw, w oparciu o standardy GSI i wymagania UE*, ILiM, Poznań 2014.

Sołtysik M., *Zarządzanie logistyczne*, Akademia Ekonomiczna, Katowice, 2000.

Spółeczeństwo i polityka. Podstawy nauk politycznych, red. K.A. Wojtaszczyk, W. Jakubowski, Ofic. wyd. ASPRA-JR, Warszawa 2003.

Stachowiak Z., *Teoria i praktyka mechanizmu ekonomicznego państwa. Ujęcie systemowe*, AON, Warszawa 2012.

Stachowiak Z., *Bezpieczeństwo żywnościowe Rzeczypospolitej Polskiej na przełomie XX i XXI wieku. Aspekt obronno-ekonomiczny*, AON, Warszawa 1995.

Stachowiak Z., *Teoria i praktyka mechanizmu bezpieczeństwa ekonomicznego państwa. Ujęcie instytucjonalne*, AON, Warszawa 2012.

Stachowiak Z., *Bezpieczeństwo żywnościowe Rzeczypospolitej Polskiej. Aspekt obronno-ekonomiczny i społeczny*, AON, Warszawa 1995.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, ISP PAN, Warszawa 1996.

Staniszewski R., *Cybernetyka systemów projektowania*, Warszawa 1981.

Stankiewicz W., *Bezpieczeństwo narodowe a walki niebrojne*, Studium, AON, Warszawa 1991.

Strategie łańcuchów dostaw, red. nauk. M. Ciesielski, J. Długosz, PWE, Warszawa 2010.

Świniarski J., *O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych*, Wyd. ULMAK, Warszawa-Pruszków 1997.

Symulacyjny model gospodarki Polski, red. nauk. Gutenbaum J., Inkelman M., PAN, IBS, Warszawa 1998.

Szmit M., Gusta M., Tomaszewski M., *101 zabezpieczeń przed atakami w sieci komputerowej*, Helion, Gliwice 2005.

Szmit M., Tomaszewski M., Lesiak D., Politowska I., *13 najpopularniejszych sieciowych ataków na twój komputer*, Helion, Gliwice 2008.

Szrejder J.A., *Równość, podobieństwo, porządek*, Warszawa 1975.

Szymonik A., *Ekonomika transportu dla potrzeb logistyka (i) Teoria i Praktyka*, Difin, Warszawa 2013.

Szymonik A., Bielecki M., *Bezpieczeństwo systemu logistycznego w nowoczesnym zarządzaniu*, Difin, Warszawa 2015.

Szymonik A., *Information Technologies in Logistics*, Lodz University of Technology, monographs 2012.

Szymonik A., *Informatyzacja zarządzania logistycznego*, Bellona, Warszawa 2005.

Szymonik A., *Logistyka jako system racjonalnego pozyskiwania wyrobów obronnych*, AON, Warszawa 2007.

Szymonik A., *Logistyka w bezpieczeństwie*, Difin, wydanie 2, Warszawa 2011.

Szymonik A., *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Difin, Warszawa 2011.

Szymonik A., *Systemy informatyczne w realizacji funkcji logistycznych*, WSK, Łódź 2006.

Szymonik A., *Technologie informatyczne w logistyce*, Placet, Warszawa 2010.

Szymonik A., *Zarządzanie dystrybucją*, WSOWL, Wrocław 2015.

Teska J., *Ekonomiczne implikacje bezpieczeństwa*, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2013.

Teska J., *Ekonomiczne implikacje bezpieczeństwa*, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2013.

Tompkins James A., Smith Jerry D., *The Warehouse management handbook, Second Edition*, Tompkins Press, Raleigh 1998.

Trejnis Z., *Nauki o bezpieczeństwie nową dyscypliną w dziedzinie nauk społecznych*, Studia Bezpieczeństwa Narodowego, red. B. Jagusiak, WAT, Warszawa 2011.

Trela A., *Zarządzanie logistyczne polskiej policji*, PŁ, Łódź 2011.

Twaróg J., *Mierniki i wskaźniki logistyczne*, IliM, Poznań 2006.

Tyrała P., *Zarządzanie kryzysowe*, wyd. A. Marszałek, Toruń 2003.

Urbanek A., *Państwo jako podmiot bezpieczeństwa – aspekty teoretyczne i praktyczne*, Acta Pomerania 4/2012.

Vademecum teleinformatyka II, Praca zbiorowa, wydanie specjalne Networkd, Wyd. IDG Poland S.A., Warszawa 2002.

Vademecum teleinformatyka III, IDG, Warszawa 2004.

Whitman M.E., Mattord H.J., *Reading and cases in the management of information security*, Thomson Course Technology, Boston 2006.

Wiąckowski S., *Ekologia ogólna*. Oficyna Wydawnicza Branta, Bydgoszcz 2008.

Wirkus M., Roszkowski H., Dostatni E., Gierulski W., *Zarządzanie projektem*, PWE, Warszawa 2014.

Witkowski J., *Zarządzanie łańcuchem dostaw*, PWE, Warszawa 2003.

Wolański W., *Ekologia człowieka. Ewolucja i dostosowanie biokulturowe*, PWN, Warszawa 2008.

Wronka J., *Transport kombinowany w aspekcie wymogów transportu zrównoważonego*, Wydawnictwo Naukowe Ośrodka Badawczego Ekonomiki Transportu, Warszawa-Szczecin 2002.

Współczesna logistyka – wybrane aspekty, red. W. Nyszk, AON, Warszawa 2013.

Współczesne Bezpieczeństwo. Perspektywa teoretyczno-metodologiczna, red. S. Jaczyński, M. Kubiak, M. Minkina, Wyd. Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Warszawa-Siedlce 2011.

Współczesne wyzwania polityki bezpieczeństwa – wybrane zagadnienia, red. M. Inicki i Z. Nowakowski, Wyd. Towarzystwo Naukowe Powszechne, Warszawa 2014.

Wstęp do informatyki gospodarczej, red. nauk. A. Rokicka-Broniatowska, SGH, Warszawa 2006.

Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa, red. A. Urbanek, Wyd. Społeczno-Prawne, Słupsk 2013.

Zarys ekonomiki bezpieczeństwa, red. J. Płaczek, AON, Warszawa 2009.

Zarzycki R., Imbierowicz M., Stelmachowski M., *Wprowadzenie do inżynierii ochrony środowiska. Ochrona środowiska naturalnego*, WNT, Warszawa 2007.

Zięba R., Zajac J., *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski*, Ekspertyza, Warszawa 2010.

Zieliński L., *BHP w magazynie*, Wydawnictwo Wiedza i Praktyka Sp. z o.o., Warszawa 2015.

Żółtowski B., Kwiatkowski K., *Zagrożone środowisko*, Wydawnictwa Uczelniane Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy, Bydgoszcz 2012.

Żukrowska K., *Bezpieczeństwo ekonomiczne*, Tekst przygotowany na panel *Problemy współczesnego wymiaru bezpieczeństwa*, zorganizowany przez Fundację Instytutu Lecha Wałęsy, Warszawa 16.12.2011 r.

B. Artykuły

Alminshid K., Omar M.N., *Detecting backdoor using stepping stone detection approach*, [w:]

Ayurzana O., Pumbuurei B., Hiesik Kim, *A study of hand-geometry recognition system*, [w:] Strategic Technology (IFOST), 2013 8th International Forum on, Volume 2, 2013.

Bartczak K., *Technologie informatyczne i telekomunikacyjne jako podstawa tworzenia systemów telematycznych w transporcie*, [w:] *Współczesne procesy i zjawiska w transporcie*, USz, Szczecin 2006.

Bendyk E., *Moloch miejski*, [w:] *Cywilizacja 2.0 Świat po rewolucji informatycznej*, wydanie specjalne, 8/2011.

Bentkowska-Senator K., Kordel Z., *Polski transport samochodowy w łańcuchach dostaw*, [w:] *Logistyka* 3/2012.

Berchmans D., Kumar S.S., *Optical character recognition*, [w:] *An overview and an insight*, Control, Instrumentation, Communication and Computational Technologies (ICCICT), International Conference on 2014.

Bi J., Liu B., Wu J., Shen Y., *Preventing IP source address spoofing*, [w:] *A two-level, state machine-based method*, Tsinghua Science and Technology, 2009, Volume 14, Issue 4.

Blumenthal K., *Generation and treatment of municipal waste*, [w:] *Eurostat: Statistics in Focus*, 31/2011. Eurostat, 2011.

Bolan C., *A Review of the Electronic Product Code Standards for RFID Technology*, [w:] *proceedings of the 7th International Network Conference: University of Plymouth, UK, 8-10 July 2008*.

Bonfatti F., *Gdy marzenia się spełniają – wizja platformy e-logistycznej*, [w:] *Logistyka* 2/2009.

Chao L., Li Qing, *Manufacturing Execution Systems (MES) assessment and investment decision study*, [w:] Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on, 2006, Volume 6.

Choraś R., *Retina recognition for biometrics*, [w:] Digital Information Management (ICDIM), 2012 Seventh International Conference on, 2012.

Choudhary K., Pandey U., Nayak M.K., Mishra D.K., *Electronic Data Interchange*, [w:] A Review, Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on, 2011.

Chow Harry K.H., Choy K.L., Lee W.B., Chan Felix T.S., *Design of a knowledge-based logistics strategy system*, *Expert Systems with Applications*, Volume 29, Issue 2, 2005.

Ciekanowski Z., *Cyberterroryzm, Zabić tysiące, przestraszyć miliony*, [w:] *Zagrożenia terrorystyczne i szanse na skuteczną obronę*, red. R. Groset, WSzZiP, Warszawa 2009.

Cieślarczyk M., *Teoretyczne, Metodologiczne i praktyczne aspekty zarządzania bezpieczeństwem w pierwszej dekadzie XXI wieku*, [w:] *Zarządzanie bezpieczeństwem – wyzwania XXI wieku*, red. nauk. WSzZiP, Warszawa 2008.

Coleman M., *Best Practices for Preventing Pallet Rack Damage*, [w:] *Inbound Logistics*, July 2015.

David S.L., Chen X., Bramel J., *The Logic of Logistics: Theory, Algorithms, and Applications for Logistics and Supply Chain Management*, 2nd ed. New York, NY, Springer, 2004.

Deore M.R., Handore S.M., *A survey on offline signature recognition and verification schemes*, [w:] *Industrial Instrumentation and Control (ICIC)*, 2015 International Conference on, 2015.

Drewek W., *Monitorowanie ładunków niebezpiecznych w transporcie drogowym*, [w:] *Logistyka* 5/2011.

Dudziński Z., *Czynniki organizacyjno-techniczne zabezpieczenia mienia w magazynach*, [w:] *Logistyka* 2/2011.

Economics and National Security, [w:] *Issues and Implications for U.S. Policy*, cor. D.K. Nanto, CRS Report for Congress, 4 January.

Edwards P., Peters M., Sharman G., *The effectiveness of information systems in supporting the extended supply chain*, *Journal of Business Logistics*, Volume 22, Issue 1, 2001.

Ejsymont J., *Czy nowa technologia EPC zastąpi kody kreskowe*, [w:] *Logistyka* 6/2006.

Mishkin F.S., *Global financial instability: framework, events, issues, journal of economic perspective*, [w:] *Journal of Economic Perspectives*, Volume 13, 1999.

Feily M., Shahrestani A., Ramadass S., *A Survey of Botnet and Botnet Detection*, [w:] *Emerging Security Information, Systems and Technologies*, 2009. SECURWARE '09. Third International Conference on, 2009.

Fiveash Ch., *What's in Your Warehouse?* [w:] *Inbound Logistics*, September 2015.

Fu Z., *Mitigating Distributed Denial-of-Service Attacks*, [w:] *Application-Defense and Network-Defense Methods*, *Computer Network Defense (EC2ND)*, 2011 Seventh European Conference on, 2011.

Gryz J., *Kształtowanie strategicznego zarządzania bezpieczeństwem narodowym*, [w:] *Strategia bezpieczeństwa narodowego Polski*, red. nauk. J. Gryz, PWE, Warszawa 2013.

Gupta A., Patel N., Khan S., *Automatic speech recognition technique for voice command*, [w:] *Science Engineering and Management Research (ICSEMR)*, 2014 International Conference on, 2014.

Halicka K., *Wykorzystanie systemów CRM w logistyce obsługi klienta*, [w:] *Ekonomia i Zarządzanie*, nr 4, 2010.

Heine T., *Cloud Inspections: Improving Productivity, Safety and Reducing Costs*, [w:] *Inbound Logistics*, Digital Issue, July 2015.

Hong-ying S., *The Application of Barcode Technology in Logistics and Warehouse Management*, [w:] *Education Technology and Computer Science*, 2009, ETCS '09. First International Workshop on (Volume 3).

Informatics and Applications (ICIA), 2013 Second International Conference on, 2013.

Jain A.K., Ross A., Prabhakar S., *An introduction to biometric recognition*, [w:] *IEEE Transactions on Circuits and Systems for Video Technology*, Volume 14, Issue 1, January 2004.

Jałowiec T., *Logistyczne wymiary systemu bezpieczeństwa państwa*, [w:] *Logistyka* 5/2014.

Jedynak M., *Efektywność systemów logistycznych*, [w:] *Zeszyty Naukowe Uniwersytetu Szczecińskiego: Finanse. Rynki finansowe. Ubezpieczenia* 2008/14.

Jerneck A., *Understanding Poverty – Seeking Synergies Between the Three Discourses of Development, Gender and Environment*, [w:] *Sage Journals*, November 2015.

Jóźwik Z., Kawa M., *Zastosowanie nowoczesnych rozwiązań logistycznych w transporcie ładunków ponadnormatywnych*, [w:] *Logistyka* 4/2009, materiał w wersji elektronicznej na CD.

Katkar V.D., Kulkarni S.V., *Experiments on detection of Denial of Service attacks using ensemble of classifiers*, [w:] *Green Computing, Communication and Conservation of Energy (ICGCE)*, 2013 International Conference on, 2013.

Kitler W., *Obrona narodowa III RP. Pojęcie. Organizacja. System*, [w:] *Zeszyty Naukowe AON*, Warszawa 2002.

Kolińska K., Jeleń I., Cudziło M., *Elektroniczna platforma logistyczna jako narzędzie wzbogacenia procesu edukacyjnego*, [w:] *Logistyka*, 2011/6.

Kołodziński E., *Modelowanie systemów bezpieczeństwa*, [w:] *Inżynieria systemów bezpieczeństwa*, red. nauk. P. Sienkiewicz, PWE, Warszawa 2015.

Koziej S., *Ocena nowej strategii bezpieczeństwa Rzeczypospolitej Polskiej*, [w:] Zeszyty Naukowe AON, 1(54),

Książkiewicz D., *Determinanty bezpieczeństwa przewozów kontenerowych*, [w:] Logistyka 5/2013.

Księżopolski K.M., *Bezpieczeństwo ekologiczne*, [w:] Bezpieczeństwo państwa, red. nauk. K.A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza Aspra-Jr, Warszawa 2009.

Kulińska E., *Wspomaganie zarządzania procesami logistycznymi – elementy metody ebXML*, [w:] *Komputerowo zintegrowane zarządzanie*, tom I, WNT, Warszawa 2005.

Kulińska K., *Metody analizy ryzyka w procesach logistycznych*, [w:] Logistyka 2/2011.

Kurek S.T., *Logistyczny wymiar systemu obronnego państwa*, [w:] Zeszyty Naukowe AON, nr 3(83), 2011.

Kurek S.T., *Model systemu zarządzania bezpieczeństwem Polski w wymiarze gospodarczym*, [w:] Zeszyty Naukowe AON, nr 1(82), 2011.

Kurek S.T., Płaczek J., *Zarys metodologii ekonomiki bezpieczeństwa*, [w:] Zeszyty Naukowe AON, nr 2 2009.

Kuźniar R., *Po pierwsze bezpieczeństwo*, [w:] Rzeczpospolita z 9 stycznia 1996 r.

Langevin A., Riopel D., *Logistics Systems*, [w:] *Design and Optimization*, Springer, 2005.

Lanier Hickman Jr H., *American Alchemy*, [w:] *The History of Solid Waste Management in United States*. Forester Press.

Lewandowski I., *Securing a sustainable biomass supply in a growing bioeconomy*, [w:] Elsevier, October 2015.

Li Yan-yan, Long W., *The Integration Model of Supply Chain Resource Allocation*, [w:] *LRP, International Asia Conference on Industrial Engineering and Management Innovation (IEMI2012) Proceedings*, May 2013.

Łacny J., *Benchmarking kosztów w polskich przedsiębiorstwach międzynarodowego transportu drogowego ładunków w 2012*, [w:] Logistyka 2/2013.

Łacny J., *Komodalność jako nowy trend w transporcie ładunków*, [w:] Logistyka 2/2009.

Łęźniak R., Nosala R., *Analiza możliwości zastosowania idei CRM dla małych przedsiębiorstw*. Zbiór referatów pod red. R. Knosali: *Komputerowo zintegrowane zarządzanie*, Zakopane, 14-16 stycznia 2002, WNT, Warszawa 2002.

M'Pherson P.K., *Systemy i nauka o systemach. Próba odpowiedzi na niektóre kwestie ontologiczne i epistemologiczne*, [w:] *Zagadnienia Naukoznawstwa*, nr 3-4, 1981.

Małec M., *Strategiczny Przegląd Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego, Strategiczny Przegląd Obrony – ich zakres i cele*, [w:] *Bezpieczeństwo Narodowe*, nr 17, 2011.

Malec M., *Strategiczny Przegląd Bezpieczeństwa Narodowego, Strategia Bezpieczeństwa Narodowego, Strategiczny Przegląd Obronny – ich zakres i cele*, [w:] *Bezpieczeństwo Narodowe*, nr 17, 2011.

Maloni M., DeWolf F., *Understanding radio frequency identification (RFID) and its impact on the supply chain*. Penn State Behrend–RFID Center of Excellence, available at, [w:] www.ebizitpa.org/Education/Operations/RFID/RFIDresearchPSU.pdf (accessed April 2, 2007).

Małysz J., *Bezpieczeństwo żywnościowe – wokół rozumienia kategorii bezpieczeństwa*, [w:] *Wokół trudnych problemów globalnego rozwoju obszarów wiejskich, gospodarki żywnościowej w erze globalizacji*, red. nauk. K. Dukaczewska-Małysz, A. Szymecka, SHG, Warszawa 2009.

Mierczyk Z., *Nowoczesne technologie w systemach monitorowania bezpieczeństwa*, [w:] *Metodologia badań bezpieczeństwa narodowego Bezpieczeństwo 2010*, t. II, AON, Warszawa 2011.

Mindur L., *Przewozy międzynarodowego transportu drogowego w Polsce po transformacji gospodarczej*, [w:] *Logistyka* 4/2015.

Mouton F., Malan M. M., Leenen L., Venter H. S., *Social engineering attack framework*, [w:] *Information Security for South Africa (ISSA)*, 2014.

Mroczek J., *Rola i zadania Zarządu Planowania Logistycznego J-4 DG RSZ*, Międzynarodowa konferencja *Integrated Logistic*, AON, Warszawa, 20.11.2014.

Nowak I., Olejniczak A., *Największy kontenerowiec świata zawinął do Gdańska*, [w:] *Logistyka* 5/2013.

Ogden P., *Applying intelligent character recognition in the “real world”*, [w:] *Document Image Processing and Multimedia (Ref. No. 1999/041)*, IEE Colloquium on, 1999.

Olszak C.M., Ziemia E., *Systemy Business Intelligence w rozwoju holistycznej infrastruktury wspomagającej podejmowanie decyzji w organizacji*, Akademia Ekonomiczna w Katowicach <http://www.ue.katowice.pl/>, 15.07.2014.

Osińska M., Zalewski W., *Ekonometryczna analiza przychodów i kosztów w przedsiębiorstwie transportowym na tle koniunktury w branży*, [w:] *Logistyka* 6/2012.

Pałęga M., *Bezpieczeństwo informacji w logistycznym systemie informatycznym klasy CRM*, [w:] *Logistyka* 2014/3.

Pałęga N., Knapiński M., *Polityka bezpieczeństwa informacji narzędziem ochrony zasobów informacyjnych w działalności logistycznej firm*, [w:] *Logistyka* 2013/6.

Pérez-Benedito J.L., Aragón E.Q., Alriols J.A., Medic L., *Optical Mark Recognition in Student Continuous Assessment*, [w:] *IEEE Revista Iberoamericana de Tecnologías del Aprendizaje*, Volume 9, Issue 4, 2014.

Petts J., *Incineration as a Waste Management Option*, [w:] *Waste Incineration and the Environment*. Ronald E. Hester, Roy M. Harrison (eds.). Cambridge, [w:] *Royal Society of Chemistry*, 1994, s. 1, seria: *Issues in Environmental Science and Technology*.

Pisz I., Łapuńska I., *Systemy transportowe wspomagające realizację projektów logistycznych w branży transport spedycja logistyka*, [w:] Logistyka 2013/5.

Rabsztyń M., *Łączność GSM-R w ruchu międzynarodowym*, Biuletyn informacyjny, Ministerstwo Infrastruktury, 4/2010, Warszawa 2010.

Rabsztyń M., *Transport kolejowy*, [w:] Biuletyn informacyjny infrastruktury nr 6/2013, Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, Warszawa 2013.

Ramaa A., Subramanya K.N., Ranganaswamy T.M., *Impact of Warehouse Management System in a Supply Chain*, [w:] International Journal of Computer Applications (0975-8887) Volume 54, No. 1, September 2012.

Rogalski W.J., *Transport kolejowy jako ogniwo w łańcuchu dostaw gospodarki polskiej*, [w:] Logistyka 2014/6.

Rolbicki R., *Infrastruktura transportowa a efektywność procesów logistycznych*, [w:] Logistyka 2/2012.

Romm J.J., *Defining National Security*, [w:] *The Nonmilitary Aspect*, Council on Foreign Relations Press, New York 1993.

Rzeczyński B., *Logistyka w systemie bezpieczeństwa narodowego Polski*, [w:] Logistyka 5/2011.

Salomon A., *Przewóz ładunków ponadgabarytowych transportem kolejowym w Polsce*, [w:] Zeszyty Naukowe nr 67, AM, Gdynia 2010.

Sienkiewicz P., *Modelowanie bezpieczeństwa systemów*, [w:] Zeszyty Naukowe AON, nr 3/4, 1991.

Sienkiewicz P., *Teoria i inżynieria bezpieczeństwa systemów*, [w:] Zeszyty Naukowe AON, nr 1(66), 2007.

Sienkiewicz P., *Teoria i inżynieria systemów*, [w:] Inżynieria Systemów Bezpieczeństwa, PWE, Warszawa 2015.

Sinha A., Lahiri R.N., Chowdhury S., Chowdhury S.P., Song Y.H., *Complete IT solution for Enterprise Asset Management (EAM) in Indian power utility business*, Universities Power Engineering Conference, 2007. UPEC 2007. 42nd International, 4-6 Sept. 2007.

Sitkowski L., *Zarządzanie bezpieczeństwem dla łańcucha dostaw – ISO 28000*, [w:] Przemysł Środowisko Jakość Zarządzanie 2(13), 2009.

Skarżyński A., *Próba ogólnej systematyki sytuacji kryzysowych oraz wybranych towarzyszących im działań techniczno-organizacyjnych*, materiały z XI Międzynarodowej Konferencji Naukowo-Technicznej Inżynierii Wojskowej, t. 1 *Zarządzanie i organizacja działań w sytuacjach kryzysowych. Ratownictwo i ochrona ludności*, Warszawa 2000.

Stappen R.K., *A Sustainable World is Possible. Der Wise Consensus*, [w:] Problemlösungen für das 21. Jahrhundert. Impuls – dokument Manuskript 1.2/2006.

Stevens B., *The Emerging Security Economy: An Introduction*, [w:] *The Security Economy*, OECD, OECD Publications, Paris 2004.

Suruchi G. Dedgaonkar, Anjali A. Chandavale, Ashok M. Sapkal, *Survey of Methods for Character Recognition*, [w:] International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 5, May 2012.

Szcześniak J., Weintrit A., *Europejskie systemy kontroli i śledzenia ruchu statków – geneza, zasady funkcjonowania oraz perspektywy rozwoju*, [w:] Zeszyty Naukowe Akademii Morskiej w Gdyni, 77/2012.

Szołtysek J., *Typologia obszarów stosowania logistyki – propozycja rozwiązania*, [w:] Gospodarka Materiałowa i Logistyka 8/2010.

Szymonik A., *Bezpieczeństwo żywnościowe*, [w:] Logistyka 5/2015.

Szymonik A., *Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce*, [w:] Logistyka 2/2011.

Szymonik A., *Niezawodność i podatność obsługowa wyrobów obronnych instrumentami regulacji łańcucha dostaw*, [w:] Zeszyty Naukowe, AMW, Gdynia 2008.

Śliwczyński B., *Elektroniczna Platforma Logistyczna – internetowe środowisko pracy logistyka*, [w:] Logistyka 2/2010.

Teska J., *Bezpieczeństwo przedmiotem wymiany?* [w:] Logistyka 6/2013.

Ucieszyński M., *Infrastruktura transportowa a efektywność procesów logistycznych*, [w:] Logistyka 2/2012.

Urbański J., Morgaś W., Kopacz Z., *Żegluga morska: jej przedmiot, zasady zarządzania oraz zarządzanie jej bezpieczeństwem morskim i ochroną na południowym Bałtyku*, [w:] Zeszyty Naukowe Akademii Marynarki Wojennej, nr 4 (171) 2007.

Verwijmeren M., *Software component architecture in supply chain management*, [w:] Computers in Industry, Volume 53, Issue 2, February 2004.

Wasiak W., *Przemysł i rynek opakowań*, [w:] Kierunki rozwoju opakowań, red. nauk. W. Wasiak, Polska Izba Opakowań, Warszawa 2014.

Wieteska S., *Pożary magazynów jako element zakłócenia funkcjonowania łańcuchów dostaw*, [w:] Logistyka 2/2013

Wolejszo J., *Teoretyczne aspekty współdziałania*, [w:] Współdziałanie systemów dowodzenia wojsk operacyjnych i wsparcia krajowego, AON, Warszawa 2005.

Yongle Wang, JunZhang Chen, *Hijacking spoofing attack and defense strategy based on Internet TCP sessions*, [w:] Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on, 2013.

Zacher L.W., *Bezpieczeństwo ekologiczne i społeczne*, [w:] Europa – kontynent ryzyka? Społeczne, polityczne i normatywne uwarunkowania bezpieczeństwa w Europie, red. M. Bożek, M. Troszyński, AON, Warszawa 2007.

Zaskórski P., *Informacyjna ciągłość działania determinantą bezpieczeństwa organizacji*, [w:] Niebezpieczny świat Systemy Informacja Bezpieczeństwo, AON, Warszawa 2015..

Zaworski J., *Systemy biometryczne* – Monitor 01/10/2002, <http://www.infolinia.com>, 01.04.2014.

Zhang H., Hu D., Palm A., *Vein Recognition System*, [w:] Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on 2010, Volume 1.

Zhu X., Li X., Yao Q., Chen Y., *Challenges and models in supporting logistics system design for dedicated-biomass-based bioenergy industry*, Bioresource Technology, Volume 102, Issue 2, 2011.

C. Dokumenty

AQAP 2070, *Proces NATO dotyczący wzajemnej realizacji rządowego zapewnienia jakości GQA*, wyd. 1, styczeń 2004, C-4.

Biała Księga Bezpieczeństwa Narodowego, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

Biała Księga, Plan utworzenia jednolitego europejskiego obszaru transportu – dążenie do osiągnięcia konkurencyjnego i zasobooszczędnego systemu transportu, KOM(2011) 144 wersja ostateczna, Bruksela, dnia 28.3.2011.

Doktryna logistyczna Sił Zbrojnych DD/4, Sztab Gen. 1566/20004, Warszawa 2004.

Doktryna Narodowa Operacje Połączone DD 3, MON, Szkol, 804/2004.

Doktryna Narodowa Operacje Połączone OP/01, Sztab Gen., Warszawa 2002.

Globalna norma bezpieczeństwa żywności, BRC Global Standard, British Retail Consortium, London, 2015.

Instrukcja o zasadach i organizacji przechowywania oraz konserwacji uzbrojenia i sprzętu wojskowego DD/4.22.8, Inspektorat Wsparcia SZ RO, Bydgoszcz 2013 r.

ISO/IEC 27001: 2007 – System zarządzania bezpieczeństwem informacji.

Konstytucja Rzeczypospolitej Polskiej, tekst uchwalony 2 kwietnia 1997 r. przez Zgromadzenie Narodowe.

PN-ISO 668:1999 – Kontenery ładunkowe serii 1. Klasyfikacja, wymiary i maksymalne ciężary brutto.

Polska Norma PN-ISO 31000: 2012P Zarządzanie ryzykiem. Zasady i wytyczne, Polski Komitet Normalizacyjny, marzec 2012.

Powódź w obliczu zagrożenia, Wydział analiz RCB, marzec 2013.

Przypisy budowy kontenerów, RPS, Gdańsk 2012.

Railway safety performance in the European Union 2014, European Railway Agency.

Regulamin organizacyjny Komendy Wojewódzkiej Państwowej Straży Pożarnej w Gdańsku.

Regulamin organizacyjny Ministra Gospodarki, załącznik do Zarządzenia Ministra Gospodarki z dnia 16 listopada 2012 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Gospodarki, Dz. U. MG z dnia 21 grudnia 2012 r. poz. 24.

- Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 roku w sprawie podniesienia ochrony statków i obiektów portowych.*
- Rozporządzenie Ministra Gospodarki z dnia 30 października 2002 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy w zakresie użytkowania maszyn przez pracowników podczas pracy.*
- Rozporządzenie Ministra Infrastruktury z dnia 26 kwietnia 2004 r. w sprawie pojazdów wykonujących pilotaż.*
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz. U. z 2003 r. Nr 169, poz. 1650, z późn.zm.).*
- Rozporządzenie Ministra Transportu z dnia 4 czerwca 2007 r. w sprawie towarów niebezpiecznych, których przewóz drogowy podlega obowiązkowi zgłoszenia.*
- Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 22 czerwca 2012 roku w sprawie zezwoleń na przejazd pojazdów nienormatywnych.*
- Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 12 kwietnia 2013 r. w sprawie przeglądów, prób i uznawania kontenerów.*
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.*
- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. z 2010 r. Nr 83, poz. 540).*
- Rozporządzenie Rady Ministrów z dnia 7 grudnia 2012 r. w sprawie rodzajów urzędzeń technicznych podlegających dozorowi technicznemu.*
- Rozporządzenie Parlamentu Europejskiego i Rady Nr 178/2002 z dnia 28 stycznia 2002 roku ustalającego ogólne zasady i wymagania prawa żywnościowego, ustanawiające Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w sprawie bezpieczeństwa żywnościowego.*
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej 2003.*
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 5 listopada 2014 r.*
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Ministerstwo Obrony Narodowej 2007.*
- Strategia Bezpieczeństwa Społecznego na lata 2007-2013.*
- Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r.*

Strategia rozwoju transportu do 2020 roku (z perspektywą do 2030 roku), Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, Warszawa, dnia 22 stycznia 2013 r.

Umowa europejska dotycząca międzynarodowego przewozu drogowego towarów niebezpiecznych ADR (Dz. U z dnia 19 lutego 2009 r.).

Ustawa Prawo Ochrony Środowiska z dnia 27 kwietnia 2001 r.

Ustawa z dnia 18 lipca 2001 r. Prawo wodne.

Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym.

Ustawa z dnia 29 października 2010 r. o rezerwach strategicznych.

Ustawa z dnia 25 sierpnia 2006 o bezpieczeństwie żywności i żywienia.

Ustawa z dnia 14 grudnia 2012 r. o odpadach.

Zagrożenia okresowe występujące w Polsce, aktualizacja, Wydział analiz RCB, styczeń 2013.

Zarządzenia nr 8 Komendanta Głównego Policji z dnia 15 marca 2013 r. w sprawie regulaminu Komendy Głównej Policji.

Zarządzenie nr 2 Komendanta Głównego Państwowej Straży Pożarnej z dnia 31 grudnia 2009 r. zmieniającego zarządzenie w sprawie nadania regulaminu organizacyjnego Komendzie Głównej Państwowej Straży Pożarnej. Decyzja nr 1 Komendanta Głównego Państwowej Straży Pożarnej z 12 stycznia 2009 r. w sprawie zakresu czynności zastępców oraz zakresu spraw zastrzeżonych do wyłącznych kompetencji Komendanta Głównego Państwowej Straży Pożarnej.

Zarządzenie nr 20, Komendanta Głównego Państwowej Straży Pożarnej z dnia 30 grudnia 2008 roku w sprawie nadania regulaminu organizacyjnego Komendzie Głównej Państwowej Straży Pożarnej.

D. Materiały statystyczne

Environment, Ochrona środowiska 2014, GUS, Warszawa 2014.

Globalny raport konkurencyjności 2015-16, Światowego Forum Gospodarczego, Warszawa, 30 września 2015 r., Departament Stabilności Finansowej.

Informacja o wynikach kontroli bezpieczeństwo ruchu kolejowego w Polsce, KIN-4114-01/2012 Nr ewid. 73/2013/I/12/003/KIN.

Logistyka w Polsce Raport 2013, red. nauk. I. Fechner, G. Szyszka, ILiM, Poznań 2014.

Mały rocznik statystyczny Polski 2015, Główny Urząd Statystyczny, Warszawa 2015.

Ocena ryzyka na potrzeby zarządzania kryzysowego Raport o zagrożeniach bezpieczeństwa narodowego, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.

Powódź w obliczu zagrożenia, Wydział analiz RCB, marzec 2013.

Raport roczny za 2014 r., 30 grudnia 2014 r., Generalna Dyrekcja Dróg Krajowych i Autostrad, <http://www.gddkia.gov.pl/pl>, 20.03.2015.

Rocznik Statystyczny Rzeczypospolitej Polskiej 2014, Główny Urząd Statystyczny, Warszawa 2015.

Transport, wyniki działalności. Roczniki statystyczne GUS, Warszawa 2004-2014.

Wypadki przy pracy w 2014, GUS, Warszawa 2015.

E. Materiały internetowe

Akademia odpadowa, <http://www.akademiaodpadowa>, 11.12.2015.

Bezpieczeństwo gospodarcze, Ministerstwo Gospodarki <http://www.mg.gov.pl/>, 12.11.2014.

Biuletynu Wydziału Analiz Rządowego Centrum Bezpieczeństwa, red. G. Świszcz, RCB, Warszawa 2013, s. 7, <http://rcb.gov.pl/>, 12.09.2014.

BRC System zarządzania bezpieczeństwem żywności, <http://www.tuv-gem.com.pl/>, 17.06.2015.

Certyfikacja zgodności z normą Safe Quality Food (SQF), <http://www.sigmaquality.pl/> 07.01.2014.

Co oznacza zarządzanie flotą, <http://www.transics.com/pl/>, 09.01.2015.

Czujniki otwarcia korka wlewu paliwa – ELTE GPS, <http://www.eltegps.pl/>, 10.07.2014.

Dura P., *E-logistyka oraz zaawansowane systemy planowania i harmonogramowania APS*, Dział Doradztwa Gospodarczego Deloitte & Touche, <http://www.mspstandard.pl/>, 14.01.2014.

Dziura ozonowa, <http://ekoproblemy.2ap.pl/>, 28.11.2015.

Efektywne zarządzanie aktywami, <http://www.4metal.pl/>, 18.01.2015.

Efektywność w zasięgu głosu, <http://synergia-it.pl/>, 20.01.2016.

Ekojazda w trzech odśłonach, <http://ulicaekologiczna.pl>, 14.07.2014.

Europejski System Zarządzania Ruchem Kolejowym, <http://www.dobralogistyka.pl/>, 11.05.2014.

Gersz A., *Szczyt klimatyczny w Paryżu: Państwa przyjęły historyczne porozumienie*, <http://www.polskatimes.pl/>, 13.12.2015.

Globalny BRC Bezpieczeństwa Żywności Standardowy, <http://www.haccp-iso22000.pl/>, 05.01.2014.

Godlewska K., *Forum Mleczarskie Biznes 2/2014 (18)*, <http://www.forummleczarskie.pl/>, 20.07.2015.

HACCAP, <http://www.izz.waw.pl/pl/>, 12.06.2015.

Hakerzy kosztują nas co roku 100 milionów złotych, <http://interaktywnie.com/biznes/artykuly/>, 22.07.2014.

IFS International Food Standard, <http://www.bheuroconsult.pl>, 06.01.2014.

IFS, <http://www.suedzucker.pl/pl/ifs,27.htm>, 12.06.2015, *IFS – Lista wymagań audytowych*, Hamilton Poland LTD, Rzeczoznawstwo i badania laboratoryjne, materiały szkoleniowe, Toruń 2012.

INRIX European National Traffic Scorecard 2010, <http://ec.europa.eu/>, 10.03.2014.

- Inteligentne systemy transportowe jako instrument poprawy efektywności transportu*, <http://www.cati.org.pl/>, 11.05.2014.
- Inteligentne Systemy Transportowe*, <https://neurosoft.pl/>, 11.11.2015.
- Internetowy słownik synonimów języka polskiego online*, <http://www.synonimy.pl/>, 25.09.2014.
- ISO 28000 Bezpieczeństwo w łańcuchu dostaw*, <http://www.lrqqa.pl/>, 01.11.2015.
- Jachimowicz Ł., *Fakty i szczegóły Głównego Inspektora Sanitarnego dotyczące działań Inspekcji Sanitarnej w sprawie fałszowania żywności solą przemysłową*, <http://gistest.pis.gov.pl/>, 25.07.2015.
- Jagodzińska K., *Zarządzanie majątkiem przedsiębiorstwa – czy warto rozbudować posiadany system ERP?*
- Januszewski J., *Stacje segmentu naziemnego nawigacyjnych systemów satelitarnych i systemów je wspomagających*, wn.am.gdynia.pl/, 18.07.2014.
- Każmierczyk P., Majewski J., *EPC Global – wprowadzenie*, <http://rfid-lab.pl/epc/>, 23.03.2014.
- Kopalinski W., *Słownik wyrazów obcych*, <http://www.slownik-online.pl/>, 23.10.2014.
- Kopaliński W., *Słownik wyrazów obcych*, <http://www.slownik-online.pl/>, 01.04.2014.
- Krawaczyński P., Zelek D., *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, <http://hackme.pl/>, 30.01.2015.
- Leksykon spedytora*, <https://www.google.pl/>, 22.07.2014.
- Mały słownik logistyczny*, <http://www.forumgospodarze.com.pl/>, 07.08.2015.
- Michalski A., *Rola zautomatyzowanych centrów logistycznych w nowoczesnych procesach łańcucha dostaw*, <http://www.logistyka.net.pl/>, 07.05.2014.
- Mszyca B., Szyller D., Fabjański M., *Cyberprzestępcy ukradli dane klientów UPS*.
- Nadolski K., *Globalne wysypisko*, <http://technowinki.onet.pl/technika/globalne-wysypisko/khckl>, 15.11.2015.
- Nadolski K., *Globalne wysypisko*, <http://technowinki.onet.pl/>, 15.11.2015.
- Ocena Funkcjonowania Rynku Transportu Kolejowego i Stanu Bezpieczeństwa Ruchu Kolejowego w 2014 roku*, <http://www.utk.gov.pl/>, 22.12.2015.
- PN-EN ISO 22000 – System zarządzania bezpieczeństwem żywności (HACCP), Urząd Dozoru Technicznego, <http://www.udt.gov.pl/>, 08.11.2015.
- Polityka transportowa UE*, <http://europa.eu/>, 10.03.2014.
- Raport roczny za 2014 r.*, 30 grudnia 2014 r., Generalna Dyrekcja Dróg Krajowych i Autostrad, <http://www.gddkia.gov.pl/pl>, 20.03.2015.
- Rozwój radiotelefonii i telewizji*, <http://itpedia.pl/>, 17.07.2014.
- Słownik synonimów i antonimów*, <http://megaslownik.pl/>, 03.04.2014.
- Sobstel J.W., *GPS na szynach*, <http://www.kosmos.gov.pl/>, 17.07.2014.

- Sokołowski G., *Traceability & Recall*, <http://www.gs1pl.org/traceability>, 22.06.2013.
- SSN LRIT imdate training, <http://www.emsa.europa.eu>, 11.05.2014.
- Stasienko J., *System informatyczny wspomagający zarządzanie relacjami z klientami*, s. 228, <http://kis.pwszchelm.pl/>, 24.08.2014.
- System telewizji przemysłowej* – <http://www.it-site.pl/>, 17.07.2014.
- Systemy zarządzania – Bezpieczeństwem żywności*, Dekra, <http://www.dekra-certification.com.pl/>, 11.11.2015.
- Szmigiel P., Szmigiel A., Stawowy M., *Wybrane metody identyfikacji pojazdów w systemie telematyki transportu*, <http://www.czasopismologistyka.pl>, 17.07.2014.
- Szulc W., *Elektroniczne metody monitorowania ruchomych środków transportowych*, <http://www.zabezpieczenia.com.pl/monitoring/elektroniczne-metody-monitorowania-ruch>, 17.07.2014.
- Traceability*, <http://antsolutions.pl/>, 05.01.2015.
- Transport lotniczy: Jednolita Europejska Przestrzeń Powietrzna*, <http://www.europarl.europa.eu/>, 11.05.2015.
- Usług informacji rzecznej (RIS)*, <http://www.google.pl>, 12.05.2014.
- Wiktor A.J., *Charakterystyka systemu HACCP*, <http://www.polhaccp.com/podstawy.htm>, 05.01.2014.
- Wydro K.B., *Telematyka – znaczenie terminu*, <https://www.itl.waw.pl/>, 17.07.2014.
- Zaworski J., *Systemy biometryczne* – Monitor 01/10/2002, <http://www.infolinia.com/monitorarticle>, 01.04.2014.
- Żuber M., *Bezpieczeństwo ekologiczne*, Dolnośląska Szkoła Wyższa Wydział Nauk Społecznych i Dziennikarstwa, s. 14, <https://www.wsiz.rzeszow.pl/>, 11.12.2015.

Charakterystyka wybranych firm, w których przeprowadzono badania

1. *Firma Kuehne + Nagel* w Polsce została założona w 1992 roku. Firma zatrudnia blisko 1600 pracowników, oferując swoje usługi logistyczne firmom krajowym oraz międzynarodowym korporacjom.
2. *Faurecia Automotive Polska* – producent wyposażenia samochodów oraz metalowych konstrukcji siedzeń. Należy do francuskiej grupy *Faurecia*, zatrudniającej 84 tysiące pracowników w 270 fabrykach w 33 krajach. Ogólne przychody *Faurecia w Polsce* w roku 2012 wyniosły ponad 3 657 mln złotych, przychody ze sprzedaży wyniosły ponad 3 613 mln złotych.
3. *DACHSER* w Polsce – obecnie w Polsce w procesy przepływu towarów oraz informacji jest zaangażowanych 332 pracowników. *DACHSER* jest jednym z wiodących dostawców usług logistycznych w Europie.
4. *Firma DTW Sp. z o.o.* działa w branży elektronicznej, elektrotechnicznej i elektroenergetycznej. Firma została założona w roku 1991 jako prywatne przedsiębiorstwo. W roku 2011 *DTW sp. z o.o.* weszła w skład *SMA Solar Technology*, czołowego producenta inwerterów z obszaru fotowoltaiki. Cechą wyróżniającą firmy na tle konkurencji jest unikatowa technologia, stosowanie nowoczesnych narzędzi zarządzania produkcją oraz dedykowany zespół badawczo-rozwojowy, który we współpracy z klientem, opracowuje optymalne, zindywidualizowane rozwiązania. Znaczną część swojej produkcji firma sprzedaje na rynkach zagranicznych, głównie w Niemczech, ale również w Stanach Zjednoczonych i Kanadzie.
5. *Frigo Logistics Sp. z o.o.* z siedzibą w Żninie koło Bydgoszczy stanowi nowoczesne centrum logistyczne dla produktów mrożonych w Polsce i należy do czołówki krajowych operatorów logistycznych tych produktów. Posiada własne magazyny wysokiego składowania w temperaturze $-23/-24^{\circ}\text{C}$ w Żninie i Radomsku. Firma powstała w 2001 roku. Trzy lata później została przejęta przez przedsiębiorstwo *Nichirei Holding Holland B.V.* z siedzibą w Rotterdamie, które wchodzi w skład japońskiego koncernu *Nichirei* z siedzibą w Tokio. Koncern *Nichirei* stanowi wiodącą organizację w Japonii specjalizującą się w usługach dla branży spożywczej. Organizacja ta należy ponadto do czołówki światowej z zakresu logistyki produktów wymagających kontrolowanych temperatur.
6. *Firma Wamtechnik* to globalny dostawca inteligentnych źródeł zasilania, które gwarantują najwyższą jakość, niezawodność i bezpieczeństwo. Bogate zaplecze doświadczeń, 20-letnia tradycja, zakład produkcyjny specjalizujący się w projektowaniu i produkcji pakietów akumulatorowych i bateryjnych oraz technologie oparte o najnowocześniejsze rozwiązania pozwoliły firmie *Wamtechnik* osiągnąć pozycję lidera w swojej branży.

7. *Przedsiębiorstwo Naprawy Taboru PKS Sp. z o.o.* istnieje na polskim rynku od 1.01.1957 roku. Początkowo jako Oddział Remontowy Wojewódzkiego Przedsiębiorstwa PKS, następnie jako Oddział Naprawczy Państwowej Komunikacji Samochodowej. Od 01.07.1990 roku samodzielne przedsiębiorstwo państwowe, a od 1.01.2001 roku Przedsiębiorstwo Naprawy Taboru Przedsiębiorstw Komunikacji Samochodowej Sp. z o.o.
8. *Panalpina Polska Sp. z o.o.* – oferuje produkty i rozwiązania z zakresu transportu morskiego oraz transportu lotniczego. Fracht morski obejmuje ogólnosiwiatowy serwis drobnicowy (LCL) oraz całokontenerowy (FCL). Natomiast transport lotniczy (eksport/import) jest zorganizowany w znacznej mierze w oparciu o sieć połączeń przez największe europejskie porty: Frankfurt i Luxemburg. Przedsiębiorstwo jest wiodącym w Polsce dostawcą usług logistycznych, pomagając swoim klientom w zakresie planowania, consultingu oraz wdrażania rozwiązań we frachcie lotniczym i morskim.
9. *CENZIN sp. z o. o.* to czołowa polska firma handlowa działająca na międzynarodowym rynku obrotu bronią, sprzętem specjalnym i logistycznym. W ramach eksportu spółka realizuje specjalistyczne dostawy sprzętu i usług dla sił zbrojnych, policji, służb mundurowych i jednostek specjalnych wielu krajów świata. W ramach importu spółka oferuje sprzęt, wyposażenie i usługi zabezpieczające potrzeby jednostek i służb podległych MON i MSW, w tym policji i jednostek specjalnych oraz innych koncesjonowanych odbiorców instytucjonalnych, jak i klientów cywilnych.
10. *WSK „PZL-KALISZ” S.A.* – Wytwórnia Sprzętu Komunikacyjnego jest przedsiębiorstwem polskiego przemysłu lotniczego od 1952 roku. Jest jedynym producentem silnika tłokowego ASz-62 IR. W zakresie produkcji lotniczej współpracuje z najważniejszymi producentami światowymi.
11. *Morska Stocznia Remontowa Gryfia S.A.* należy do grona najbardziej znanych stoczní remontowych w kraju i za granicą. Dysponuje wyposażeniem technicznym niezbędnym do prawidłowego diagnozowania i zapewniania wysokiej jakości usług z zakresu budowy konstrukcji stalowych i offshore. Posiada własne nabrzeża o łącznej długości ponad 2,5 km, które pozwalają na załadunek konstrukcji wielkogabarytowych oraz hale produkcyjne o łącznej powierzchni ponad 26 tys. m².

Źródło: opracowano na podstawie danych z Internetu.

Ankieta

Szanowni Państwo

Nazywam się Andrzej Szymonik. Jestem pracownikiem naukowym Wydziału Organizacji i Zarządzania Politechniki Łódzkiej na stanowisku profesora nadzwyczajnego. Obecnie realizuję badania w obszarze bezpieczeństwa systemów logistycznych w kontekście bezpieczeństwa gospodarczego.

Zwracam się do Państwa z uprzejmą prośbą o udzielenie odpowiedzi na poniższe pytania, pozwalające opracować monografię, która będzie wykorzystana przez studentów i słuchaczy studiów podyplomowych kierunku logistyki i bezpieczeństwa.

Pragnę zapewnić Państwa o **anonimowości** badania oraz o tym, że uzyskane informacje będą wykorzystane tylko i wyłącznie do celów naukowych. Wyniki będą ujęte w formie danych statystycznych.

Ankieta

1. Proszę określić, jakiej Firmy/Instytucji dotyczy ankieta?

- Mikro (do 10 pracowników)
- Małej (do 50 pracowników)
- Średniej (do 250 pracowników)
- Dużej (powyżej 250 pracowników)

- Prywatnej
- Państwowej
- Spółdzielczej
- Komunalnej

- Usługowej
- Produkcyjnej
- Usługowo-produkcyjnej
- Konsultingowej
- Innej

- Krajowej
- Z kapitałem obcym

Pytania zasadnicze

1. Czy w Firmie/Instytucji wdrożono podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych?
 - TAK
 - NIE
2. Czy zapewniona jest zgodność funkcjonowania podmiotu z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie kryzysowe?
 - TAK
 - NIE
3. Czy identyfikowana i analizowana jest struktura kosztów (strat) zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego?
 - TAK
 - NIE
4. Czy znane są narzędzia wspomagające zarządzanie kryzysowe?
 - a) w planowaniu systemów logistycznych?
 - TAK
 - NIE
 - b) w realizacji systemów logistycznych?
 - TAK
 - NIE
5. Czy strategia rozwoju Firmy/Instytucji ujmuje działania zapewniające bezpieczeństwo planowanych i realizowanych procesów logistycznych?
 - TAK
 - NIE
6. Czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji?
 - TAK
 - NIE
7. W jakiej formie prowadzony jest monitoring bezpieczeństwa funkcjonowania systemu logistycznego (monitoring fizyczny, wizyjny, mierników efektywności bezpieczeństwa systemu logistycznego)?
Mile widziana odpowiedź w 2-3 zdaniach.

8. Czy znana jest struktura Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego?
- TAK
 - NIE
9. Jaki jest stopień samodzielności (autonomiczności) zarządzania bezpieczeństwem systemu logistycznego w Firmie/Instytucji? – *zакreślamy jedną pozycję:*
- a) pełna samodzielność
 - b) współzarządzanie z innymi podmiotami
 - c) zarządzanie przez podmiot zewnętrzny
10. Czy w strukturze systemu zarządzania Firmą/Instytucją funkcjonuje komórka (osoba) odpowiedzialna za bezpieczeństwo funkcjonowania systemu logistycznego?
- TAK
 - NIE
11. Które procedury zarządzania bezpieczeństwem systemu logistycznego są stosowane w Firmie/Instytucji dla etapu? (*należy udzielić odpowiedzi od a do d*):
- a) planowania (analizy i oceny ryzyka zagrożeń, planowania sił i środków, procedur reagowania zachowania ciągłości działania)?
 - TAK
 - NIE
 - b) zapobiegania mogącym powstać zagrożeniom (prewencja)?
 - TAK
 - NIE
 - c) reagowania na występujące zakłócenia w funkcjonowaniu systemu logistycznego?
 - TAK
 - NIE
 - d) odbudowy systemu po wystąpieniu zakłóceń częściowych lub całkowitych?
 - TAK
 - NIE
12. W jakiej formie odbywa się zarządzanie zasobami własnymi (materialne, ludzkie, finansowe, informacyjne) dla zapewnienia wymaganego poziomu bezpieczeństwa funkcjonowania systemu logistycznego?
- a) autonomicznie – jest integralną częścią zarządzania Firmą/Instytucją?
 - b) realizowane jest przez wyspecjalizowany podmiot zewnętrzny?
13. Czy zostały wdrożone procedury współdziałania z otoczeniem zewnętrznym w celu efektywnego zarządzania bezpieczeństwem systemu logistycznego?
- TAK
 - NIE

14. Czy wypracowane procedury oraz wydzielone zasoby zapewniające akceptowalny (przez Firmę/Instytucję i obowiązujące wymogi formalno-prawne) poziom bezpieczeństwa zgodne są z obowiązującymi standardami krajowymi i europejskimi?
- TAK
 - NIE
15. Czy organizacja produkcji/usług w Firmie/Instytucji realizowana jest:
- a) na zamówienie (dla konkretnego klienta/usługobiorcy)?
- TAK
 - NIE
- b) na magazyn (na podstawie prognozowania popytu)?
- TAK
 - NIE
16. Czy podstawą produkcji/usług w Firmie/Instytucji jest:
- a) zaopatrzenie z własnego magazynu (towary są wcześniej zakupione i znajdują się we własnym magazynie)?
- TAK
 - NIE
- b) bieżąca realizacja potrzeb (pojawiająca się potrzeba generuje konieczność złożenia zamówienia na wybrany towar)?
- TAK
 - NIE
17. Proszę podać przykłady praktycznych i konkretnych rozwiązań (organizacyjnych, technicznych i innych) w zakresie zapewnienia bezpieczeństwa systemów logistycznych?
Bardzo mile widziane obecne i przyszłościowe – nawet w kilkunastu zdaniach.
18. Czy w Firmie/Instytucji prowadzi się szkolenia związane z zarządzaniem bezpieczeństwem systemów logistycznych?
- Jeśli tak to czy:
- a) własnymi „siłami”?
- TAK
 - NIE
- b) za pomocą wyspecjalizowanych firm zewnętrznych?
- TAK
 - NIE

Analiza ilości użytych określenia „logistyka”, „logistycznych” i „logistycznego” w Strategiach Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej i „Białej Księdze” 2013

1. Dokument: *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2003*

Rozdział IV. Gospodarcze podstawy bezpieczeństwa państwa

3. Infrastruktura. Działania na rzecz utrzymania właściwego stanu polskiej infrastruktury są jednym z warunków zapewnienia odpowiedniego potencjału obronnego i bezpieczeństwa kraju, zarówno wewnętrznego, jak i zewnętrznego. W nadchodzących latach konieczne jest zwiększenie wysiłku państwa na rzecz modernizacji infrastruktury transportowej, w tym budowy autostrad i dróg ekspresowych, zrównoważonego rozwoju transportu kolejowego, budowy lotnisk i lądowisk oraz systemu nawigacyjnego, zmiany w strukturze i wielkości przeładunków żeglugi morskiej i śródlądowej oraz lądowo-morskich **łańcuchów transportowych i logistycznych**.

2. Dokument: *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007*

Podrozdział 3.2. Bezpieczeństwo militarne

57. Udział Polski w obronie kolektywnej zgodnie z artykułem V Traktatu Waszyngtońskiego oraz wspieranie polityki ONZ, NATO, UE w dziedzinie reagowania kryzysowego i w działaniach stabilizacyjnych, wiązał się będzie z potrzebą uwzględnienia w planowaniu strategicznym rozszerzonego spektrum zagrożeń, zwłaszcza o charakterze asymetrycznym, oraz nowego kontekstu technologicznego. Warunkami powodzenia operacji wojskowych będą przede wszystkim: uzyskanie przewagi informacyjnej; ubycie struktur zadaniowych sił zbrojnych, wyposażonych w nowocześniejszy sprzęt techniczny od sprzętu przeciwnika; zastosowanie zaawansowanych technologii w zakresie dowodzenia; posiadanie możliwości skutecznego rażenia, dokonywania manewru i ochrony przed rażeniem przeciwnika; umiejętne stosowanie symetrycznej strategii wobec działań przeciwnika, pełne wykorzystanie zasobów **logistycznych** kraju oraz współpracy cywilno-wojskowej.

Podrozdział 4.3. Podsystemy wykonawcze

99. Liczebność Sił Zbrojnych RP w najbliższej przyszłości nie będzie ulegać istotnym zmianom. Dokonujące się od około dwudziestu lat redukcje spowodowały rozmiary sił zbrojnych do poziomu, w którym kontynuacja tego trendu może nieść niepożądane ryzyko. Będzie natomiast postępował proces profesjonalizacji sił zbrojnych. Struktura sił zbrojnych: Wojska Lądowe, Siły Powietrzne, Marynarka Wojenna, Wojska Specjalne oraz Inspektorat Wsparcia Sił Zbrojnych, jako organizator systemu wsparcia **logistycznego** sił zbrojnych, jest właściwie dostosowana do wypełniania zadań. W kontekście trwającej

wojny z terroryzmem szczególnego znaczenia nabierają Wojska Specjalne, jako najlepiej przygotowane do działań przeciwko zagrożeniom asymetrycznym oraz do współpracy z innymi wyspecjalizowanymi instytucjami i organami działającymi w systemie bezpieczeństwa państwa. Należy wspierać rozwiązania mające na celu efektywne wykorzystanie tego rodzaju wojsk.

137. Istotnym zadaniem w zakresie ochrony zdrowia jest utrzymywanie rezerw państwowych produktów leczniczych i wyrobów medycznych, a także zestawów sprzętowo-lekowych przechowywanych w szpitalach oraz magazynach Agencji Rezerw Materiałowych, a także w Bazach Sprzętu Specjalistycznego Państwowej Straży Pożarnej. Ochrona zdrowia stanowi także ważne ogniwo w łańcuchu cywilnego wsparcia **logistycznego** narodowych i sojusznicznych sił zbrojnych, odpowiedzialne za realizację zadań w zakresie wspólnej obrony oraz kompleksowe i wszechstronne świadczenie wsparcia ze strony państwa – gospodarza.

3. Dokument: *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*

Nie ma żadnej wzmianki o logistyce.

4. Dokument: *Biała Księga 2013*

Podrozdział 1.2. Potencjał Polski w dziedzinie bezpieczeństwa

Służba zdrowia w systemie bezpieczeństwa narodowego. Ministerstwo Zdrowia odpowiada m.in. za organizację systemu ochrony zdrowia, politykę zdrowotną i lekową. Narzędzia prawne będące w dyspozycji ministra zdrowia pozwalają na prowadzenie polityki wypełniającej konstytucyjny obowiązek państwa, polegający m.in. na zapewnieniu każdemu obywatelowi prawa do ochrony zdrowia, równym dostępie do świadczeń opieki zdrowotnej finansowanej ze środków publicznych, zapewnieniu szczególnej opieki zdrowotnej dzieciom, kobietom ciężarnym, osobom niepełnosprawnym i osobom w podeszłym wieku oraz zwalczaniu chorób epidemicznych i zapobieganiu negatywnym dla zdrowia skutkom degradacji środowiska. W obowiązujących ramach prawnych, wykonując konstytucyjny obowiązek zapewnienia dostępu do świadczeń medycznych, również w sytuacjach kryzysowych, należy mieć na uwadze, że wszystkie działania podmiotów uprawnionych do udzielania świadczeń medycznych i wsparcia organizacyjno-**logistycznego** wynikają wyłącznie z umocowanych w prawie właściwości organów, zaś skuteczna, w pełni nowoczesna i kompetentna pomoc medyczna powinna być wypadkową współpracy i współdziałania wszystkich jednostek oraz służb porządkowych, technicznych, medycznych i administracyjnych. Mówiąc o właściwości organów państwa, odpowiedzialnych za zapewnienie na wymaganym poziomie opieki zdrowotnej, należy mieć na uwadze, że właściwość ta leży nie tylko w gestii ministra zdrowia, ale również organów administracji rządowej w terenie i samorządowej.

Podrozdział 3.3. Zadania strategiczne podsystemów wsparcia bezpieczeństwa narodowego

Służba zdrowia w systemie bezpieczeństwa. Podstawowym zadaniem operacyjnym w podsystemie ochrony zdrowia jest zapewnienie ciągłości funkcjonowania podmiotów leczniczych oraz świadczenie przez nie usług medycznych w przypadku wystąpienia sytuacji kryzysowych, zagrożenia bezpieczeństwa państwa lub wojny. Do najważniejszych działań w tym zakresie należy zaliczyć: stworzenie warunków do zabezpieczenia zdrowia i życia ludności, w tym formalno-prawnych, organizacyjnych i **logistycznych**; przygotowanie i utrzymanie gotowości systemu ochrony zdrowia do działania w stanach zagrożenia bezpieczeństwa państwa i wojny; łagodzenie oraz likwidacja skutków zagrożeń oraz ograniczenie powstawania strat masowych; wsparcie systemu ochrony zdrowia służb mundurowych RP; realizacja obowiązków państwa – gospodarza względem wojsk sojusznicznych, wynikających z Programu wsparcia państwa – gospodarza (*Host Nation Support, HNS*).

Podrozdział 4.3. Przygotowanie podsystemów operacyjnych bezpieczeństwa narodowego

Kolejnym elementem w systemie służb i formacji porządku publicznego są straże gminne (miejskie). Po ponad dwudziestu latach funkcjonowania straży pojawiła się dyskusja co do przyszłości tych formacji. Powstały koncepcje rozszerzające zakres uprawnień straży, które przekształciłyby się w policje municypalne, czyli rodzaj samorządowej policji lokalnej, co wiązałoby się z uzyskaniem uprawnień także w zakresie uposażenia i przywilejów emerytalnych. W razie podniesienia rangi straży miejskich konieczna stałaby się implementacja właściwych procedur doboru, szkolenia, nadzoru nad działalnością i tworzenia zaplecza **logistycznego**. Z drugiej strony pojawiają się propozycje, by straże gminne włączyć do struktur policyjnych, łącznie ze środkami budżetowymi przeznaczonymi na ich funkcjonowanie.

5. Dokument: *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022*

16 razy użyto określeń „logistyka”, „logistycznych”, „logistycznego”.

Źródło: opracowanie własne.

Wykaz podstawowych aktów prawnych dotyczących transportu kolejowego

1. Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2007 r. Nr 16, poz. 94 ze zm.).
2. Rozporządzenie Ministra Infrastruktury z dnia 18 lipca 2005 r. w sprawie ogólnych warunków prowadzenia ruchu kolejowego i sygnalizacji (Dz. U. Nr 172, poz. 1444 ze zm.).
3. Rozporządzenie Ministra Transportu z dnia 19 marca 2007 r. w sprawie systemu zarządzania bezpieczeństwem w transporcie kolejowym (Dz. U. Nr 60, poz. 407 ze zm.).
4. Rozporządzenie Ministra Infrastruktury z dnia 20 lipca 2010 r. w sprawie wspólnych wskaźników bezpieczeństwa CSI (Dz. U. Nr 142, poz. 952).
5. Rozporządzenie Ministra Transportu z dnia 5 grudnia 2006 r. w sprawie sposobu uzyskania certyfikatu bezpieczeństwa (Dz. U. Nr 230, poz. 1682).
6. Rozporządzenie Ministra Transportu z dnia 12 marca 2007 r. w sprawie warunków oraz trybu wydawania, przedłużania, zmiany i cofania autoryzacji bezpieczeństwa, certyfikatów bezpieczeństwa i świadectw bezpieczeństwa (Dz. U. Nr 57, poz. 389).
7. Rozporządzenie Ministra Infrastruktury z dnia 18 lutego 2011 r. w sprawie licencji maszynisty (Dz. U. Nr 66, poz. 346 ze zm.).
8. Rozporządzenie Ministra Infrastruktury z dnia 18 lutego 2011 r. w sprawie świadectwa maszynisty (Dz. U. Nr 66, poz. 347).
9. Rozporządzenie Ministra Infrastruktury z dnia 15 marca 2011 r. w sprawie wpisu na listę podmiotów uprawnionych do przeprowadzania badań w celu sprawdzenia spełniania wymagań zdrowotnych, fizycznych i psychicznych, niezbędnych do uzyskania licencji oraz świadectwa maszynisty (Dz. U. Nr 66, poz. 348).
10. Rozporządzenie Ministra Infrastruktury z dnia 18 lutego 2011 r. w sprawie pracowników zatrudnionych na stanowiskach bezpośrednio związanych z prowadzeniem i bezpieczeństwem ruchu kolejowego, prowadzeniem określonych rodzajów pojazdów kolejowych oraz pojazdów kolejowych metra (Dz. U. Nr 59, poz. 301 ze zm.).
11. Rozporządzenie Ministra Infrastruktury z dnia 12 października 2005 r. w sprawie ogólnych warunków technicznych eksploatacji pojazdów kolejowych (Dz. U. Nr 212, poz. 1771 ze zm.).
12. Rozporządzenie Ministra Infrastruktury z dnia 26 września 2003 r. w sprawie wykazu typów budowli i urządzeń przeznaczonych do prowadzenia ruchu kolejowego oraz typów pojazdów kolejowych, na które wydawane są świadectwa dopuszczenia do eksploatacji (Dz. U. Nr 175, poz. 1706).

14. Rozporządzenie Ministra Infrastruktury z dnia 15 lutego 2005 r. w sprawie świadectw prawności technicznej pojazdów kolejowych (Dz. U. Nr 37, poz. 330).
15. Rozporządzenie Ministra Transportu z dnia 2 listopada 2006 r. w sprawie dokumentów, które powinny znajdować się w pojeździe kolejowym (Dz. U. z 2007 r. Nr 9, poz. 63).
16. Rozporządzenie Ministra Transportu z dnia 19 lutego 2007 r. w sprawie zawartości raportu z postępowania w sprawie poważnego wypadku, wypadku lub incydentu kolejowego (Dz. U. Nr 41, poz. 268).
17. Rozporządzenie Ministra Transportu z dnia 30 kwietnia 2007 r. w sprawie poważnych wypadków, wypadków i incydentów na liniach kolejowych (Dz. U. Nr 89, poz. 593).
18. Rozporządzenie Ministra Infrastruktury z dnia 22 października 2009 r. w sprawie opłaty za udzielenie licencji i licencji tymczasowej na prowadzenie działalności gospodarczej w zakresie transportu kolejowego (Dz. U. Nr 196, poz. 1515).
19. Rozporządzenie Ministra Transportu z dnia 12 marca 2007 r. w sprawie trybu wykonywania kontroli przez Prezesa Urzędu Transportu Kolejowego (Dz. U. Nr 57, poz. 388 ze zm.).
20. Dyrektywa Parlamentu Europejskiego i Rady 2004/49/WE z dnia 29 kwietnia 2004 roku w sprawie bezpieczeństwa kolei wspólnotowych oraz zmieniająca dyrektywę Rady 95/18/WE w sprawie przyznawania licencji przedsiębiorstwom kolejowym oraz dyrektywę 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej i pobierania opłat za użytkowanie infrastruktury kolejowej oraz certyfikację w zakresie bezpieczeństwa (Dz. U. UE L 2004. 164. 44 ze zm.).
21. Dyrektywa Parlamentu Europejskiego i Rady 2008/110/WE z dnia 16 grudnia 2008 roku zmieniająca dyrektywę w sprawie bezpieczeństwa kolei wspólnotowych (Dz. U. UE L 2008.345. 62).
22. Dyrektywa Parlamentu Europejskiego i Rady 2008/57/WE z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie (Dz. U. UE L 2008.191.1 ze zm.).
23. Zarządzenie Nr 5/2011 Zarządu PKP PLK S.A. z dnia 8 lutego 2011 r. w sprawie wprowadzenia do stosowania regulaminu przydzielania tras pociągów i korzystania z przydzielonych tras pociągów przez licencjonowanych przewoźników kolejowych w ramach rozkładu jazdy 2011/2012 – niepublikowane.
24. Instrukcja o prowadzeniu ruchu pociągów Ir-1 (tekst ujednoczony przyjęty uchwałą PKP PLK SA, Nr 176/2008 z dnia 2 kwietnia 2008 r.) – niepublikowana.

Instrukcja o postępowaniu w sprawach poważnych wypadków, wypadków, incydentów oraz trudności eksploatacyjnych na liniach kolejowych Ir-8 – niepublikowana.

25. Instrukcja o organizacji i użytkowaniu sieci radiotelefonicznych Ir-14 – niepublikowana.

26. Zarządzenie Nr 14 Zarządu PKP PLK SA w sprawie wprowadzenia „Warunków technicznych utrzymania nawierzchni na liniach kolejowych” Id-1 (D-1) – niepublikowane.

27. Zarządzenie Nr 14 Zarządu PKP PLK SA w sprawie wprowadzenia „Warunków technicznych utrzymania nawierzchni na liniach kolejowych” Id-1 (D-1) – niepublikowane.

28. Zarządzenie Nr 16/2007 Zarządu PKP PLK SA z dnia 21 czerwca 2007 r. wprowadzające Instrukcję sygnalizacji Ie-1 (E-1) – niepublikowane.

Akta normatywno-prawne – Unia Europejska

1. Dyrektywę 2001/12 Parlamentu Europejskiego i Rady z 26 lutego 2001 r. zmieniającą Dyrektywę Rady EWG 91/440 w sprawie rozwoju kolei wspólnotowych (Dz. U. UE L 2001.75.1).

2. Dyrektywę 2001/13 Parlamentu Europejskiego i Rady z 26 lutego 2001 r. zmieniającą Dyrektywę Rady 95/18 w sprawie przyznawania licencji przedsiębiorstwom kolejowym (Dz. U. UE L 2001.75.26).

3. Dyrektywę Rady nr 96/49/WE z dnia 23 lipca 1996 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich w zakresie kolejowego transportu towarów niebezpiecznych (Dz. U. UE L 1996.235.25).

4. Rozporządzenie Rady EWG Nr 1191/69/EWG z dnia 26 czerwca 1969 r. w sprawie działania Państw Członkowskich dotyczącego zobowiązań związanych z pojęciem usługi publicznej w transporcie kolejowym, drogowym i w żegludze śródlądowej (Dz. U. UE L 1969.156.1) wraz z Rozporządzeniem Rady (EWG) Nr 1893/91 z 20 czerwca 1991 r. zmieniającym Rozporządzenie Rady (EWG) Nr 1191/69 w sprawie działania Państw Członkowskich dotyczącego zobowiązań związanych z pojęciem usługi publicznej w transporcie kolejowym, drogowym i w żegludze śródlądowej (Dz. U. UE L 1991.169.1).

5. Dyrektywa 2004/49/WE Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa kolei wspólnotowych oraz zmieniająca dyrektywę 95/18/WE w sprawie przyznawania licencji przedsiębiorstwom kolejowym oraz dyrektywę 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej i pobierania opłat za użytkowanie infrastruktury kolejowej oraz certyfikację w zakresie bezpieczeństwa – Dz. U. UE L 2004.164.44 ze zm.

6. Dyrektywa 2004/50/WE Parlamentu Europejskiego i Rady zmieniająca dyrektywę 96/48/WE w sprawie interoperacyjności transeuropejskiego systemu kolei dużych prędkości i dyrektywę 2001/16/WE w sprawie interoperacyjności transeuropejskiego systemu kolei konwencjonalnej.

– Dz. U. UE L 2004.164.114.

7. Dyrektywa 2004/51/WE Parlamentu Europejskiego i Rady, zmieniająca dyrektywę 91/440/EWG w sprawie rozwoju kolei wspólnotowych. – Dz. U. UE L 2004.164.164.
8. Rozporządzenie 881/2004 Parlamentu Europejskiego i Rady z 30.04.2004 r. ustanawiające Europejską Agencję Kolejową – Dz. U. UE L 2004.164.1 ze zm.
9. Dyrektywa 2007/58/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. (Dz. U. UE L 2007.315.44) zmieniająca dyrektywę Rady 91/440/EWG w sprawie rozwoju kolei wspólnotowych oraz dyrektywę 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej i pobierania opłat za użytkowanie infrastruktury kolejowej.
10. Rozporządzenie (WE) NR 1371/2007 Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. (Dz. U. UE L 2007.315.14), dotyczące praw i obowiązków pasażerów w ruchu kolejowym.
11. Dyrektywa 2007/59/WE Parlamentu Europejskiego i Rady z dnia 23 października 2007 r. (Dz. U. UE L 2007.315.51) w sprawie przyznawania uprawnień maszynistom prowadzącym lokomotywy i pociągi w obrębie systemu kolejowego Wspólnoty.

Źródło: opracowanie własne na podstawie: A. Michalski, *Rola zautomatyzowanych centrów logistycznych w nowoczesnych procesach łańcucha dostaw*, <http://www.logistyka.net.pl>, 07.05.2014.

Logistyczny softwarowy pakiet firmy Swisslog

Pakiet ten obejmuje następujące moduły (w nawiasach przedstawiono ich główne funkcje):

- umożliwiające realizację procesów logistycznych:
 - ✓ *WarehouseManager* (maksymalizacja wydajności łańcucha dostaw poprzez automatyzację kluczowych procesów, m.in. przyjęcia, magazynowania kompletacji zamówień, ekspedycji),
 - ✓ *AutomationControl* (monitorowanie i sterowanie kompletnym systemem logistycznym),
 - ✓ *BillingManager* (automatyzacja obliczania kwot zapłaty od kontrahentów logistycznych za określone czynności, np. kompletację, pakowanie, paletyzację itd.),
 - ✓ G-TRACK (śledzenie serii),
 - ✓ *VoiceManager* (głosowe sterowanie operacjami),
 - ✓ *AutomationManager* (zarządzanie systemami automatyki),
 - ✓ moduły specjalne;
- umożliwiające optymalizację procesów logistycznych:
 - ✓ *SlottingManager* (generowanie w czasie rzeczywistym optymalnych pod względem ekonomicznym schematów magazynowania oraz przyporządkowań towarów do określonych lokacji),
 - ✓ *CubingManager* (planowanie i optymalizacja załadunków),
 - ✓ *RouteManager* (planowanie i optymalizacja tras);
- służące do wieloaspektowego monitorowania procesów logistycznych:
 - ✓ *WarehouseMonitor* (monitorowanie i sterowanie różnymi zdarzeniami w środowisku *WarehouseManager*, włącznie ze statusami zamówień/doków, produktywnością itd.),
 - ✓ *ResourceMonitor* (oszacowywanie obciążenia poszczególnych stref centrum logistycznego, w celu spełnienia wymagań komplekcyjnych dla otwartych zamówień),
 - ✓ *EventManager* (zarządzanie zdarzeniami),
 - ✓ KPI Monitor (obliczanie kluczowych wskaźników dotyczących wydajności),
 - ✓ *AutomationVisualiser* (dynamiczna wizualizacja instalacji);
- pozwalające na współpracę z bliższym lub dalszym otoczeniem:
 - ✓ *EventForwarder* (monitoring i sterowanie zdarzeniami),
 - ✓ *HostManager* (interfejs z systemem ERP Host, np. SAP R/3),
 - ✓ obsługa spedycji,
 - ✓ WWW (obsługa sprzedaży przez Internet).

Źródło: opracowanie własne.

Podstawowe przepisy prawne regulujące odpowiedzialność materialną pracowników magazynowych

1. Kodeks pracy (uchwalony ustawą z 26 czerwca 1974 r. i ustawą z 2 lutego 1996 r.).
2. Rozporządzenie wykonawcze Rady Ministrów z 4 października 1974 r. w sprawie wspólnej odpowiedzialności materialnej pracowników za powierzone mienie (Dz. U. nr 40, poz. 236).
3. Rozporządzenie Rady Ministrów z 10 października 1975 r. w sprawie warunków odpowiedzialności materialnej pracowników za szkodę w powierzonym mieniu (Dz. U. nr 35, poz. 191).
4. Rozporządzenie Rady Ministrów z 28 maja 1996 r. zmieniające rozporządzenie w sprawie warunków odpowiedzialności materialnej za szkodę w powierzonym mieniu (Dz. U. nr 60, poz. 276).

Źródło: opracowanie własne.

Rozporządzenia i dyrektywy EWG i WE w sprawie higieny
i bezpieczeństwa żywności

1. Rozporządzenie Rady (EURATOM) nr 3954/87 z dnia 22 grudnia 1987 r. ustanawiające maksymalne dozwolone poziomy skażenia radioaktywnego środków spożywczych oraz pasz po wypadku jądrowym lub w każdym innym przypadku pogotowia radiologicznego.
2. Rozporządzenie Komisji (EURATOM) nr 944/89 z dnia 12 kwietnia 1989 r. ustanawiające maksymalne dozwolone poziomy skażenia radioaktywnego w środkach spożywczych o mniejszym znaczeniu w następstwie wypadku jądrowego lub w każdym innym przypadku pogotowia radiologicznego.
3. Rozporządzenie Rady (EWG) nr 315/93 z dnia 8 lutego 1993 r. ustanawiające procedury Wspólnoty w odniesieniu do substancji skażających w żywności.
4. Rozporządzenie (WE) nr 2232/96 Parlamentu Europejskiego i Rady z dnia 28 października 1996 r. ustanawiające wspólnotową procedurę dla substancji aromatycznych używanych lub przeznaczonych do użycia w lub na środkach spożywczych.
5. Rozporządzenie (WE) nr 258/97 Parlamentu Europejskiego i Rady z dnia 27 stycznia 1997 r. dotyczące nowej żywności i nowych składników żywności.
6. Rozporządzenie Komisji (WE) nr 1565/2000 z dnia 18 lipca 2000 r. ustanawiające środki konieczne do przyjęcia programu oceny w zastosowaniu rozporządzenia (WE) nr 2232/96 Parlamentu Europejskiego i Rady.
7. Rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności.
8. Rozporządzenie (WE) nr 1829/2003 Parlamentu Europejskiego i Rady z dnia 22 września 2003 r. w sprawie genetycznie zmodyfikowanej żywności i paszy.
9. Rozporządzenie (WE) nr 1830/2003 Parlamentu Europejskiego i Rady z dnia 22 września 2003 r. dotyczące możliwości śledzenia i etykietowania organizmów zmodyfikowanych genetycznie oraz możliwości śledzenia żywności i produktów paszowych wyprodukowanych z organizmów zmodyfikowanych genetycznie i zmieniające dyrektywę 2001/18/WE.
10. Rozporządzenie (WE) nr 1946/2003 Parlamentu Europejskiego i Rady z dnia 15 lipca 2003 r. w sprawie transgranicznego przemieszczania organizmów genetycznie zmodyfikowanych.
11. Rozporządzenie (WE) nr 2065/2003 Parlamentu Europejskiego i Rady z dnia 10 listopada 2003 r. w sprawie środków aromatyzujących dymu wędzarniczego używanych lub przeznaczonych do użycia w środkach spożywczych lub na ich powierzchni.
12. Rozporządzenie (WE) nr 852/2004 Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie higieny środków spożywczych.

13. Rozporządzenie (WE) nr 882/2004 Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie kontroli urzędowych przeprowadzanych w celu sprawdzenia zgodności z prawem paszowym i żywnościowym oraz regułami dotyczącymi zdrowia zwierząt i dobrostanu zwierząt.
14. Rozporządzenie (WE) nr 1935/2004 Parlamentu Europejskiego i Rady z dnia 27 października 2004 r. w sprawie materiałów i wyrobów przeznaczonych do kontaktu z żywnością oraz uchylające dyrektywy 80/590/EWG i 89/109/EWG.
15. Rozporządzenie (WE) nr 396/2005 Parlamentu Europejskiego i Rady z dnia 23 lutego 2005 r. w sprawie najwyższych dopuszczalnych poziomów pozostałości pestycydów w żywności i paszy pochodzenia roślinnego i zwierzęcego oraz na ich powierzchni, zmieniające dyrektywę Rady 91/414/EWG.
16. Rozporządzenie Komisji (WE) nr 1895/2005 z dnia 18 listopada 2005 r. w sprawie ograniczenia wykorzystania niektórych pochodnych epoksydowych w materiałach i wyrobach przeznaczonych do kontaktu z żywnością.
17. Rozporządzenie Komisji (WE) nr 2073/2005 z dnia 15 listopada 2005 r. w sprawie kryteriów mikrobiologicznych dotyczących środków spożywczych wykonawcze w odniesieniu do niektórych produktów objętych rozporządzeniem (WE) nr 853/2004 i do organizacji urzędowych kontroli na mocy rozporządzeń (WE) nr 854/2004 oraz (WE) nr 882/2004, ustanawiające odstępstwa od rozporządzenia (WE) nr 852/2004 i zmieniające rozporządzenia (WE) nr 853/2004 oraz (WE) nr 854/2004.
18. Rozporządzenie Komisji (WE) nr 401/2006 z dnia 23 lutego 2006 r. ustanawiające metody pobierania próbek i analizy do celów urzędowej kontroli poziomów mikotoksyn w środkach spożywczych.
19. Rozporządzenie Rady (WE) nr 509/2006 z dnia 20 marca 2006 r. w sprawie produktów rolnych i środków spożywczych będących gwarantowanymi tradycyjnymi specjalnościami.
20. Rozporządzenie Komisji (WE) nr 627/2006 z dnia 21 kwietnia 2006 r. w sprawie wykonania rozporządzenia (WE) nr 2065/2003 Parlamentu Europejskiego i Rady w odniesieniu do kryteriów jakościowych dla uznanych metod analitycznych w zakresie pobierania próbek, identyfikacji i charakterystyki początkowych produktów wędzarniczych.
21. Rozporządzenie Komisji (WE) nr 1881/2006 z dnia 19 grudnia 2006 r. ustalające najwyższe dopuszczalne poziomy niektórych zanieczyszczeń w środkach spożywczych.
22. Rozporządzenie Komisji (WE) nr 1882/2006 z dnia 19 grudnia 2006 r. ustanawiające metody pobierania próbek i analizy do celów urzędowej kontroli poziomu azotanów w niektórych środkach spożywczych.
23. Rozporządzenie Komisji (WE) nr 1883/2006 z dnia 19 grudnia 2006 r. ustanawiające metody pobierania próbek i metody analizy do celów urzędowej kontroli dioksyn i dioksynopodobnych polichlorowanych bifenyli (PCB) w środkach spożywczych.

24. Rozporządzenie (WE) nr 1924/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie oświadczeń żywieniowych i zdrowotnych dotyczących żywności.
25. Rozporządzenie (WE) nr 1925/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dodawania do żywności witamin i składników mineralnych oraz niektórych innych substancji.
26. Rozporządzenie Komisji (WE) nr 1981/2006 z dnia 22 grudnia 2006 r. ustalające szczegółowe zasady wykonania przepisów art. 32 rozporządzenia (WE) nr 1829/2003 Parlamentu Europejskiego i Rady w odniesieniu do wspólnotowego laboratorium referencyjnego dla organizmów zmodyfikowanych genetycznie.
27. Rozporządzenie Komisji (WE) nr 2023/2006 z dnia 22 grudnia 2006 r. w sprawie dobrej praktyki produkcyjnej w odniesieniu do materiałów i wyrobów przeznaczonych do kontaktu z żywnością.
28. Rozporządzenie Komisji (WE) nr 333/2007 z dnia 28 marca 2007 r. ustanawiające metody pobierania próbek i metody analiz do celów urzędowej kontroli poziomów ołowiu, kadmu, rtęci, cyny nieorganicznej, 3-MCPD i benzo[a]pirenu w środkach spożywczych.
29. Rozporządzenie Rady (WE) nr 834/2007 z dnia 28 czerwca 2007 r. w sprawie produkcji ekologicznej i znakowania produktów ekologicznych i uchylające rozporządzenie (EWG) nr 2092/91.
30. Rozporządzenie Komisji (WE) nr 884/2007 z dnia 26 lipca 2007 r. w sprawie środków nadzwyczajnych zawieszających stosowanie E 128 czerwień 2G jako barwnika żywności.
31. Rozporządzenie Komisji (WE) nr 282/2008 z dnia 27 marca 2008 r. w sprawie materiałów i wyrobów z tworzyw sztucznych pochodzących z recyklingu przeznaczonych do kontaktu z żywnością oraz zmieniające rozporządzenie (WE) nr 2023/2006.
32. Rozporządzenie Komisji (WE) nr 353/2008 z dnia 18 kwietnia 2008 r. ustanawiające przepisy wykonawcze w odniesieniu do wniosków o wydanie zezwolenia na stosowanie oświadczeń zdrowotnych zgodnie z art. 15 rozporządzenia (WE) nr 1924/2006 Parlamentu Europejskiego i Rady.
33. Rozporządzenie Rady (WE) nr 733/2008 z dnia 15 lipca 2008 r. w sprawie warunków regulujących przywóz produktów rolnych pochodzących z krajów trzecich w następstwie wypadku w elektrowni jądrowej w Czarnobylu.
34. Rozporządzenie Komisji (WE) nr 889/2008 z dnia 5 września 2008 r. ustanawiające szczegółowe zasady wdrażania rozporządzenia Rady (WE) nr 834/2007 w sprawie produkcji ekologicznej i znakowania produktów ekologicznych w odniesieniu do produkcji ekologicznej, znakowania i kontroli.
35. Rozporządzenie Komisji (WE) nr 1235/2008 z dnia 8 grudnia 2008 r. ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 834/2007 w odniesieniu do ustaleń dotyczących przywozu produktów ekologicznych z krajów trzecich.

36. Rozporządzenie Komisji (WE) nr 1243/2008 z dnia 12 grudnia 2008 r. zmieniające załączniki III i VI do dyrektywy 2006/141/WE w odniesieniu do wymogów dotyczących składu niektórych preparatów do początkowego żywienia niemowląt.
37. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1331/2008 z dnia 16 grudnia 2008 r. ustanawiające jednolitą procedurę wydawania zezwoleń na stosowanie dodatków do żywności, enzymów spożywczych i środków aromatyzujących.
38. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1332/2008 z dnia 16 grudnia 2008 r. w sprawie enzymów spożywczych, zmieniające dyrektywę Rady 83/417/EWG, rozporządzenie Rady (WE) nr 1493/1999, dyrektywę 2000/13/WE, dyrektywę Rady 2001/112/WE.
39. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1333/2008 z dnia 16 grudnia 2008 r. w sprawie dodatków do żywności.
40. Rozporządzenie Komisji (WE) nr 41/2009 z dnia 20 stycznia 2009 r. dotyczące składu i etykietowania środków spożywczych odpowiednich dla osób nietolerujących glutenu.
41. Rozporządzenie Komisji (WE) nr 124/2009 z dnia 10 lutego 2009 r. ustalające maksymalne zawartości w żywności kokcydiostatyków i histomonostatyków pochodzących z nieuniknionego zanieczyszczenia krzyżowego tymi substancjami pasz, dla których nie są one przeznaczone.
42. Rozporządzenie Komisji (WE) nr 450/2009 z dnia 29 maja 2009 r. w sprawie aktywnych i inteligentnych materiałów i wyrobów przeznaczonych do kontaktu z żywnością.
43. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 470/2009 z dnia 6 maja 2009 r. ustanawiające wspólnotowe procedury określania maksymalnych limitów pozostałości substancji farmakologicznie czynnych w środkach spożywczych pochodzenia zwierzęcego oraz uchylające rozporządzenie Rady (EWG) nr 2377/90 oraz zmieniające dyrektywę 2001/82/WE Parlamentu Europejskiego i Rady i rozporządzenie (WE) nr 726/2004 Parlamentu Europejskiego i Rady.
44. Rozporządzenie Komisji (WE) nr 669/2009 z dnia 24 lipca 2009 r. w sprawie wykonania rozporządzenia (WE) nr 882/2004 Parlamentu Europejskiego i Rady w sprawie zwiększonego poziomu kontroli urzędowych przywozu niektórych rodzajów pasz i żywności niepochodzących od zwierząt i zmieniające decyzję 2006/504/WE.
45. Rozporządzenie Komisji (WE) nr 901/2009 z dnia 28 września 2009 r. dotyczące wieloletniego skoordynowanego wspólnotowego programu kontroli na lata 2010, 2011 i 2012, mającego na celu zapewnienie zgodności z najwyższymi dopuszczalnymi poziomami pozostałości pestycydów w żywności pochodzenia roślinnego i zwierzęcego oraz na jej powierzchni oraz ocenę narażenia na nie konsumenta.

46. Rozporządzenie Komisji (WE) nr 953/2009 z dnia 13 października 2009 r. w sprawie substancji, które mogą być dodawane w szczególnych celach odżywczych do środków spożywczych specjalnego przeznaczenia żywieniowego.

47. Rozporządzenie Komisji (WE) nr 975/2009 z dnia 19 października 2009 r. zmieniające dyrektywę 2002/72/WE w sprawie materiałów i wyrobów z tworzyw sztucznych przeznaczonych do kontaktu ze środkami spożywczymi.

48. Rozporządzenie Komisji (WE) nr 983/2009 z dnia 21 października 2009 r. w sprawie udzielania i odmowy udzielenia zezwoleń na oświadczenia zdrowotne dotyczące żywności i odnoszące się do zmniejszenia ryzyka choroby oraz do rozwoju i zdrowia dzieci.

49. Rozporządzenie Komisji (WE) nr 984/2009 z dnia 21 października 2009 r. w sprawie odmowy udzielenia zezwoleń na niektóre oświadczenia zdrowotne dotyczące żywności inne niż dotyczące zmniejszenia ryzyka choroby oraz rozwoju i zdrowia dzieci.

50. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1169/2011 z dnia 25 października 2011 r. w sprawie przekazywania konsumentom informacji na temat żywności, zmiany rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 1924/2006 i (WE) nr 1925/2006 oraz uchylecia dyrektywy Komisji 87/250/EWG, dyrektywy Rady 90/496/EWG, dyrektywy Komisji 1999/10/WE, dyrektywy 2000/13/WE Parlamentu Europejskiego i Rady, dyrektyw Komisji 2002/67/WE i 2008/5/WE oraz rozporządzenia Komisji (WE) nr 608/2004.

Dyrektywy Wspólnot Europejskich

1. Dyrektywa Rady 78/142/EWG z dnia 30 stycznia 1978 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do materiałów i wyrobów zawierających monomer chlorku winylu przeznaczonych do kontaktu ze środkami spożywczymi.

2. Dyrektywa Komisji 80/766/EWG z dnia 8 lipca 1980 r. ustanawiająca wspólnotową metodę analizy do celów urzędowej kontroli poziomu monomeru chlorku winylu w materiałach i wyrobach, które przeznaczone są do kontaktu ze środkami spożywczymi.

3. Dyrektywa Komisji 81/432/EWG z dnia 29 kwietnia 1981 r. ustanawiająca wspólnotową metodę analizy do celów urzędowej kontroli chlorku winylu uwalnianego z materiałów i wyrobów do środków spożywczych.

4. Dyrektywa Komisji 81/712/EWG z dnia 28 lipca 1981 r. ustanawiająca wspólnotowe metody analiz w celu kontroli spełniania kryteriów czystości przez niektóre dodatki stosowane w środkach spożywczych.

5. Dyrektywy Rady 82/711/EWG z dnia 18 października 1982 r. ustanawiające podstawowe zasady, niezbędne w badaniach migracji składników materiałów i wyrobów z tworzyw sztucznych przeznaczonych do kontaktu ze środkami spożywczymi.

6. Dyrektywa Rady 84/500/EWG z dnia 15 października 1984 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich dotyczących wyrobów ceramicznych przeznaczonych do kontaktu ze środkami spożywczymi.
7. Dyrektywa Rady 85/572/EWG z dnia 19 grudnia 1985 r. ustanawiająca wykaz płynów modelowych do zastosowania w badaniach migracji składników materiałów i wyrobów z tworzyw sztucznych przeznaczonych do kontaktu ze środkami spożywczymi.
8. Dyrektywa Rady 89/108/EWG z dnia 21 grudnia 1988 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do głęboko mrożonych środków spożywczych przeznaczonych do spożycia przez ludzi.
9. Dyrektywa Rady 89/369/EWG z dnia 14 czerwca 1989 r. w sprawie wskazówek lub oznakowań identyfikacyjnych partii towaru, do której należy dany środek spożywczy.
10. Dyrektywa Komisji 92/2/EWG z dnia 13 stycznia 1992 r. ustanawiającej procedurę pobierania próbek oraz wspólnotową metodę analizy do celów urzędowej kontroli temperatur głęboko mrożonych środków spożywczych przeznaczonych do spożycia przez ludzi.
11. Dyrektywa Rady 92/52/EWG z dnia 18 czerwca 1992 r. w sprawie preparatów dla niemowląt i receptur przeznaczonych na wywóz do państw trzecich.
12. Dyrektywa Rady 92/52/EWG z dnia 18 czerwca 1992 r. w sprawie preparatów dla niemowląt i receptur przeznaczonych na wywóz do państw trzecich.
13. Dyrektywa Rady 93/5/EWG z dnia 25 lutego 1993 r. w sprawie pomocy Komisji i współpracy Państw Członkowskich w naukowym badaniu zagadnień dotyczących żywności.
14. Dyrektywa Komisji 93/11/EWG z dnia 15 marca 1993 r. dotyczącej uwalniania N-nitrozoamin i substancji zdolnych do tworzenia N-nitrozoamin ze smoczków do karmienia niemowląt i smoczków do uspokajania wykonanych z kauczuku naturalnego lub elastomerów syntetycznych.
15. Dyrektywa Komisji 96/3/WE z dnia 26 stycznia 1996 r. przyznającej odstępstwo od niektórych przepisów dyrektywy Rady 93/43/EWG w sprawie higieny środków spożywczych w odniesieniu do transportu morskiego płynnych olejów i tłuszczów luzem.
16. Dyrektywa Komisji 96/8/WE z dnia 26 lutego 1996 r. w sprawie żywności przeznaczonej do użycia w dietach o obniżonej energetyczności.
17. Dyrektywa Komisji 98/28/WE z dnia 29 kwietnia 1998 r. przyznającej odstępstwo od niektórych przepisów dyrektywy 93/43/EWG w sprawie higieny środków spożywczych w odniesieniu do transportu morskiego cukru nierafinowanego luzem.
18. Dyrektywa 1999/2/WE Parlamentu Europejskiego i Rady z dnia 22 lutego 1999 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich dotyczących

środków spożywczych oraz składników środków spożywczych poddanych działaniu promieniowania jonizującego.

19. Dyrektywa 1999/3/WE Parlamentu Europejskiego i Rady z dnia 22 lutego 1999 r. w sprawie ustanowienia wspólnotowego wykazu środków spożywczych oraz składników środków spożywczych poddanych działaniu promieniowania jonizującego.

20. Dyrektywa Komisji 1999/21/WE z dnia 25 marca 1999 r. w sprawie dietetycznych środków spożywczych specjalnego przeznaczenia medycznego.

21. Dyrektywa Komisji 2001/15/WE z dnia 15 lutego 2001 r. w sprawie substancji, które mogą być dodawane w szczególnych celach odżywczych do żywności specjalnego przeznaczenia żywieniowego.

22. Dyrektywa 2002/46/WE Parlamentu Europejskiego i Rady z dnia 10 czerwca 2002 roku w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do suplementów żywnościowych.

23. Dyrektywa Komisji 2002/63/WE z dnia 11 lipca 2002 r. ustanawiającej wspólnotowe metody pobierania próbek do celów urzędowej kontroli pozostałości pestycydów w produktach pochodzenia roślinnego i zwierzęcego oraz na ich powierzchni oraz uchylającej dyrektywę 79/700/EWG.

24. Dyrektywa Komisji 2002/72/WE z dnia 6 sierpnia 2002 r. w sprawie materiałów i wyrobów z tworzyw sztucznych przeznaczonych do kontaktu ze środkami spożywczymi.

25. Dyrektywa Komisji 2003/40/WE z dnia 16 maja 2003 r. ustanawiającej wykaz, stężenia graniczne i wymogi w zakresie etykietowania dla składników naturalnych wód mineralnych oraz warunki zastosowania powietrza wzbogaconego w ozon do oczyszczania naturalnych wód mineralnych i wód źródłanych.

26. Dyrektywa Komisji 2006/125/WE z dnia 5 grudnia 2006 r. w sprawie przetworzonej żywności na bazie zbóż oraz żywności dla niemowląt i małych dzieci.

27. Dyrektywa Komisji 2006/141/WE z dnia 22 grudnia 2006 r. w sprawie preparatów do początkowego żywienia niemowląt i preparatów do dalszego żywienia niemowląt oraz zmieniającej dyrektywę 1999/21/WE.

28. Dyrektywy Komisji 2007/42/WE z dnia 29 czerwca 2007 r. w sprawie materiałów i wyrobów wykonanych z folii z regenerowanej celulozy przeznaczonych do kontaktu ze środkami spożywczymi.

29. Dyrektywa Komisji 2008/60/WE z dnia 17 czerwca 2008 r. ustanawiającej szczególne kryteria czystości dotyczące substancji słodzących stosowanych w środkach spożywczych.

Klasyfikacja maksymalnych prędkości wiatru w Polsce i ich skutki działania

| Nr klasy | Prędk. wiatru w m/s na wys.10 m | Prędk. wiatru w km/h na wys.10 m | Charakterystyka wiatru | Skutki działania |
|----------|---------------------------------|----------------------------------|---------------------------------------|---|
| I | 17,2-20,7 | 62-74 | Wiatr gwałtowny | Wiatr łamie gałęzie drzew, chodzenie pod wiatr utrudnione. |
| II | 20,8-24,4 | 75-88 | Wichura | Wiatr powoduje uszkodzenia budynków, zrywa dachówki, łamie całe drzewa. |
| III | 24,5-28,4 | 89-102 | Silna wichura | Wiatr wyrwa drzewa z korzeniami, powoduje duże uszkodzenia budynków(zrywanie dachów, łamanie wież i słupów energetycznych). |
| IV | 28,5-32,6 | 103-117 | Gwałtowna wichura | Wiatr powoduje rozległe zniszczenia, zagrożenie życia. |
| V | ≥ 32,7 | ≥ 118 | Wiatr huraganowy lub trąba powietrzna | Wiatr powoduje zniszczenia i spustoszenia, możliwe wypadki śmiertelne. |
| V-1 | 35,1-50,1 | 126-180 | Silny niszczycielski dewastujący | |
| V-2 | 50,2-70,2 | 181-253 | | |
| V-3 | ≥ 70,3 | ≥ 254 | | |

Źródło: *Identyfikacja i ocena ekstremalnych zdarzeń meteorologicznych i hydrologicznych w Polsce w II połowie XX wieku*,
http://klimat.imgw.pl/wp-content/uploads/2013/01/4_7.pdf, 12.12.2015.

Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla wiatrów

| Stopień zagrożenia | Warunki | Możliwe straty/ zalecenia |
|-------------------------------------|---|---|
| Stopień zagrożenia 1 (żółty) | 54 km/h < V _{śr} ≤ 72 km/h, tj. 15 m/s < V _{śr} ≤ 20 m/s lub w porywach 72 km/h < V ≤ 90 km/h, tj. 20 m/s < V ≤ 25 m/s | Uszkodzenia budynków, dachów; szkody w drzewostanie, łamanie gałęzi i drzew; utrudnienia komunikacyjne. Zalecana ostrożność, potrzeba śledzenia komunikatów i rozwoju sytuacji pogodowej. |
| Stopień zagrożenia 2 (pomarańczowy) | 72 km/h < V _{śr} ≤ 90 km/h, tj. 20 m/s < V _{śr} ≤ 25 m/s lub w porywach 90 km/h < V ≤ 115 km/h, tj. 25 m/s < V ≤ 32 m/s | Uszkodzenia budynków, dachów; łamanie i wyrywanie drzew z korzeniami; utrudnienia w komunikacji; uszkodzenia linii napowietrznych. Zalecana ostrożność, potrzeba śledzenia komunikatów i rozwoju sytuacji pogodowej. |
| Stopień zagrożenia 3 (czerwony) | V _{śr} > 90 km/h, tj. V _{śr} > 25 m/s lub w porywach V > 115 km/h, tj. V > 32 m/s | Niszczenie zabudowań, zrywanie dachów; niszczenie linii napowietrznych; duże szkody w drzewostanie; znaczne utrudnienia w komunikacji; zagrożenie życia. |

gdzie: V_{śr} – średnia prędkość wiatru (w treści ostrzeżenia w km/h),
V – prędkość wiatru w porywach (w treści ostrzeżenia w km/h).

Źródło: *Klasyfikacja stopni zagrożeń groźnych zjawisk meteorologicznych*,
<http://www.imgw.pl/>, 22.11.2015.

Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia
meteorologicznego dla silnych mrozów

| Stopień zagrożenia | Kryteria | Skutki |
|--|--|---|
| Stopień zagrożenia 1 (żółty) | -25°C < T _{min} ≤ -20°C T _{max} > -10°C Czas trwania – co najmniej dwa dni. | Ryzyko wychłodzenia organizmów, odmrożenia, zamarznięcia. |
| Stopień zagrożenia 2 (pomarańczowy) | -25°C > T _{min} ≤ -20°C T _{max} < -10°C Czas trwania – co najmniej dwa dni. | Duże ryzyko wychłodzenia organizmów, odmrożenia, zamarznięcia, zamarzanie instalacji i urządzeń hydrotechnicznych. |
| Stopień zagrożenia 3 (czerwony) | T _{min} ≤ -25°C Czas trwania – co najmniej dwa dni. | Na znacznym obszarze bardzo duże ryzyko wychłodzenia organizmów, odmrożenia, zamarznięcia, zamarzanie instalacji i urządzeń hydrotechnicznych, zagrożenie życia. |

Źródło: *Zagrożenia okresowe występujące w Polsce*, aktualizacja, Wydział analiz RCB,
styczeń 2013, s. 11.

Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla intensywnych opadów śniegu

| Stopień zagrożenia | Kryteria | Skutki |
|-------------------------------------|--|--|
| Stopień zagrożenia 1 (żółty) | Przyrost pokrywy śnieżnej powyżej 15 cm w ciągu 24 godz. | Utrudnienia komunikacyjne, śliskość na drogach. |
| Stopień zagrożenia 2 (pomarańczowy) | Przyrost pokrywy śnieżnej powyżej 25 cm w ciągu 24 godz. na terenach nizinnych lub powyżej 40 cm w ciągu 24 godz. na obszarach położonych powyżej 600 m npm. | Utrudnienia komunikacyjne, nieprzejezdność dróg lokalnych. |
| Stopień zagrożenia 3 (czerwony) | Przyrost pokrywy śnieżnej powyżej 35 cm w ciągu 24 godz. na terenach nizinnych lub powyżej 50 cm w ciągu 24 godz. na obszarach położonych powyżej 600 m npm. | Duże trudności komunikacyjne, nieprzejezdność dróg, uszkodzenia drzewostanu, uszkodzenia dachów, zagrożenie życia. |

Źródło: *Zagrożenia okresowe występujące w Polsce*, aktualizacja, Wydział analiz RCB, styczeń 2013, s. 11.

Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla zawiei i zamieci śnieżnych

| Stopień zagrożenia | Kryteria | Skutki |
|-------------------------------------|---|---|
| Stopień zagrożenia 1 (żółty) | Niestabilna pokrywa śnieżna lub słabe albo umiarkowane opady śniegu i wiatr o: $V_{\text{śr}} > 6 \text{ m/s}$ <i>$V_{\text{śr}}$ – średnia prędkość wiatru</i> | Tworzenie się zasp, utrudnienia komunikacyjne. |
| Stopień zagrożenia 2 (pomarańczowy) | a) Niestabilna pokrywa śnieżna lub słabe albo umiarkowane opady śniegu i wiatr o: $V_{\text{śr}} > 10 \text{ m/s}$ b) silne opady śniegu i wiatr o: $V_{\text{śr}} > 6 \text{ m/s}$ <i>$V_{\text{śr}}$ – średnia prędkość wiatru</i> | Szybkie tworzenie się zasp, utrudnienia komunikacyjne. |
| Stopień zagrożenia 3 (czerwony) | Silne opady śniegu i wiatr o: $V_{\text{śr}} > 10 \text{ m/s}$ <i>$V_{\text{śr}}$ – średnia prędkość wiatru</i> | Liczne, szybko narastające zasy na dużych obszarach, trudności w komunikacji, nieprzejezdność dróg. |

Źródło: *Zagrożenia okresowe występujące w Polsce*, aktualizacja, Wydział analiz RCB, styczeń 2013, s. 11.

Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla opadów marznących

| Sopień zagrożenia | Warunki | Możliwe straty/zalecenia |
|-------------------------------------|---|--|
| Stopień zagrożenia 1 (żółty) | Opady marznącej mżawki lub deszczu, trwające w jednym miejscu do 12 godz. | Gołoledź; śliskość dróg, jezdni i chodników; utrudnienia komunikacyjne. |
| Stopień zagrożenia 2 (pomarańczowy) | Opady marznącej mżawki lub deszczu, trwające w jednym miejscu od 12 do 24 godz. | Gołoledź; trudności komunikacyjne; oblodzenie dróg, utrudnienia w ruchu pieszym; uszkodzenia drzewostanu i linii napowietrznych. |
| Stopień zagrożenia 3 (czerwony) | Opady marznącej mżawki lub deszczu, trwające w jednym miejscu powyżej 12 godz. | Gołoledź; szybkie oblodzenie dróg; duże trudności komunikacyjne i w ruchu pieszym; uszkodzenia drzewostanu i linii napowietrznych. |

Źródło: *Klasyfikacja stopni zagrożeń groźnych zjawisk meteorologicznych*, <http://www.imgw.pl/>, 22.11.2015.

Zestawienie parametrów systemów RFID pracujących w różnych zakresach częstotliwości

| | | | |
|-------------------------------|------------------------|------------------------|------------------------|
| Częstotliwość pracy systemu | 100-135 kHz | 13,56 MHz | 2,45 GHz |
| Odległość odczytu | do 120 cm | do 100 cm | do 12 m |
| Zasilanie taga | pasywne | pasywne | semipasywne aktywne |
| Żywotność | zależnie od obciążenia | zależnie od obciążenia | do 10 lat |
| Szybkość obiektu (opakowania) | do 3 m/s | do 3 m/s | do 20 m/s |
| Obszar odczytu | okrąg | zależny od anteny | kierunkowy |
| Przenikanie przeszkód | wysokie | wysokie | zależy od materiału |
| Użycie na metalu | ograniczone | ograniczone | możliwe |

Źródło: *Automatyczna identyfikacja w systemach logistycznych*,
red. nauk. S. Kwaśniewski, P. Zajac, PW, Wrocław 2004, s. 154.

Rodzaje komunikatów standardowych

| Grupa | Rodzaj |
|--------------|--|
| Transakcyjne | <p>ORDER (<i>Purchase Order</i>) – komunikat przesyłany od kupującego do sprzedającego, w celu zamówienia towaru, z dokładnym określeniem wielkości zamawianych produktów, terminów i miejsca dostawy.</p> <p>ORDRSP (<i>Purchase Order Response</i>) – komunikat potwierdzający otrzymanie zamówienia przez sprzedawcę, wysłany do kupującego.</p> <p>DESADV (<i>Despatch Advice</i>) – komunikat wysłany przez sprzedawcę do strony kupującej, zawierający opis ładunku wysyłanego przez sprzedającego.</p> <p>RECADV (<i>Receiving Advice</i>) – komunikat przesyłany przez kupującego do sprzedającego w celu poinformowania go, jakie towary zostały przez niego odebrane i zaakceptowane.</p> <p>INVOIC (<i>Invoice</i>) – komunikat nadany przez stronę sprzedającą spełniający rolę faktury.</p> <p>SLSRPT (<i>Sales Report</i>) – komunikat wysyłany przez sprzedającego do dostawcy/producenta, informujący o bieżącej ilości sprzedaży określonych towarów (raport ten może służyć producentowi do planowania produkcji).</p> <p>INVRPT (<i>Inventory Report</i>) – komunikat nadawany przez sprzedawcę do producenta/dostawcy, informujący o bieżącym stanie zapasów towaru.</p> <p>SLSFCT (<i>Sales Forecast Report</i>) – komunikat nadawany przez sprzedawcę do zainteresowanego podmiotu, zawierający dane o przewidywanej sprzedaży poszczególnych towarów.</p> |
| Informacyjne | <p>PRICAT (<i>Price Catalogue</i>) – komunikat, który umożliwia transmisję informacji na temat cen i szczegółów katalogowych dotyczących towarów i usług oferowanych przez sprzedawcę nabywcy.</p> <p>PRODAT (<i>Product Data</i>) – komunikat zbliżony do PRICAT, ale zawiera on tylko dane taktyczne i funkcjonalne danego produktu – nie zawiera danych handlowych i logistycznych.</p> <p>PARTIN (<i>Party Information</i>) – komunikat, który jest wymieniany pomiędzy partnerami biznesowymi, którzy rozpoczynają współpracę przy użyciu EDI (jego zadaniem jest wymiana podstawowych danych o firmach).</p> |
| Transportowe | <p>HANMOV (<i>Cargo/Goods Handling and Movement</i>) – komunikat zlecający przygotowanie towaru do transportu, w przypadku gdy znajduje się on w centrum dystrybucji firmy trzeciej (komunikat jest wysyłany przez sprzedającego lub kupującego w zależności od tego, kto jest odpowiedzialny za transport towaru).</p> <p>INSDS (<i>Instruction to Despatch</i>) – komunikat używany do specyfikacji transportu towarów dla firmy zewnętrznej</p> |

| | |
|----------------------|---|
| | <p>(spedytor, przewoźnik, centrum logistyczne), jest on wysyłany przez sprzedającego lub kupującego w zależności od tego, kto jest odpowiedzialny za transport towaru (wiadomość wykorzystywana do identyfikacji miejsca i terminu dostawy).</p> <p>IFTMBF (<i>Firm Booking</i>) – komunikat używany do rezerwacji usług transportowych, jeżeli taka rezerwacja jest wymagana.</p> <p>IFTMBC (<i>Booking Confirmation</i>) – wiadomość ta jest wysyłana przez firmę (spedytor, przewoźnik) jako odpowiedź na rezerwację usługi transportowej i jest potwierdzeniem sygnalizującym, że rezerwacja jest akceptowana, warunkowo akceptowana lub odrzucona.</p> <p>IFTMBI (<i>Transport Instruction</i>) – komunikat będący zamówieniem usługi transportowej wysyłany przez kupującego lub sprzedającego do dostawcy usług transportowych (instrukcja może dotyczyć jednej bądź kilku przesyłek odpowiednio opakowanych).</p> <p>IFCSUM (<i>Forwarding and Consolidation Summary</i>) – komunikat będący zbiorczą specyfikacją usług transportowych (jest równoważny wielokrotnemu komunikatowi <i>Transport Instruction</i>).</p> <p>IFTSTA (<i>Transport Status</i>) – komunikat pozwalający na uzyskanie informacji o stanie i miejscu, w którym aktualnie znajduje się przesyłka.</p> <p>IFTMAN (<i>Arrival Notice</i>) – komunikat wysyłany przez firmę spedycyjną, informujący o przybyciu przesyłki do odbiorcy i sposobie jej odebrania. Jedna nota przyjazdowa odpowiada jednej dostawie towaru.</p> |
| Komunikaty finansowe | <p>PAYMUL (<i>Payment Order</i>) – komunikat ten wysyła kupujący do swojego banku, aby zlecić obciążenie własnego rachunku i zrealizować wyszczególnione płatności na rzecz jednego lub więcej wierzycieli.</p> <p>DEBMUL (<i>Multiple Debit Advice</i>) – wiadomość wysyłana przez bank do klienta, informująca go o obciążeniach jego konta. Informacje mogą dotyczyć jednej lub więcej transakcji finansowych lub handlowych, takich jak faktury, noty kredytowe, noty debetowe, opłaty za usługi bankowe.</p> <p>CREMUL (<i>Multiple Credit Advice</i>) – wiadomość wysyłana przez bank do klienta, informująca go o wpływach na jego koncie. Informacje mogą dotyczyć jednej lub więcej transakcji finansowych lub handlowych, takich jak faktury, noty kredytowe, noty debetowe, opłaty za usługi bankowe.</p> <p>BANSTA (<i>Banking Status</i>) – wiadomość wysłana przez bank do klienta, informująca go o stanie realizacji zleceń finansowych (przelewy) lub odpowiedzi na wcześniejsze pytania.</p> |

Źródło: *Kody kreskowe i inne globalne standardy w biznesie*, red. nauk. Hałas E., ILiM, Poznań 2012, ss. 145-147; *Podstawowe fakty EDI*, <http://www.edi.pl/>, 02.04.2014.

Wykaz rozporządzeń Komisji UE i ustaw krajowych, które wymusiły stosowanie *traceability*

1. Rozporządzenie 178/2002 nr 1935/2004 w sprawie artykułów i wyrobów przeznaczonych do kontaktu z żywnością.
2. Rozporządzenie 852/2004 z 29.04.2004 w sprawie higieny środków spożywczych.
3. Rozporządzenie 1224/2009 dotyczące produktów rybnych, którego wymogi mają zastosowanie od dnia 1 stycznia 2013 r.
4. Rozporządzenie 1223/2009 dotyczące produktów kosmetycznych, którego wymogi mają zastosowanie od dnia 11 lipca 2013 r.
5. Rozporządzenie 995/2010 dotyczące produktów drzewnych, którego wymogi mają zastosowanie od dnia 3 marca 2013 r.
6. Ustawa z 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia.
7. Ustawa z dnia 28 lipca 2005 r. o zmianie ustawy o warunkach zdrowotnych żywności i żywienia oraz niektórych innych ustaw.
8. Ustawa o wymaganiach weterynaryjnych dla produktów pochodzenia zwierzęcego z dnia 29.01.2004 r.

Źródło: opracowanie własne.

Wybrane ustawy i rozporządzenia dotyczące ochrony informacji niejawnych

1. Konstytucja Rzeczypospolitej Polskiej.
2. Ustawa z 22.01.1999 r. o ochronie informacji niejawnej, Dz. U. 11/99 poz. 95. Znowelizowana 3.02.2001 (nowelizacja weszła w życie 8.04.2001).
3. Rozporządzenie Rady Ministrów z 9.02.1999 w sprawie wzorów: kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, odmowy wydania świadectwa bezpieczeństwa przemysłowego, Dz. U. 18/99 poz. 157.
4. Rozporządzenie Prezesa Rady Ministrów z 25.02.1999 w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych, Dz. U. 18/99 poz. 162.
5. Rozporządzenie MSWiA oraz ON z 26.02.1999 w sprawie oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach, Dz. U. 18/99 poz. 167.
6. Rozporządzenie MSWiA oraz ON z 26.02.1999 w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów. Dz. U. 18/99 poz. 168.
7. Ustawa z 29.08.97 o ochronie danych osobowych. Dz. U. z 29.10.97 (znowelizowana ustawą z 25.08.2001).
8. Rozporządzenie MSWiA z 3.06.98 w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Dz. U. z 30.06.98.
9. Ustawa z 29.09.1994 o rachunkowości. Dz. U. nr 121 poz. 591. Znowelizowana – nowelizacja obejmuje również szczegółowe wytyczne dotyczące techniki komputerowej stosowanej w rachunkowości (nowelizacja obowiązuje od 01.01.2002).
10. Ustawa z 18.09.2001 o podpisie elektronicznym Dz. U. nr 130, poz. 1450 (wejście w życie 16.08.2002).
11. Ustawa z 4.02.1994 prawo autorskie i prawa pokrewne. Dz. U. 94.24.83.
12. Ustawa z 21.08.1997 prawo o obrocie papierami wartościowymi. Dz. U. 118/97.
13. Ustawa z 16.04.1993 o zwalczaniu nieuczciwej konkurencji. Dz.U. 93.47.211.
14. Ustawa z 10.01.2003 o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych. Dz. U. nr 17, poz. 155.
15. Ustawa z 21.07.2000 Prawo Telekomunikacyjne Dz. U. nr 73, poz. 852.

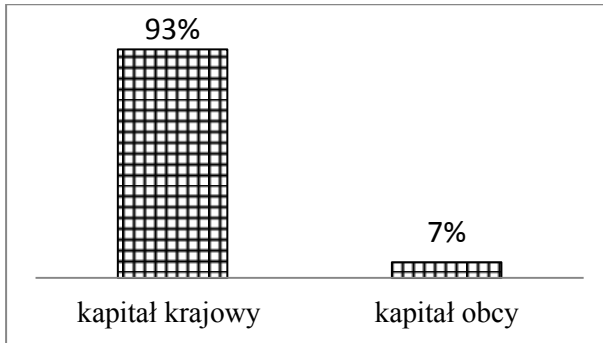
16. Ustawa z 6.09.2001 o dostępie do informacji publicznej Dz. U. nr 112, poz. 1198.
17. Ustawa z 27.07.2001 o ochronie baz danych Dz. U. nr 128, poz. 1402 (wejście w życie 9.11.2002).
18. Ustawa z 18.07.2002 o świadczeniu usług drogą elektroniczną. Dz. U. nr 144, poz. 1204 (wejście w życie 10.03.2003 z wyjątkiem art. 5 ust. 5 który stosuje się od dnia uzyskania przez Polskę członkostwa w Unii Europejskiej).
19. Ustawa z 05.07.2002 o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym. Dz. U. nr 126/02 poz. 1068 (wejście w życie 10.11.2002).
20. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
21. Rozporządzenie Prezesa Rady Ministrów z 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z dnia 8 września 2005 r.).
22. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych.
23. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne.
24. Rozporządzenie Ministra Obrony Narodowej z dnia 2 listopada 2011 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.
25. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.
26. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego.
27. Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych.
28. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

Źródło: opracowanie własne.

Uzupełniająca tabela i wykresy do podrozdziału 6.2

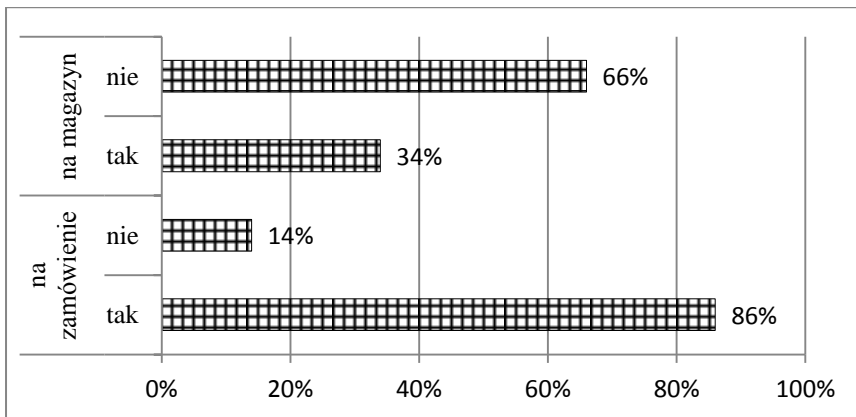
Wykres 6.4

Odsetek firm z udziałem kapitału krajowego
i zagranicznego



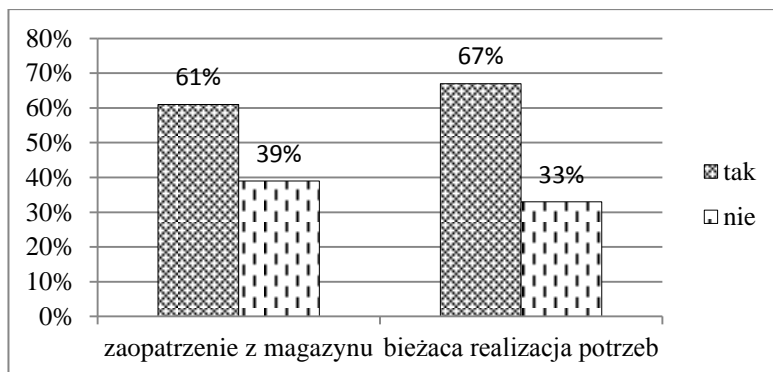
Wykres 6.5

Odsetek odpowiedzi na pytanie o sposób organizacji produkcji lub usług
w firmach realizowane w wariantach: na zamówienie i na magazyn



Wykres 6.10

Odsetek firm, w których podstawą produkcji i/lub usług jest zaopatrzenie z magazynu lub bieżąca realizacja potrzeb



Wykres 6.16

Odsetek firm, które zapewniają zgodność funkcjonowania z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie w zależności od wielkości podmiotu

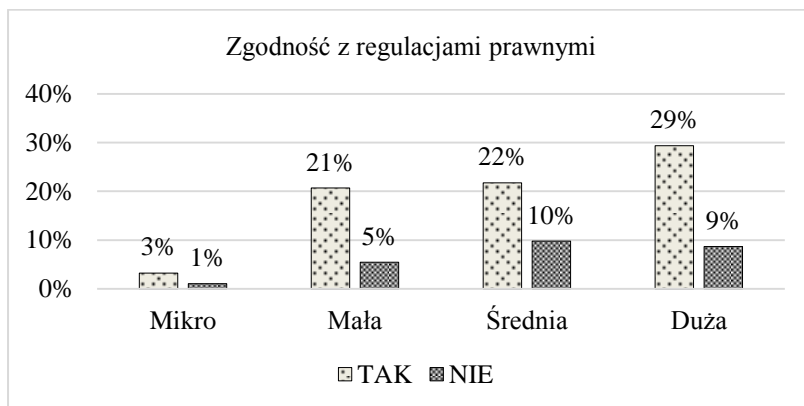


Tabela 6.16

Rozkład odpowiedzi w zależności od formy własności firmy

| Forma własności firmy | N = 92 | | | | Suma |
|-----------------------|--------|-----|-----|-----|------|
| | TAK | % | NIE | % | |
| Prywatna | 14 | 15% | 17 | 18% | 31 |
| Państwowa | 36 | 39% | 6 | 7% | 42 |
| Spółdzielcza | 3 | 3% | 0 | 0% | 3 |
| Komunalna | 16 | 17% | 0 | 0% | 16 |
| Razem | 69 | 75% | 23 | 25% | 92 |

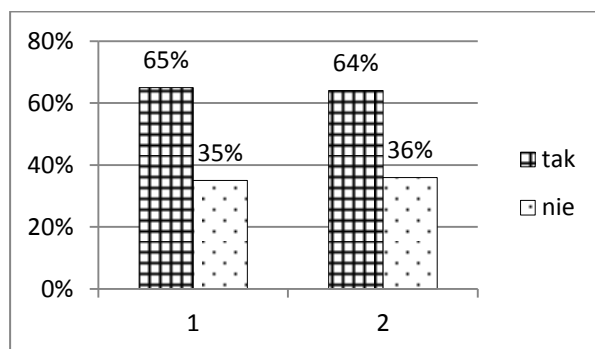
Tabela 6.20

Liczebność obserwowana dla danej grupy

| Forma własności firmy | N = 92 | | | |
|-----------------------|----------------|-----|----------------|-----|
| | Liczebność TAK | % | Liczebność NIE | % |
| Mikro | 2 | 2% | 2 | 2% |
| Mała | 17 | 18% | 7 | 8% |
| Średnia | 15 | 16% | 14 | 15% |
| Duża | 19 | 21% | 16 | 17% |
| Razem | 53 | 58% | 39 | 42% |

Wykres 6.20

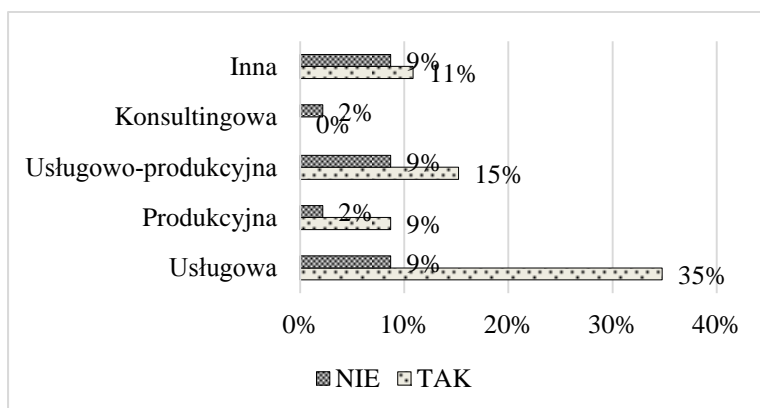
Odsetek firm, dla których znane są narzędzia wspomagające zarządzanie kryzysowe zarówno dla fazy projektowania, jak i wdrażania



Planowanie – 1 Wdrażanie – 2

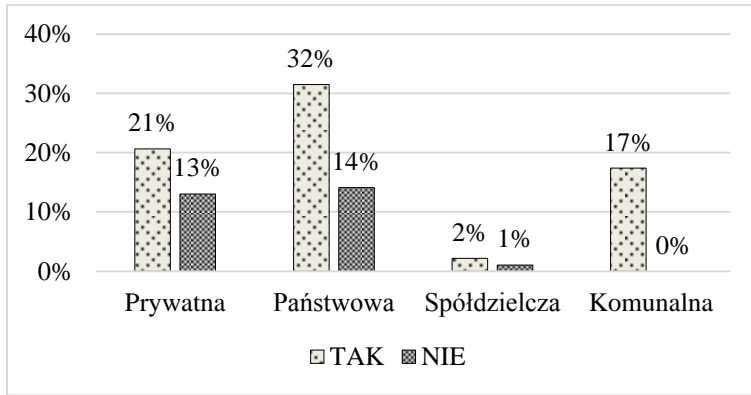
Wykres 6.31

Odsetek odpowiedzi na pytanie o znajomość struktury Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego w zależności od rodzaju prowadzonej działalności



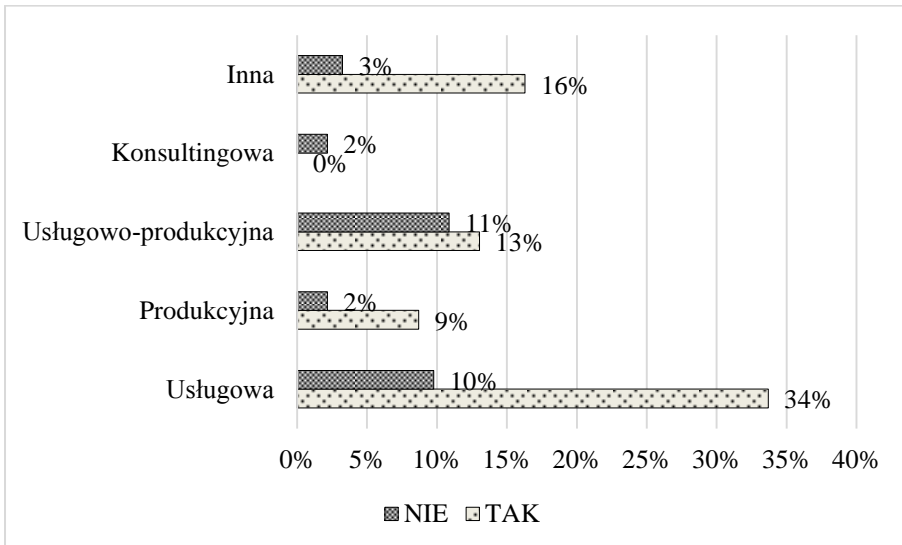
Wykres 6.34

Odsetek odpowiedzi o odpowiedzialność za bezpieczeństwo logistyki w zależności od rodzaju własności



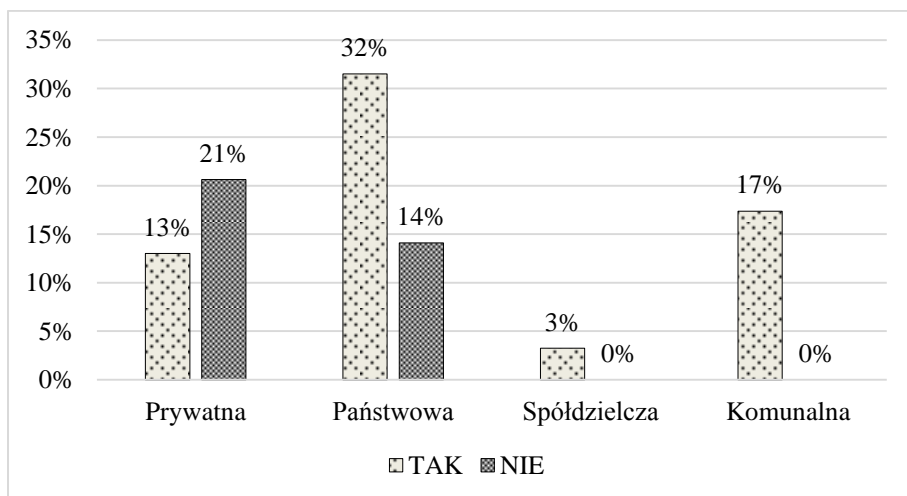
Wykres 6.35

Odsetek odpowiedzi o odpowiedzialność za bezpieczeństwo logistyki w zależności od rodzaju wykonywanej działalności



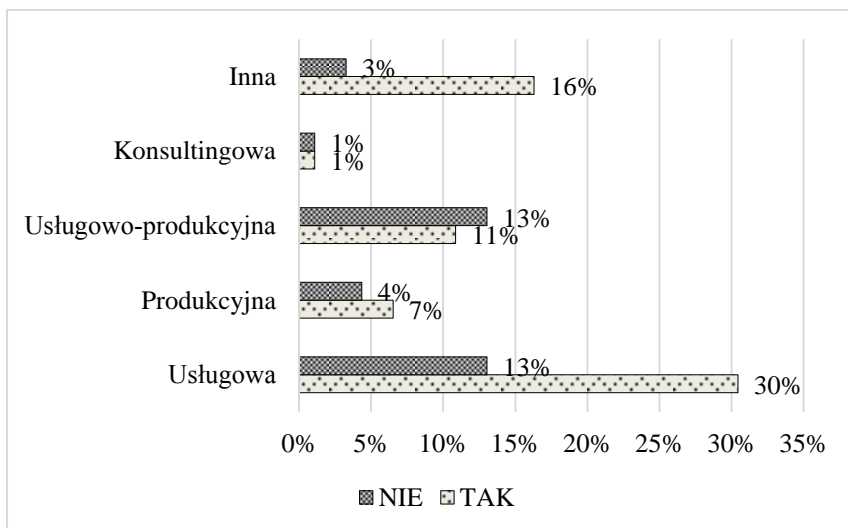
Wykres 6.50

Odsetek odpowiedzi na pytanie o wdrożenie procedur współdziałania z otoczeniem w zależności od rodzaju własności firmy



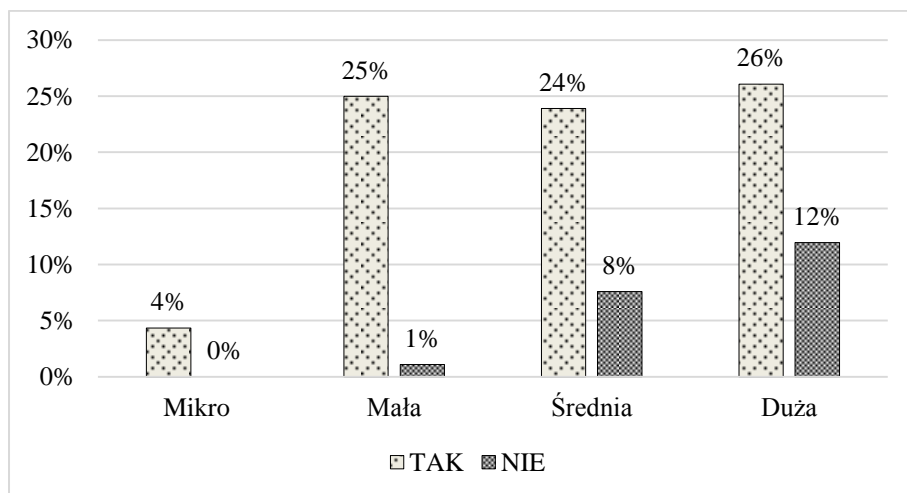
Wykres 6.51

Odsetek odpowiedzi na pytanie o wdrożenie procedur współdziałania z otoczeniem w zależności od rodzaju prowadzonej działalności



Wykres 6.53

Odsetek odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskimi w zależności od wielkości firmy



Wykres 6.59

Odsetek odpowiedzi na pytanie o samodzielne bądź specjalistyczne prowadzenie szkoleń w zależności od wielkości firmy

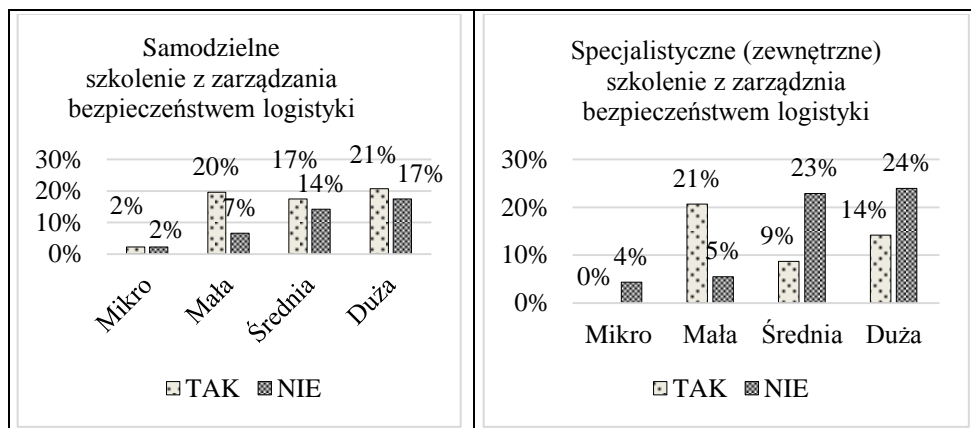


Tabela 6.57

Rozkład odpowiedzi wyboru wariantów szkoleń w zależności
od formy własności firmy

| Forma własności firmy | N = 92 (wariant a) | | | | N = 92 (wariant b) | | | |
|-----------------------|--------------------|-----|-----|-----|--------------------|-----|-----|-----|
| | TAK | % | NIE | % | TAK | % | NIE | % |
| Prywatna | 10 | 11% | 21 | 23% | 5 | 5% | 26 | 28% |
| Państwowa | 26 | 28% | 16 | 17% | 16 | 17% | 26 | 28% |
| Spółdzielcza | 3 | 3% | 0 | 0% | 3 | 3% | 0 | 0% |
| Komunalna | 16 | 17% | 0 | 0% | 16 | 17% | 0 | 0% |
| Razem | 55 | 60% | 37 | 40% | 52 | 43% | 52 | 57% |

Wykaz rysunków

| | | |
|-----------|--|-----|
| Rys. 1.1. | Bezpieczeństwo w kontekście obszaru wiedzy nauk społecznych, ścisłych, przyrodniczych, technicznych | 19 |
| Rys. 1.2. | Struktura bezpieczeństwa narodowego ze szczególnym uwzględnieniem bezpieczeństwa gospodarczego | 28 |
| Rys. 1.3. | Płaszczyzny kształtowania bezpieczeństwa państwa (narodowego) | 29 |
| Rys. 1.4. | Determinanty bezpieczeństwa gospodarczego | 35 |
| Rys. 2.1. | Składowe bezpieczeństwa systemu logistycznego | 48 |
| Rys. 2.2. | Zagrożenia dla systemów logistycznych | 55 |
| Rys. 2.3. | Formy relacji we współdziałaniu | 60 |
| Rys. 2.4. | Zależności pomiędzy podmiotami | 61 |
| Rys. 3.1. | Schemat satelitarnego systemu śledzenia pojazdu | 94 |
| Rys. 3.2. | Algorytm komunikacji pomiędzy obiektem transportowym a systemem monitorowania (centrum nadzoru) | 96 |
| Rys. 3.3. | Schemat satelitarnego systemu śledzenia pojazdu | 97 |
| Rys. 4.1. | Koncepcja analizy systemowej bezpieczeństwa środowiska naturalnego | 130 |
| Rys. 4.2. | Algorytm opracowania raportu cząstkowego dla zagrożeń naturalnych i cywilizacyjnych środowiska naturalnego | 144 |
| Rys. 4.3. | Model sieci ekologii | 149 |
| Rys. 5.1. | Architektura CRM | 156 |
| Rys. 5.2. | Obszary odpowiedzialności EAM | 163 |
| Rys. 5.3. | Elektroniczna platforma logistyczna | 167 |
| Rys. 5.4. | Architektura EPCglobal | 174 |
| Rys. 5.5. | Standardy EDI | 183 |
| Rys. 5.6. | Model funkcjonowania systemu <i>traceability</i> w łańcuchu dostaw | 186 |
| Rys. 5.7. | <i>Traceability</i> w śledzeniu partii produkcji | 188 |
| Rys. 5.8. | Uproszczony schemat informacyjny z miejscami narażonymi na ataki aktywne i pasywne | 194 |
| Rys. 5.9. | Procesy wdrażania i zarządzania bezpieczeństwem informacji | 203 |
| Rys. 6.1. | Rola modelu w obserwacji systemu | 209 |
| Rys. 6.2. | Ogólny schemat modelowania systemowego | 213 |
| Rys. 6.3. | Istotne czynniki kompleksowego modelowania systemów | 218 |
| Rys. 6.4. | System bezpieczeństwa gospodarczego w kontekście bezpieczeństwa systemów logistycznych | 222 |
| Rys. 6.5. | Sektory bezpieczeństwa gospodarczego w systemie bezpieczeństwa narodowego | 223 |

| | | |
|------------|--|-----|
| Rys. 6.6. | Model logistycznego podmiotu bezpieczeństwa na przykładzie przedsiębiorstwa produkcyjnego – przepływ strumienia rzeczowego | 227 |
| Rys. 6.7. | Model logistycznego podmiotu bezpieczeństwa na przykładzie przedsiębiorstwa produkcyjnego – przepływ informacji | 228 |
| Rys. 6.8. | Relacja bezpieczeństwa logistyki z systemem bezpieczeństwa narodowego | 229 |
| Rys. 6.9. | Relacje w ujęciu horyzontalno-wertykalnym systemu bezpieczeństwa narodowego z systemami logistycznymi | 229 |
| Rys. 6.10. | Ogólny schemat modelowania zależności pomiędzy modelem systemu logistycznego a systemem (obiekt) bezpieczeństwa narodowego | 230 |
| Rys. 6.11. | Procedura konstruowania MZBSL (schemat matematycznego modelowania) | 307 |
| Rys. 6.12. | Hierarchia celów (etap I) | 308 |
| Rys. 6.13. | Model zarządzania bezpieczeństwem systemu logistycznego | 311 |

Wykaz wykresów

| | | |
|-------------|--|-----|
| Wykres 3.1. | Długość autostrad w Polsce w latach 2010-2014, w km | 80 |
| Wykres 3.2. | Ilość wypadków drogowych na 10 tys. pojazdów samochodowych i ciągników zarejestrowanych | 82 |
| Wykres 3.3. | Ważniejsze przyczyny wypadków drogowych | 82 |
| Wykres 3.4. | Ofiary wypadków drogowych | 83 |
| Wykres 3.5. | Stan techniczny nawierzchni kolejowej na dzień 31.12.2012 | 87 |
| Wykres 3.6. | Wielkość ogółem powierzchni magazynów zamkniętych w Polsce w latach 2007-2012 w mln m ² | 107 |
| Wykres 3.7. | Nowoczesna powierzchnia magazynowa w latach 2007-2013 w tys. m ² | 107 |
| Wykres 3.8. | Wypadki w 2014 r. w transporcie i gospodarce magazynowej – zestawienie liczbowe | 115 |
| Wykres 3.9. | Wypadki w 2014 r. w transporcie i gospodarce magazynowej – liczba dni niezdolnych do pracy spowodowanych wypadkami ogółem | 116 |
| Wykres 5.1. | Liczba udanych ataków hackerskich | 192 |
| Wykres 5.2. | Liczba incydentów zgłaszanych w latach 2005-2011 | 192 |
| Wykres 6.1. | Charakterystyka próby badawczej – struktura wielkości badanych firm | 239 |
| Wykres 6.2. | Wyróżnienie firm ze względu na formę własności | 240 |
| Wykres 6.3. | Rodzaj prowadzonej działalności przez firmy | 240 |
| Wykres 6.4. | Odsetek firm z udziałem kapitału krajowego i zagranicznego | 374 |
| Wykres 6.5. | Odsetek odpowiedzi na pytanie o sposób organizacji produkcji lub usług w firmach realizowane w wariantach: na zamówienie i na magazyn | 374 |
| Wykres 6.6. | Odsetek odpowiedzi na pytanie: czy organizacja produkcji /usług w Firmie/Instytucji jest realizowana na zamówienie dla konkretnego klienta/ usługodawcy czy „na magazyn” w zależności od wielkości firmy | 242 |
| Wykres 6.7. | Odsetek firm organizujących procesy produkcji i usług na zamówienie dla konkretnego klienta oraz „na magazyn” w zależności od formy własności firmy | 243 |
| Wykres 6.8. | Odsetek firm organizujących procesy produkcji i usług na zamówienie konkretnego klienta oraz w oparciu o „na magazyn” w zależności od rodzaju firmy w zależności od profilu działalności firmy | 244 |

| | | |
|--------------|---|-----|
| Wykres 6.9. | Odsetek firm organizujących procesy produkcji i usług na zamówienie konkretnego klienta oraz w oparciu o sposób „na magazyn” w zależności od finansowania działalności | 244 |
| Wykres 6.10. | Odsetek firm, w których podstawą produkcji i/lub usług jest zaopatrzenie z magazynu lub bieżąca realizacja potrzeb | 375 |
| Wykres 6.11. | Odsetek firm stosujących zaopatrzenie „z magazynu” jako podstawę organizacji produkcji i/lub usług oraz według bieżącej realizacji potrzeb w zależności od wielkości | 246 |
| Wykres 6.12. | Odsetek firm organizujących produkcję i/lub usługi w oparciu o „na magazyn” oraz sposobu „na zamówienie” w zależności od formy własności | 246 |
| Wykres 6.13. | Odsetek firm stosujących zaopatrzenie „z magazynu” jako podstawę organizacji produkcji i/lub usług w zależności od rodzaju działalności | 247 |
| Wykres 6.14. | Odsetek firm, które wdrożyły podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych w zależności od wielkości | 249 |
| Wykres 6.15. | Odsetek firm, które wdrożyły podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych w zależności od formy własności | 249 |
| Wykres 6.16. | Odsetek firm, które zapewniają zgodność funkcjonowania z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie w zależności od wielkości podmiotu | 375 |
| Wykres 6.17. | Odsetek firm, które zapewniają zgodność funkcjonowania z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie w zależności od formy własności | 252 |
| Wykres 6.18. | Odsetek firm, w których dokonuje się analizy kosztów zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego ze względu na wielkość firmy | 254 |
| Wykres 6.19. | Odsetek firm, w których dokonuje się analizy kosztów zabezpieczenia przed skutkami zagrożeń (zakłóceń) bezpieczeństwa w systemie zarządzania kryzysowego w kontekście formy własności | 255 |
| Wykres 6.20. | Odsetek firm, dla których znane są narzędzia wspomagające zarządzanie kryzysowe zarówno dla fazy projektowania, jak i wdrażania | 377 |

| | | |
|--------------|---|-----|
| Wykres 6.21. | Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania oraz etapu realizacji systemów logistycznych w zależności od wielkości firm | 257 |
| Wykres 6.22. | Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania oraz fazy realizacji systemów logistycznych w zależności od formy własności | 258 |
| Wykres 6.23. | Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania systemów logistycznych oraz etapu realizacji w zależności od rodzaju prowadzonej działalności | 259 |
| Wykres 6.24. | Odsetek odpowiedzi na pytanie o znajomość narzędzi wspomagających zarządzanie kryzysowe dla etapu projektowania systemów logistycznych w zależności od rodzaju finansowania działalności | 260 |
| Wykres 6.25. | Odsetek odpowiedzi na pytanie o ujmowanie działań zapewniających bezpieczeństwo planowanych i realizowanych procesów logistycznych w strategii firmy w zależności od wielkości firmy | 261 |
| Wykres 6.26. | Odsetek odpowiedzi na pytanie: czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji w zależności od wielkości firmy? | 264 |
| Wykres 6.27. | Odsetek odpowiedzi na pytanie: czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji w zależności od formy własności? | 265 |
| Wykres 6.28. | Odsetek odpowiedzi na pytanie: czy opracowane są procedury zarządzania ryzykiem utraty ciągłości działania Firmy/Instytucji w zależności od rodzaju prowadzonej działalności? | 266 |
| Wykres 6.29. | Odsetek firm stosujących formy monitoringu w zależności od formy własności firmy | 268 |
| Wykres 6.30. | Odsetek odpowiedzi na pytanie o znajomość struktury Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego w zależności od wielkości firmy | 270 |
| Wykres 6.31. | Odsetek odpowiedzi na pytanie o znajomość struktury Firmy/Instytucji pod względem podatności na wewnętrzne i/lub zewnętrzne zagrożenia (zakłócenia) funkcjonowania systemu logistycznego w zależności od rodzaju prowadzonej działalności | 377 |

| | | |
|--------------|--|-----|
| Wykres 6.32. | Odsetek odpowiedzi wyboru wariantu zarządzania bezpieczeństwem systemu logistycznego w zależności od wielkości firmy | 273 |
| Wykres 6.33. | Odsetek odpowiedzi dotyczących wyboru wariantu zarządzania bezpieczeństwem systemu logistycznego w zależności od rodzaju prowadzonej działalności | 275 |
| Wykres 6.34. | Odsetek odpowiedzi na pytanie o odpowiedzialność za bezpieczeństwo logistyki w zależności od rodzaju własności | 378 |
| Wykres 6.35. | Odsetek odpowiedzi na pytanie o odpowiedzialność za bezpieczeństwo logistyki w zależności od rodzaju wykonywanej działalności | 378 |
| Wykres 6.36. | Częstość odpowiedzi na pytanie o odpowiedzialność za bezpieczeństwo logistyki w zależności od rodzaju finansowania działalności | 278 |
| Wykres 6.37. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od wielkości firmy | 281 |
| Wykres 6.38. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie odbudowy w zależności od wielkości firmy | 282 |
| Wykres 6.39. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie zapobiegania w zależności od formy własności | 283 |
| Wykres 6.40. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od formy własności firmy | 284 |
| Wykres 6.41. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie odbudowy w zależności od własności firmy | 284 |
| Wykres 6.42. | Odsetek odpowiedzi na pytanie o stosowanie procedur zarządzania bezpieczeństwem w fazie planowania w zależności od rodzaju prowadzonej działalności | 285 |
| Wykres 6.43. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie zapobiegania w zależności od rodzaju działalności | 286 |
| Wykres 6.44. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od rodzaju prowadzonej działalności | 287 |
| Wykres 6.45. | Odsetek odpowiedzi dotyczących stosowania procedur zarządzania bezpieczeństwem systemu logistycznego w fazie reagowania w zależności od rodzaju prowadzonej działalności | 288 |

| | | |
|--------------|--|-----|
| Wykres 6.46. | Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy w zależności od wielkości podmiotu | 290 |
| Wykres 6.47. | Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy w zależności od formy własności firmy | 291 |
| Wykres 6.48. | Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy w zależności od rodzaju prowadzonej działalności | 292 |
| Wykres 6.49. | Odsetek odpowiedzi na pytanie o sposób zarządzania zasobami firmy w zależności od sposobu finansowania działalności | 292 |
| Wykres 6.50. | Odsetek odpowiedzi na pytanie o wdrożenie procedur współdziałania z otoczeniem w zależności od rodzaju własności firmy | 379 |
| Wykres 6.51. | Odsetek odpowiedzi na pytanie o wdrożenie procedur współdziałania z otoczeniem w zależności od rodzaju prowadzonej działalności | 379 |
| Wykres 6.52. | Odsetek odpowiedzi na pytanie o wdrożenie procedur współdziałania z otoczeniem w zależności od sposobu finansowania działalności | 295 |
| Wykres 6.53. | Odsetek odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskimi w zależności od wielkości firmy | 380 |
| Wykres 6.54. | Odsetek odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskimi w zależności od rodzaju prowadzonej działalności | 297 |
| Wykres 6.55. | Odsetek odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskimi w zależności od sposobu finansowania działalności | 298 |
| Wykres 6.56. | Odsetek odpowiedzi w zależności od wielkości firmy | 299 |
| Wykres 6.57. | Odsetek odpowiedzi w zależności od rodzaju prowadzonej działalności | 300 |
| Wykres 6.58. | Odsetek odpowiedzi w zależności od sposobu finansowania działalności | 301 |
| Wykres 6.59. | Odsetek odpowiedzi na pytanie o samodzielne bądź specjalistyczne prowadzenie szkoleń w zależności od wielkości firmy | 380 |
| Wykres 6.60. | Odsetek odpowiedzi w przypadku wyboru wariantu „a” i „b” w zależności od formy własności firmy | 303 |
| Wykres 6.61. | Odsetek odpowiedzi w przypadku wyboru wariantu „a” „b” w zależności od sposobu finansowania działalności | 304 |

Wykaz tabel

| | | |
|--------------|---|-----|
| Tabela 1.1. | Systematyzacja istoty i treści bezpieczeństwa ekonomicznego państwa | 25 |
| Tabela 1.2. | Klasyfikacja determinant bezpieczeństwa gospodarczego | 39 |
| Tabela 3.1. | Zestawienie kosztów funkcjonowania przedsiębiorstwa międzynarodowego transportu samochodowego | 69 |
| Tabela 3.2. | Poziom rozwoju infrastruktury technicznej w Polsce z perspektywy badań Światowego Forum Ekonomicznego | 71 |
| Tabela 3.3. | Przewozy ładunków – stan na 31.12. 2014 r. | 77 |
| Tabela 3.4. | Przewozy pasażerów – stan na 31.12. 2014 r. | 78 |
| Tabela 3.5. | Stan pojazdów samochodowych i ciągników (w tys. szt.) zarejestrowanych na 31.12.2014 r. | 81 |
| Tabela 3.6. | Ryzyko wystąpienia ofiar śmiertelnych w zależności od rodzaju transportu, w EU w latach 2008-2012 | 81 |
| Tabela 3.7. | Przewozy ładunków w Polsce | 88 |
| Tabela 3.8. | Tabor kolejowy w Polsce | 88 |
| Tabela 3.9. | Przewozy w milionach pasażerokilometrów w Polsce | 88 |
| Tabela 3.10. | Ekonomiczne skutki wypadków kolejowych w Polsce w 2012 r. | 89 |
| Tabela 3.11. | Zestawienie przyczyn zdarzeń i wypadków kolejowych w Polsce w latach 2011 i 2012 | 90 |
| Tabela 3.12. | Długość linii kolejowych, na których uruchomiono łączność GSM-R w Europie | 104 |
| Tabela 3.13. | Czynniki decydujące o bezpieczeństwie w magazynie | 111 |
| Tabela 3.14. | Požary magazynów w Polsce w latach 2000-2010 | 117 |
| Tabela 3.15. | Częstość pożarów dla magazynów handlowych (zamknięte i zadaszone) w Polsce w latach 2000-2009 | 118 |
| Tabela 4.1. | Tabela zagrożeń wraz z okresem wystąpienia | 134 |
| Tabela 4.2. | Całkowita emisja dwutlenku węgla w Polsce (w tys. ton) | 142 |
| Tabela 6.1. | Klasyfikacja modeli badawczych | 211 |
| Tabela 6.2. | Rodzaje modeli i kryteria ich wyróżnienia | 212 |
| Tabela 6.3. | Klasyfikacja związków przyczynowych | 217 |
| Tabela 6.4. | Wartość współczynnika kontyngencji C Pearsona a siła relacji pomiędzy badanymi czynnikami | 237 |
| Tabela 6.5. | Charakterystyka próby badawczej – struktura wielkości badanych firm | 239 |
| Tabela 6.6. | Wyróżnienie firm ze względu na formę własności | 240 |
| Tabela 6.7. | Rodzaj prowadzonej działalności przez firmy | 240 |
| Tabela 6.8. | Rozkład odpowiedzi na pytanie o organizację produkcji/usług | 241 |

| | | |
|--------------|---|-----|
| Tabela 6.9. | Zestawienie liczebności i odsetka odpowiedzi dla pytania o organizację produkcji i/lub usług w wariantach „na zamówienie” i „na magazyn” w zależności od wielkości firmy | 241 |
| Tabela 6.10. | Rozkład odpowiedzi na pytanie o podstawę produkcji/usług w firmie w zależności od wyboru wariantu | 245 |
| Tabela 6.11. | Rozkład odpowiedzi na pytanie: czy wdrożono podstawy prawne zarządzania kryzysowego w obszarze zarządzania bezpieczeństwem systemów logistycznych? | 248 |
| Tabela 6.12. | Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności | 250 |
| Tabela 6.13. | Rozkład odpowiedzi związany z finansowaniem działalności | 250 |
| Tabela 6.14. | Rozkład odpowiedzi na pytanie o zapewnienie zgodności funkcjonowania podmiotu z aktualnymi regulacjami prawnymi i z wewnętrznymi dokumentami organizacyjnymi wspomagającymi zarządzanie kryzysowe | 251 |
| Tabela 6.15. | Rozkład odpowiedzi w zależności od wielkości firmy | 252 |
| Tabela 6.16. | Rozkład odpowiedzi w zależności od formy własności firmy | 376 |
| Tabela 6.17. | Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności | 253 |
| Tabela 6.18. | Rozkład odpowiedzi w zależności od formy finansowania działalności | 253 |
| Tabela 6.19. | Rozkład odpowiedzi na pytanie nr 3 | 254 |
| Tabela 6.20. | Liczebność obserwowana dla danej grupy | 376 |
| Tabela 6.21. | Liczebność obserwowana dla danej grupy oraz rozkład procentowy odpowiedzi w zależności od rodzaju prowadzonej działalności | 256 |
| Tabela 6.22. | Częstość i odsetek odpowiedzi dla pytania nr 4 | 256 |
| Tabela 6.23. | Rozkład odpowiedzi dla pytania nr 5 | 260 |
| Tabela 6.24. | Rozkład odpowiedzi w zależności od formy własności firmy | 262 |
| Tabela 6.25. | Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności | 263 |
| Tabela 6.26. | Rozkład odpowiedzi w zależności od sposobu finansowania działalności | 263 |
| Tabela 6.27. | Rozkład odpowiedzi dla pytania nr 6 | 264 |
| Tabela 6.28. | Rozkład odpowiedzi na pytanie nr 7 | 267 |
| Tabela 6.29. | Rozkład odpowiedzi w zależności od wielkości firmy | 267 |
| Tabela 6.30. | Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności | 268 |

| | | |
|--------------|---|-----|
| Tabela 6.31. | Rozkład odpowiedzi w zależności od sposobu finansowania działalności | 269 |
| Tabela 6.32. | Rozkład odpowiedzi na pytanie nr 8 | 270 |
| Tabela 6.33. | Rozkład odpowiedzi w zależności od formy własności firmy | 271 |
| Tabela 6.34. | Rozkład odpowiedzi w relacji do kryterium rodzaju prowadzonej działalności | 271 |
| Tabela 6.35. | Rozkład odpowiedzi na pytanie nr 9 | 272 |
| Tabela 6.36. | Rozkład odpowiedzi w zależności od wielkości firmy | 273 |
| Tabela 6.37. | Rozkład odpowiedzi w zależności od formy własności firmy | 274 |
| Tabela 6.38. | Rozkład odpowiedzi dla pytania nr 10 | 276 |
| Tabela 6.39. | Rozkład odpowiedzi w zależności od wielkości firmy | 276 |
| Tabela 6.40. | Rozkład odpowiedzi w zależności od formy własności firmy | 277 |
| Tabela 6.41. | Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności | 277 |
| Tabela 6.42. | Rozkład odpowiedzi dla pytania nr 11 | 279 |
| Tabela 6.43. | Rozkład odpowiedzi wyboru wariantu w zależności od wielkości firmy | 280 |
| Tabela 6.44. | Częstość rozkładu odpowiedzi w zależności od rodzaju prowadzonej działalności w fazie planowania | 285 |
| Tabela 6.45. | Rozkład odpowiedzi dla pytania nr 12 | 289 |
| Tabela 6.46. | Rozkład odpowiedzi na pytanie nr 13 | 293 |
| Tabela 6.47. | Częstość odpowiedzi na pytanie o potwierdzenie wdrożenia procedur w zależności od wielkości firmy | 294 |
| Tabela 6.48. | Rozkład odpowiedzi w zależności od formy własności firmy | 294 |
| Tabela 6.49. | Rozkład odpowiedzi w zależności od rodzaju prowadzonej działalności | 295 |
| Tabela 6.50. | Rozkład odpowiedzi na pytanie nr 14 | 296 |
| Tabela 6.51. | Rozkład odpowiedzi na pytanie o zgodność procedur wewnętrznych ze standardami krajowymi i europejskim w zależności od wielkości firmy | 296 |
| Tabela 6.52. | Rozkład odpowiedzi w zależności od formy własności firmy | 297 |
| Tabela 6.53. | Rozkład odpowiedzi do pytania nr 17 | 299 |
| Tabela 6.54. | Rozkład odpowiedzi w zależności od formy własności firmy | 300 |
| Tabela 6.55. | Rozkład odpowiedzi do pytania nr 18 | 302 |
| Tabela 6.56. | Rozkład odpowiedzi w zależności od wielkości firmy | 302 |
| Tabela 6.57. | Rozkład odpowiedzi dotyczących wyboru wariantów szkoleń w zależności od formy własności firmy | 381 |
| Tabela 6.58. | Rozkład wyboru wariantu szkolenia w zależności od rodzaju prowadzonej działalności | 303 |

Wykaz załączników

| | | |
|----------------|--|-----|
| Załącznik 1. | Charakterystyka wybranych firm, w których przeprowadzono badania | 340 |
| Załącznik 2. | Ankieta | 342 |
| Załącznik 2.1. | Analiza ilości użytych określenia „logistyka”, „logistycznych” i „logistycznego” w Strategiach Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej i „Białej Księdze” 2013 | 346 |
| Załącznik 3.1. | Wykaz podstawowych aktów prawnych dotyczących transportu kolejowego | 349 |
| Załącznik 3.2. | Logistyczny softwarowy pakiet firmy Swisslog | 353 |
| Załącznik 3.3. | Podstawowe przepisy prawne regulujące odpowiedzialność materialną pracowników magazynowych | 354 |
| Załącznik 3.4. | Rozporządzenia i dyrektywy EWG i WE w sprawie higieny i bezpieczeństwa żywności | 355 |
| Załącznik 4.1. | Klasyfikacja maksymalnych prędkości wiatru w Polsce i ich skutki działania | 362 |
| Załącznik 4.2. | Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla wiatrów | 363 |
| Załącznik 4.3. | Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla silnych mrozów | 364 |
| Załącznik 4.4. | Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla intensywnych opadów śniegu | 365 |
| Załącznik 4.5. | Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla zawiei i zamieci śnieżnych | 366 |
| Załącznik 4.6. | Stopnie zagrożenia w zależności od kryteriów wydawania ostrzeżenia meteorologicznego dla opadów marznięcych | 367 |
| Załącznik 5.1. | Zestawienie parametrów systemów RFID pracujących w różnych zakresach częstotliwości | 368 |
| Załącznik 5.2. | Rodzaje komunikatów standardowych | 369 |
| Załącznik 5.3. | Wykaz rozporządzeń Komisji UE i ustaw krajowych, które wymusiły stosowanie <i>traceability</i> | 371 |
| Załącznik 5.4. | Wybrane ustawy i rozporządzenia dotyczące ochrony informacji niejawnych | 372 |
| Załącznik 6.1. | Uzupełniające tabele i wykresy do podrozdziału 6.2 | 374 |



ISBN 978-83-7283-729-5