LOGISTYKA W BEZPIECZEŃSTWIE – BEZPIECZEŃSTWO W LOGISTYCE. WYBRANE ZAGADNIENIA

Andrzej SZYMONIK

Streszczenie: Artykuł tematycznie związany jest z logistyką w sytuacjach zagrożeń. Na wstępie zostały zaprezentowane kategorie pojęciowe dotyczące bezpieczeństwa, zagrożeń, bezpieczeństwa logistyki. Dokonano klasyfikacji zagrożeń w kontekście bezpieczeństwa systemów logistycznych. Zaprezentowany podziały zakłóceń pokazał szerokie spektrum i wieloaspektowość niekorzystnych działań, jakie mogą wystąpić w funkcjonowaniu procesów w łańcuchu dostaw. Wiele miejsca w artykule poświęcono wynikom badań, przeprowadzonych w 92 firmach. Przedmiotem badań były systemy logistyczne oraz uwarunkowania ich funkcjonowania z uwzględnieniem ewentualnych zagrożeń w podmiotach bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo, logistyka, zagrożenia, system logistyczny.

Wstęp

Bezpieczeństwo jest zjawiskiem dynamicznym, zmieniającym się w czasie, przestrzeni i wymiarze. Architektura bezpieczeństwa to wiedza, działalność praktyczna obejmująca szerokie spektrum form i sposobów organizowania warunków między innymi bezpiecznego funkcjonowania gospodarki tzw. bezpieczeństwa gospodarczego, które ma za zadanie ochronę podmiotów przed destabilizacją, dezintegracją wywołaną negatywnymi czynnikami (zagrożeniami), zarówno wewnętrznymi jak i zewnętrznymi.

Bezpieczeństwo gospodarcze obejmuje takie sektory jak finansowy, energetyczny, transportowy, infrastruktury, w tym infrastruktury krytycznej, środowiska naturalnego, żywnościowego, podmiotów produkcyjnych i usługowych.

Nie sposób pominąć znaczenia i roli w bezpieczeństwie gospodarczym logistyki, sprawnej, skutecznej, nowoczesnej a nade wszystko odpornej na wszelkie zakłócenia i zagrożenia.

Ta logistyka, która ściśle jest związana z podmiotami i instytucjami zaangażowanymi w systemie bezpieczeństwa gospodarczego, w literaturze przedmiotu, nazywana jest: *logistyką bezpieczeństwa lub logistyką w bezpieczeństwie* [1,2]. 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.

1. Wybrane kategorie pojęciowe - obszar bezpieczeństwa

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. [3].

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 [3].

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

Zagrożenie bezpieczeństwa – pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot. Najbardziej klasyczny czynnik środowiska bezpieczeństwa; rozróżnia 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.

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 – 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 zagwarantowania warunków niezbędnych do funkcjonowania podmiotowi bezpieczeństwa (indywidualnemu i zbiorowemu).

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, redukowanie 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, redukowanie ryzyka, niepewności oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla działań logistycznych.

2. Podsystemy logistyczne w logistyce bezpieczeństwa

Zadania realizowane w logistyce bezpieczeństwa (SLwLB) są wykonywane w oparciu o funkcje zarządzania i nowoczesne instrumenty oraz reguły. Do jednej z nich zaliczamy reguły logistyczne 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 zmniejszenia „oporu" ich przepływu, co powinno prowadzić do skrócenia czasu oraz zmniejszenia strat.

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

System logistyczny w logistyce bezpieczeństwa (SLwLB), niezależnie od miejsca funkcjonowania (np. w przedsiębiorstwie produkcyjnym, handlowym, militarnym) jest przeznaczony dla zaspokojenia potrzeb podmiotu bezpieczeństwa. SLwLB tworzą [4]:

- podsystem kierowania – przeznaczony do planowania, organizowania, koordynowania i monitorowania wysiłku logistycznego oraz utrzymywania wydzielonych zasobów (podległych sił i środków) w odpowiedniej gotowości i zdolności do wykonywania zadań;
- podsystem materiałowy – przeznaczony do planowania, organizowania i zaspokajania potrzeb w zakresie realizacji procesu zaopatrywania na rzecz określonego podmiotu bezpieczeństwa;
- 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 i sprzętu technicznego i zabezpieczenia.

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

Podsystemy logistyczne w logistyce bezpieczeństwa traktować możemy również, jako zbiór organów kierowania oraz wykonawczych sprzężonych relacjami informacyjnymi i zasileniowymi przeznaczonymi do utrzymania ciągłości procesów logistycznych realizowanych na rzecz podmiotu bezpieczeństwa.

Można to zapisać jako:

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

gdzie: E – zbiór elementów systemu SLwLB, R – zbiór relacji w więzi organizacyjnej, C – cel działania systemu SLwLB, którym jest zabezpieczenie interesów podmiotu bezpieczeństwa (żywotnych i pożądanych).

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

3. Klasyfikacja zagrożeń

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

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

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

Zagrożenia dla funkcjonowania systemów logistycznych w podmiotach bezpieczeństwa 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, gwałtowne wahania temperatur, gęste mgły, susze, 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, 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 gospodarczego, globalizacji, finansowego, które tak naprawdę dotykają wszystkich, nie omijając procesów i systemów logistycznych. Bezrobocie, mały przyrost PKB, destrukcyjna polityka płacowa i emerytalna, niż demograficzny, napływ tanich wyrobów, to tylko niektóre zagrożenia mające wpływ na funkcjonowanie systemów logistycznych.

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

Zakłócenia te można podzielić ze względu na [5]:

- miejsce zagrożenia – podsystem:
  - dróg wszystkich gałęzi transportu (tj. drogowego, kolejowego, powietrznego, wodnego, morskiego),
  - punktów modalnych sieci logistycznej nazywanych często punktami transportowymi (np. magazyny, samodzielne punkty kontenerowe, lotniska, porty, centra logistyczne itp.),
  - urządzeń pomocniczych ułatwiających obsługę dróg i punktów transportowych,
  - zarządzania (np. brak pełnej identyfikacji i skutków zagrożeń, przeszacowanie możliwości, niewłaściwa interpretacja wyników, brak narzędzi do optymalizacji i symulacji działań, nie uwzględnienie 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 kadrę 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, sfałszowanie 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 możności dysponowania, naturalne zagrożenia, jak pożary, zakłócenia klimatyczne, elektrostatyka, ataki bierne i aktywne, przypadkowe błędy);
- czas trwania:
  - krótkotrwałe, sporadyczne(np. zła jakość w pojedynczej dostawie części w ilości 0.5%),
  - długotrwałe, narastające(zła jakość części w kilku kolejnych dostawach),
  - 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),
  - 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 (np. wzdłuż całego łańcucha dostaw – błędne dane z systemu traceability),
  - 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*[6]. 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 społecznaej 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 oraz wynikających z niewłaściwej struktury organizacyjnej systemu delegowania uprawnień i odpowiedzialności oraz braku lub niewłaściwych zasad postępowania pracowników oraz kierowników komórek organizacyjnych;
- zniezgodności z przepisami prawa powszechnie obowiązującego, regulacji wewnętrznych oraz z zobowiązań umownych
- niedpowiedniego poziomu bezpieczeństwa fizycznego aktywów i osób;
- niewłaściwego zarządzania zasobami teleinformatycznymi wynikającymi z nieaktualnej i przestarzałej technologii teleinformatycznej oraz brakiem 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.

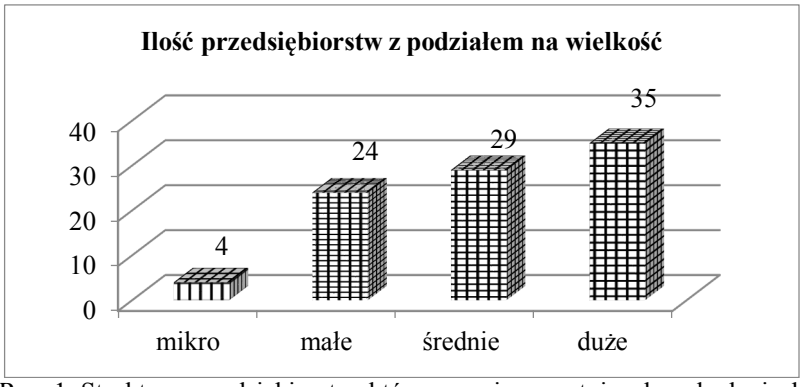
4. Bezpieczeństwo logistyki w praktyce

Przedmiotem badań były systemy logistyczne oraz uwarunkowania ich funkcjonowania z uwzględnieniem ewentualnych zagrożeń w podmiotach bezpieczeństwa. Tymi podmiotami 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 (Policji, Państwowej Straży Pożarnej);
- jednostki administracji rządowej i samorządowej.

Badania w obszarze bezpieczeństwa systemów logistycznych w podmiotach bezpieczeństwa przeprowadzono 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 – rys.1.

Dodatkowo, w celu zweryfikowania wyników badań przeprowadzono pięć rozmów z ekspertami, logistykami dużych firm prywatnych i państwowych, w oparciu o materiały zgromadzone w kwestionariuszu.



Rys. 1. Struktura przedsiębiorstw, które czynnie uczestniczyły w badaniach

W badanych firmach, jak wynika z udzielonych odpowiedzi, największą uwagę (100% odpowiedzi na TAK) 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 (np. na potrzeby Zintegrowanego Systemu Zarządzania według ISO 9001: 2015, ISO/IEC 27001: 2007, ISO 22000: 2005, ISO 14001: 2004 i PN-N-18001: 2004), a niektóre rozwiązania są wynikiem, niestety, negatywnych zdarzeń, zewnętrznych i wewnętrznych, które wywołały stany czasowych trudności w organizacji (inne niż kryzys). Monitoringiem 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 SLwLB z ekspertami wynika, że najwięcej uwagi poświęcano zagrożeniom, które wynikają z:

- makrootoczenia organizacji (np. sytuacji gospodarczej w kraju, polityki płacowej, podatkowej, emerytalnej, demograficznej);
- mikrootoczenia 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 związanymi 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;
- wynikającym z lokalizacji magazynu i infrastruktury drogowej;
- wynikającymi z niezadowolenia pracowników (np. strajk lub inna forma walki z pracodawcą).

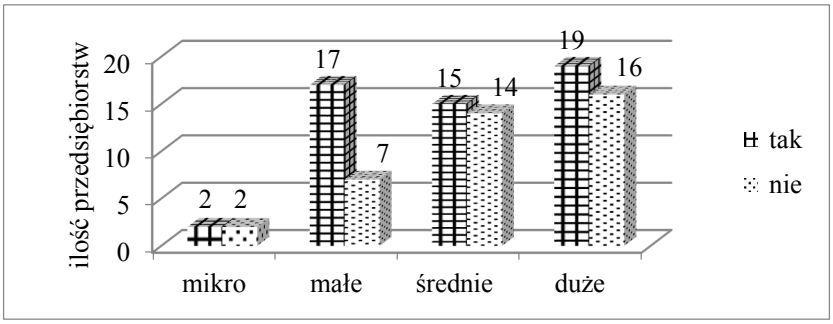
Obecnie najmniej uwagi poświęca się zagrożeniom, do których zalicza się zdarzenia godzące w porządek konstytucyjny państwa (państw), terroryzm, blokady dróg, nielegalne demonstracje, masowa migracja. Również marginalnie traktuje się zagrożenia związane z zmianami klimatycznymi czy wynikające z niezadowolenia pracowników (np. strajk czy inna forma walki z pracodawcą).

Należy podkreślić, że szczególnie w dużych firmach wiele uwagi i zapisów dotyczących zarządzania zdarzeniami kryzysowymi znajduje się w strategii działania firmy, strategii działania kluczowych klientów oraz bezpieczeństwa energetycznego.

Znacznie częściej niż w przeszłości przedsiębiorstwa przywiązują wagę do bezpieczeństwa najwyższego kierownictwa w obszarze zabezpieczenia kapitału intelektualnego związanego z klientami i kontaktami, z procesami, z badaniami i rozwojem w kontekście SLwLB. W firmach, w celu skutecznego przeciwdziałania zabezpieczenia lub wycieku informacji wykorzystuje się takie rozwiązania jak [7]:

- uzyskanie od Urzędu Patentowego – na wynalazek patentu, a na wzór użytkowy, prawa ochronnego;
- zastrzeżenia w umowach z klientami/partnerami zakazu nawiązywania współpracy z pracownikami firmy;
- zastrzeżenia zakazu konkurencji w umowie o pracę;
- klasyfikacja i znakowanie poufnych danych;
- ograniczenie dostępu oraz fizyczna ochrona miejsc przechowywania informacji;
- zabezpieczenie nośników, szyfrowanie danych zapisanych w postaci elektronicznej;
- stosowanie zabezpieczeń systemów informatycznych;
- zobowiązanie pracowników do zachowania poufności udostępnionych informacji;
- zawieranie umów o zachowanie poufności informacji udostępnionych w toku negocjacji,
- wprowadzenie klauzul o poufności do umów z kontrahentami;
- oznakowanie dokumentów, poczty elektronicznej.
- odwoływanie się do sądów, włącznie z dochodzeniem odszkodowania, w przypadku jawnego naruszenia własności, kapitału intelektualnego.

Kolejnym problemem badawczym, który podlegał ocenie był obszar związany z identyfikowaniem i analizowaniem struktury kosztów (strat), zabezpieczenia przed skutkami zagrożeń (zakłóceń) SLwBL?



Rys. 2. Analiza firm w kontekście struktury i bilansowania kosztów (strat) zabezpieczenia przed skutkami zagrożeń (zakłóceń) SLwBL

Na badane 92 firmy, w 53 (odpowiedź na TAK) dokonuje się systematycznej oceny kosztów na zabezpieczenie się przed skutkami działań nieplanowych i ewentualnych strat, powstałych lub mogących powstać w wyniku dotkliwych zagrożeń w systemach logistycznych (rys. 2). Struktura kosztów, w tym logistycznych, w zależności od wielkości firmy, w większym lub mniejszym stopniu dotyczyły:

- zaniechanych projektów i inwestycji (gdy były obarczone zbyt dużym ryzykiem);
- działań prewencyjnych (w różnorodnych obszarach);
- przenoszenia ryzyka na inne podmioty (najczęściej w formie ubezpieczenia i gwarancji);
- tworzenia określonych rezerw finansowych, które umożliwią pokrycie ewentualnych strat.

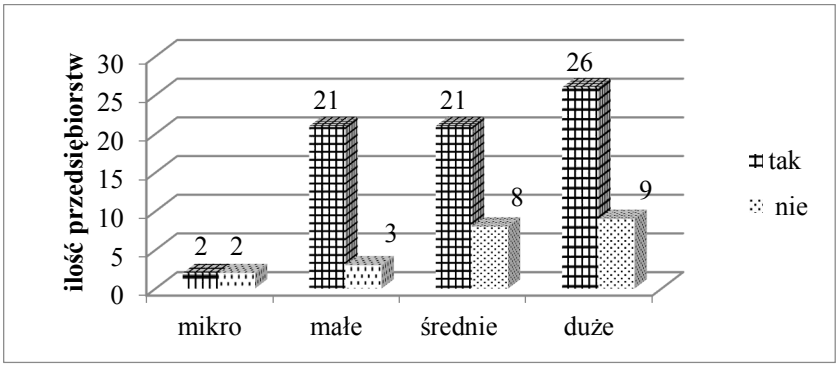
Część z tych kosztów, szczególnie prewencyjnych pokrywają klienci, reszta wydatków pomniejsza zyski firmy. W celu eliminacji ewentualnych strat wiele uwagi przywiązuje się do takich obszarów, jak zarządzanie ryzykiem oraz zaufaniem. Coraz częściej podpisywane są dobrowolne porozumienia między kontrahentami biznesowymi, o dzieleniu się zarówno zyskami jak i stratami.

Czy strategia rozwoju firmy/instytucji ujmuje działania zapewniające bezpieczeństwo planowanych i realizowanych procesów logistycznych – to kolejne pytanie dotyczące obszaru badań w bezpieczeństwie logistyki.

Z badań wynika, że 76% odpowiedzi była na TAK (rys. 3), co świadczy, że jest to istotny i ważny problem, gdyż jest on gwarantem poważnego traktowania firmy na rynku w danej dziedzinie czy branży.

Ujęcie działań zapewniających bezpieczeństwo procesów logistycznych w strategii, jest wymuszone przede wszystkim, wymogami klientów/kontrahentów. Jak wynika z wypowiedzi ekspertów, zatrudnionych w dużych firmach produkcyjno-usługowych, w strategii w obszarze zabezpieczenia przed skutkami zagrożeń (zakłóceń) SLwBL ujmuje się:

- sposób ochrony marki i reputacji firmy;
- sposób identyfikacji, zarządzania, monitorowania bieżącymi i przyszłymi zagrożeniami mającymi wpływ na funkcjonowanie firmy;



Rys. 3. Struktura odpowiedzi na pytanie: *czy strategia rozwoju firmy/instytucji ujmuje działania zapewniające bezpieczeństwo planowanych i realizowanych procesów logistycznych?*

- 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 zagwarantowanie natychmiastowego ich wycofania, w przypadku gdy zagrażają bezpieczeństwu życia i zdrowiu.

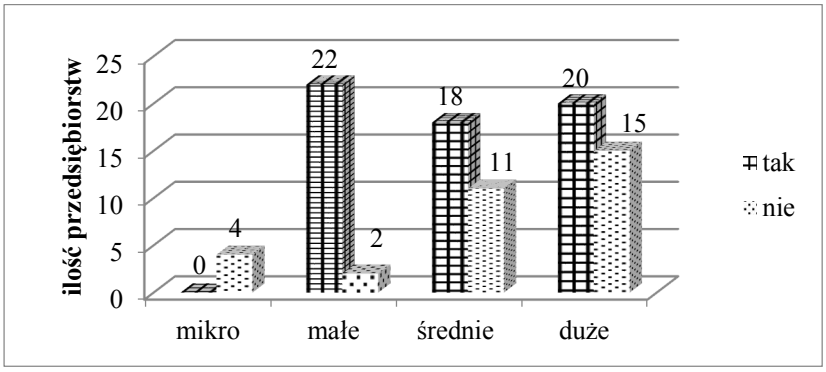
Czy zostały wdrożone procedury współdziałania z otoczeniem zewnętrznym w celu efektywnego zarządzania bezpieczeństwem systemu logistycznego – to następne badane działania, które ściśle są związane z niwelowaniem skutków zagrożeń (zakłóceń) SLwBL.

Z analizy wynika, że 2/3 ankieterów odpowiedziało na TAK, a 1/3 na NIE – co obrazuje rys. 4.

Jak wynika z rozmów z ekspertami, w celu skutecznego niwelowania negatywnych skutków funkcjonowania systemów logistycznych podejmowane są działania długofalowe z podmiotami zewnętrznymi, które obejmują:

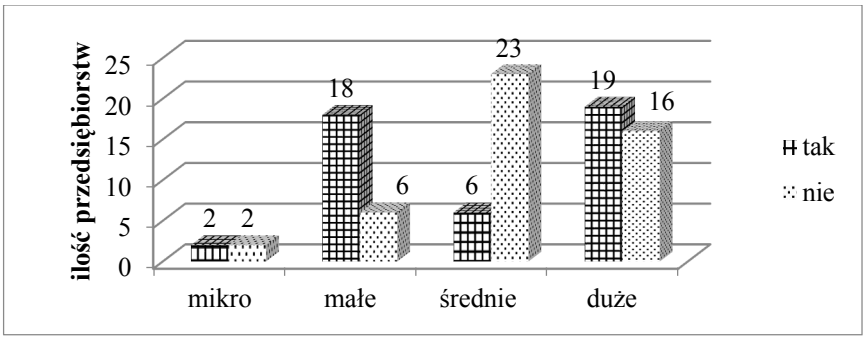
- okresowe audyty bezpieczeństwa (fizycznego, teleinformatycznego, ppoż., urządzeń technicznych) przez wyspecjalizowane firmy;
- systematyczne szkolenia personelu przez zewnętrznych specjalistów w uruchamianiu i realizowaniu procedur na wypadek sytuacji nieplanowych;
- ochronę fizyczną przez profesjonalne 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, energie elektryczną);
- zapasy utrzymywane przez inne podmioty gospodarcze.

Kolejnym problemem badawczym, który podlegał ocenie był obszar związany ze szkoleniem w firmach z zarządzania bezpieczeństwem systemów logistycznych.

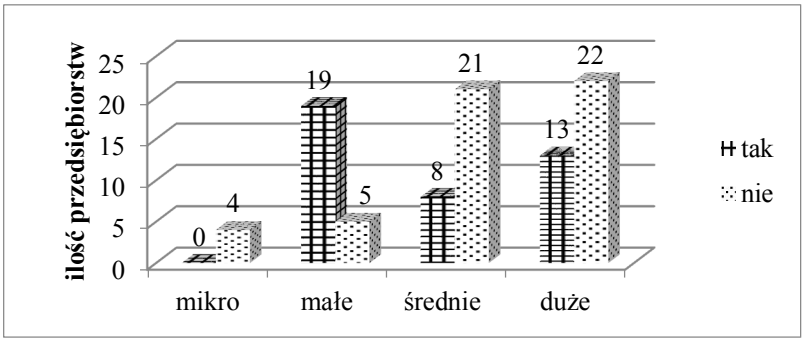


Rys. 4. Struktura odpowiedzi na pytanie: *czy zostały wdrożone procedury współdziałania z otoczeniem zewnętrznym w celu efektywnego zarządzania bezpieczeństwem systemu logistycznego?*

Respondenci mieli do wyboru dwie możliwości: „a" – szkolenie własnymi „siłami" (TAK lub NIE) i „b" – szkolenie za pomocą wyspecjalizowanych firm zewnętrznych (TAK lub NIE).



Rys. 5. Struktura odpowiedzi na pytanie: *czy w firmie powadzi się szkolenia związane z zarządzaniem bezpieczeństwa systemów logistycznych? (dla możliwości a)*



Rys. 6. Struktura odpowiedzi na pytanie: *czy w firmie powadzi się szkolenia związane z zarządzaniem bezpieczeństwa systemów logistycznych? (dla możliwości b)*

Na badane 92 firmy, dla przypadku „a" 50% prowadzi szkolenie własnymi siłami, dla przypadku „b" 40 przedsiębiorstw korzysta z usług firm specjalistycznych, 52 nie korzysta z usług firm specjalistycznych zewnętrznych – rys. 5 i 6. A zatem np. w dużych firmach około 30% nie prowadzi się żadnego szkolenia.

Z informacji uzyskanych od ekspertów wynika, że mankamentem jest brak dobrych firm na rynku, które kompleksowo, systematycznie szkoliłyby personel firmy z obszaru bezpieczeństwa szeroko rozumianego.

Wnioski

Nawet najlepiej zaplanowane działania nie dają gwarancji ich pełnej realizacji z powodu turbulencji środowiska, które to może 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.

Litertaura

1. Jałowiec T., Logistyczne wymiary systemu bezpieczeństwa państwa, [w:] Logistyka 5/2014, s. 617.
2. Szymonik A., Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce, [w:] Logistyka 2/2011, s. 7.
3. Biała Księga Bezpieczeństwa Narodowego, Biuro Bezpieczeństwa Narodowego, Warszawa 2013, s. 247 i 248.
4. Doktryna logistyczna SZ RP DD/4, Sztab. Gen. Warszawa 2004, s. 21.
5. Sienkiewicz P., Teoria i inżynieria bezpieczeństwa systemów, [w:] Zeszyty Naukowe AON nr 1 (66) 2007, s. 254.
6. Sienkiewicz P., Teoria i inżynieria systemów, [w:] Inżynieria systemów bezpieczeństwa, PWE, Warszawa 2015, s. 9.
7. Stec P., Ochrona pracodawcy przed nieuczciwą konkurencją ze strony pracownika, www.valor.pl, 22.12.2015.

Prof. PŁ dr hab. inż. Andrzej SZYMONIK
Katedra Zarządzania Produkcją i Logistyki
Politechnika Łódzka
90-924 Łódź ul. Wólczańska 215
tel. 601 261 602
e-mail: andrzej.szymonik@p.lodz.pl