ZYGMUNT DOMAŃSKI

Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie

*zdomanski@gmail.com*

# Bezpieczeństwo w wybranych dziedzinach logistyki

## *Security in selected areas of logistics*

STRESZCZENIE

Tematem artykułu jest zagrożenie bezpieczeństwa w logistyce i stosowanie nowoczesnych technologii w celu wykrywania, monitorowania i zwalczania tych zagrożeń. Najpierw została dokonana klasyfikacja zagrożeń bezpieczeństwa w logistyce. Następnie przedstawiono wyzwania współczesnej logistyki w tym zakresie. Ukazane zostały także innowacyjne technologie i metody wykrywania oraz eliminacji zagrożeń bezpieczeństwa logistycznego.

ABSTRACT

The topic of the article is the threat of security in logistics and the use of modern technologies to detect them, monitor and eliminate these threats. The first was the classification of safety hazards in logistics. The challenges of modern logistics in this area are presented. The challenges of modern logistics in this area are presented. Innovative technologies and methods of detecting and eliminating logistic security threats have also been demonstrated.

**Słowa kluczowe:** bezpieczeństwo, logistyka, zagrożenia, system logistyczny, logistyka bezpieczeństwa, technologie bezpieczeństwa, zarządzanie bezpieczeństwem.

**Keywords:** security, logistics, threats, logistic system, security logistics, security technologies, security management.

## Wprowadzenie

Rozwój nauk o bezpieczeństwie pozwolił na zmianę sposobu jego postrzegania. Współczesne rozumienie bezpieczeństwa skupia się na jego dynamice

i rozwoju. Bezpieczeństwo to teoria i praktyka, która zapewnia możliwości przetrwania i realizacji własnych interesów przez dany podmiot, w szczególności przez wykorzystanie szans, podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów (Biała Księga BN, s. 247). Bezpieczeństwo dotyczy wielu dziedzin życia człowieka i otaczającego go środowiska. W dobie dynamicznie rozwijającej się gospodarki szczególnie ważną rolę przypisuje się **bezpieczeństwu logistycznemu**, zarówno w zakresie teoretycznym, jak i w praktycznej działalności. Bezpieczeństwo gospodarcze obejmuje szeroki wachlarz obszarów, dziedzin i sektorów, m.in. finanse, energetyka, transport, infrastruktura, produkcja i usługi. Jego podstawowym zadaniem jest ochrona podmiotów gospodarczych przed destabilizacją wywołaną czynnikami wewnętrznymi i zewnętrznymi, w tym działalnością człowieka i negatywnym wpływem sił natury. Ważną rolę odgrywa w tym zakresie nowoczesna, sprawna i skuteczna logistyka, często zwana **logistyką bezpieczeństwa**. W literaturze przedmiotu można znaleźć wiele określeń tego pojęcia. Logistyka bezpieczeństwa, według profesora Andrzeja Szymonika, to wiedza, umiejętności potrzebne do kształtowania racjonalnych strumieni rzeczowych i związanych z nimi strumieni informacji oraz projektowania procesów przepływu materiałów i informacji w celu zagwarantowania warunków niezbędnych do funkcjonowania podmiotowi bezpieczeństwa (Szymonik, 2011, s. 90).

Bezpieczeństwo logistyki natomiast to teoria i praktyka, zapewniająca przepływ strumienia rzeczowego i towarzyszących mu informacji, na rzecz podmiotu bezpieczeństwa, w szczególności przez wykorzystanie szans, podejmowanie wyzwań, zmniejszanie ryzyka oraz przeciwdziałanie wszelakim zagrożeniom dla działań logistycznych. Bezpieczeństwo logistyczne ma także ścisły związek z bezpieczeństwem informacyjnym, polegającym na ochronie informacji osobowych i rzeczowych przed niepożądanym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania oraz stworzeniem możliwości dalszego rozwoju systemów informacyjnych. Bezpieczeństwo logistyczne ma na celu zapewnienie możliwości realizacji sprawnych procesów logistycznych w dowolnym podmiocie bezpieczeństwa, w określonych warunkach, przez wykorzystywanie nowych technologii, innowacyjnych rozwiązań, sprzyjających systemów podatkowych, podejmowanie wyzwań gospodarczych oraz redukowanie do minimum ryzyka. Powstała zatem konieczność stworzenia kompetentnego zarządzania bezpieczeństwem w logistyce. Z tym wiąże się potrzeba ciągłego dosko-

nalenia zawodowego osób ściśle związanych z problematyką bezpieczeństwa, w różnych dziedzinach gospodarki oraz systematycznej edukacji społeczeństwa.

Artykuł wpisuje się w społeczną politykę informacyjno-edukacyjną przez przedstawienie problematyki zagrożeń bezpieczeństwa w logistyce ze szczególnym uwzględnieniem dwóch kluczowych obszarów: przepływu towarów (transport) i przepływu danych i informacji (techniki IT) oraz przybliżenie sposobów, form i metod wykrywania i eliminacji tych zagrożeń.

Materiał źródłowy artykułu stanowi przegląd aktualnej literatury w zakresie bezpieczeństwa wybranych dziedzin logistyki oraz analizę obowiązujących rozwiązań prawnych i polskich norm w tym obszarze.

## Wyzwania i zagrożenia współczesnej logistyki w zakresie bezpieczeństwa

Wszystkie działania w logistyce są obarczone ryzykiem, które może być wywołane pojawiającymi się zagrożeniami lub zakłóceniami. Terminu tego używa się powszechnie na określenie takich sytuacji lub stanów, jak: stan zagrożenia, możliwość wystąpienia zdarzenia nieprzewidzianego, poniesienia straty lub uzyskania wyniku odmiennego od oczekiwanego.

Ryzyko logistyczne może nastąpić wskutek błędów w planowaniu, np. dotyczących wyboru miejsca produkcji, niewłaściwej oceny odbiorców czy użytkowników, nieprawidłowego wyboru dostawców, nieodpowiedniej lokalizacji pewnych działów produkcji itp. Inny rodzaj ryzyka logistycznego dotyczy błędów w bieżącym zarządzaniu przedsiębiorstwem, w zakresie zaopatrzenia, produkcji czy dystrybucji. Biorąc pod uwagę typowy łańcuch logistyczny w przedsiębiorstwie, który obejmuje wszystkie jego działy, daje się zauważyć ryzyko związane z produkowaniem, magazynowaniem, transportowaniem, kontrolą, planowaniem oraz przetwarzaniem informacji.

Wybrane czynniki ryzyka w sferze logistyki wymienili w swojej pracy Piotr Jedynak, Janusz Teczke i Sławomir Wyciślak (Jedynak i in., 2001, s. 90). Są to:

- przekroczenie założonych kosztów logistycznych;
- ewentualne konflikty celów logistycznych;
- błędny wybór własnego bądź obcego magazynowania;
- znaczne obniżenie wartości towarów podczas magazynowania i transportu;
- opracowanie niewłaściwej strategii dystrybucji produktów;

- niewłaściwa strategia recyklingu;
- przestoje i przerwy przy transporcie towarów;
- zmiany polityczno-prawne (np. wysokości ceł, warunków odpraw itp.).

Ponadto istnieje na rynku ryzyko przekupstwa i łapownictwa, które mogą narazić przedsiębiorstwo na znaczne straty.

W **logistyce transportu** można spodziewać się ryzyka wystąpienia szkód, kradzieży czy opóźnień w dostawie.

W **logistce magazynowania** występuje bardzo duże ryzyko strat mogących powstać wskutek ponadnormatywnych zapasów, których koszt utrzymania jest bardzo wysoki, oraz w następstwie zniszczenia lub uszkodzenia towarów, ubytków lub kradzieży.

Skuteczne zarządzanie ryzykiem w celu zapewnienia maksymalnej ochrony zasobów przedsiębiorstwa polega na opracowaniu i zastosowaniu systemu metod i działań zmierzających do obniżenia stopnia oddziaływania ryzyka na funkcjonowanie przedsiębiorstwa i do podejmowania w odpowiednim czasie czynności zapobiegawczych.

Zagrożeniem dla bezpieczeństwa w logistyce są wszystkie wydarzenia, zjawiska czy działania, które zakłócają lub uniemożliwiają zachodzące procesy logistyczne. Zaliczamy do nich: przepływy dóbr rzeczowych i informacji, infrastrukturę, zapasy i koszty logistyczne. Zagrożenia bezpieczeństwa logistycznego można podzielić na kilka grup zobrazowanych w tabeli 1.

Wymienione w powyższej tabeli zagrożenia mogą mieć negatywny wpływ na funkcjonowanie systemów logistycznych, zakłócając prawidłowy przepływ strumienia rzeczy i informacji.

Podziału zagrożeń czy zakłóceń bezpieczeństwa w logistyce można dokonać ze względu na:

a) miejsce zagrożenia,
b) własności fizykalne,
c) czas trwania,
d) zasięg (Szymonik, 2011, s. 7).

**Miejsce zagrożenia** obejmuje wszystkie działy logistyki: zarządzanie, infrastrukturę, przepływ informacji, zaopatrzenie, produkcję, dystrybucję, transport i spedycję, magazynowanie, obsługę zapasów, obsługę klienta.

**Tabela 1**. Rodzaje zagrożeń bezpieczeństwa w logistyce

| Grupa | Rodzaj zagrożenia | Zjawiska i wydarzenia |
|---|---|---|
| I | Klęski żywiołowe | Pożary, powodzie, podtopienia, huragany, burze, gwałtowne zmiany pogody, gęste mgły, zawieje i zamiecie śnieżne, susze. |
| II | Katastrofy | Epidemie chorobowe ludzi, zwierząt i roślin, skażenia chemiczne i biologiczne, katastrofy budowlane, górnicze, hutnicze, komunikacyjne. |
| III | Awarie | Sieci energetycznych, urządzeń i maszyn, transportowe. |
| IV | Inne negatywne zdarzenia spowodowane przez działalność ludzką | Kradzieże, sabotaż, defraudacja mienia. |
| V | Zdarzenia godzące w porządek konstytucyjny państwa | Terroryzm, blokady drogowe, nielegalne demonstracje, masowe migracje. |
| VI | Celowe zakłócenia w obiegu informacji | Niszczenie i zniekształcanie systemów informatycznych, wirusy komputerowe. |
| VII | Skutki kryzysu gospodarczego, finansowego, globalizacji | Bezrobocie, nikły przyrost PKB, destrukcyjna polityka płacowa i emerytalna. |

Źródło: Opracowanie własne na podstawie Szymonik, A. (2011). *Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce*, „Logistyka" 2, s. 7.

**Własności fizykalne** zagrożenia mogą być materialne (np. skażenia, ubytki, uszkodzenia) oraz niematerialne (np. kryzysy w sferze społecznej, politycznej, finansowej) oraz zagrożenia informacyjne (np. wadliwy system identyfikacji czy informacji), a także energetyczne (np. zakłócenia paliwowe, gazowe itp.).

Ze względu na **czas trwania** zagrożenie może być pojedyncze, sporadyczne (np. zła jakość w pojedynczej dostawie części), długotrwałe, narastające przy dostawie złej jakości części w kilku kolejnych transportach, powtarzające się przy cyklicznie dostarczanych wadliwych dostawach.

**Zasięg** zagrożenia można podzielić na cztery grupy: rozległy, lokalny, rozprzestrzeniający się i stabilny. Rozległy czas trwania zagrożenia dotyczy całego łańcucha logistycznego; zasięg lokalny zaś może dotyczyć pojedynczego ogniwa. Czas trwania rozprzestrzeniający się oznacza wydłużenie okresu zagrożenia spowodowane np. dostawą wadliwych części. Stabilny, ale nie rozprzestrzeniający się czas trwania zagrożenia następuje np. z powodu opóźnienia dostaw wadliwych części.

W zamieszczonej tabeli nr 2 przedstawione są zakłócenia systemów logistycznych ze względu na miejsce i przyczyny zagrożenia.

**Tabela 2.** Miejsce zagrożeń i przyczyny zakłóceń systemów logistycznych

| Miejsce zagrożenia | Przyczyna zakłóceń |
|---|---|
| Zarządzanie logistyką | Brak pełnego rozeznania i identyfikacji przewidywanych i istniejących zagrożeń oraz możliwości zapobiegania im, likwidacji i usuwania skutków, nieprawidłowa interpretacja zebranych informacji, niewłaściwa orientacja cenowa, brak rzetelnej informacji o rynku usługodawczym, zaburzony system kontroli pracowników i ich działań. |
| Zaopatrzenie | Wydłużone, nieoptymalne i absorbujące nadmiernie kadrę kierowniczą procedury przetargowe i zakupowe, niespójne kryteria wyboru dostawcy, nieterminowość procesu zakupowego, zła jakość produktu, zawyżona cena lub ilość, niewłaściwy asortyment, przekupstwo, łapownictwo, brak możliwości pozyskania komponentów do wytwarzania, brak buforowego zapasu. |
| Produkcja | Niedomagania systemów wytwarzania, zniszczenia, ubytki, kradzieże zasobów, brak dostępności fachowego personelu, nieuzasadnione przerwy produkcyjne, awarie, pożary, powodzie, katastrofy, sfałszowanie produktu. |
| Dystrybucja | Zignorowanie nowych produktów, nowych producentów, kradzieże, niesprzyjające warunki atmosferyczne, zła jakość wyrobów gotowych, kryzys gospodarczy, lekceważenie zarządzania relacjami z klientem i przepływem wyrobów w łańcuchu dostaw. |
| Transport | 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 komunikacyjne. |
| Magazynowanie | Katastrofy budowlane, zniszczenia urządzeń i towarów, awarie sieci energetycznej i systemu informatycznego, uszkodzenie systemu automatycznej identyfikacji, straty w wyniku ponadnormatywnych zapasów, wypadki pracownicze. |
| Obsługa opakowań | Zniszczenie wyrobów w transporcie na skutek złego doboru opakowań, niedostarczenie opakowań na czas, zanieczyszczenie środowiska niewłaściwym składowaniem opakowań, problemy z pracownikami, którzy dopuszczają się defraudacji mienia lub innych nadużyć, np. wyboru niewłaściwego dostawcy. |
| Obsługa klienta | Brak zapasów, błędne zamówienia i faktury, brak możliwości zlokalizowania produktu, nieterminowość, uszkodzenie wyrobu dostarczonego klientowi, brak reakcji na reklamacje i opóźnienia. |
| Obieg informacji | Utrata poufności, integralności oraz możności dysponowania danymi, awarie sprzętu systemów, błędy w obsłudze. |
| Inne | Naturalne zagrożenia, zakłócenia klimatyczne, pożary, powodzie, ataki bierne i aktywne, kradzieże, przypadkowe błędy ludzkie. |

Źródło: Opracowanie własne na podstawie: Sienkiewicz P. (2007). *Teoria i inżynieria bezpieczeństwa systemów*, „Zeszyty Naukowe AON", nr 1 (66), s. 254.

Pokazane w tabeli nr 2 podziały zagrożeń zakłócających prawidłowe funkcjonowanie procesów logistycznych wskazują na ogrom zadań stojących przed instytucjami odpowiedzialnymi za bezpieczeństwo logistyczne w wielu dziedzinach gospodarki. Przede wszystkim konieczne jest przeprowadzenie kompleksowych badań przez wyspecjalizowane w tej tematyce grupy uczelniane i firmy badawcze. Badania ankietowe przeprowadzone przez prof. Andrzeja Szymonika w nowoczesnych firmach polskich i zagranicznych oraz wybranych jednostkach administracji rządowej i samorządowej potwierdzają taką potrzebę. Przedmiotem badań i rozmów z ekspertami z dziedziny bezpieczeństwa logistyki było funkcjonowanie systemów logistycznych w przedsiębiorstwach z uwzględnieniem ewentualnych zagrożeń ich bezpieczeństwa.

Jak wynika z badań, najwięcej uwagi poświęca się monitorowaniu zgodności funkcjonowania przedsiębiorstwa z zaleceniami prawnymi i organizacyjnymi w obszarze logistyki. Większość rozwiązań stosowanych w przedsiębiorstwach w zakresie bezpieczeństwa w logistyce jest wynikiem analiz przewidywanych zagrożeń przeprowadzonych przez interdyscyplinarne zespoły pracowników pod kierownictwem najwyższego szczebla, wspomagane przez własnych i zewnętrznych audytorów. Świadczy to o randze i priorytetach zagadnienia, jakim jest bezpieczeństwo logistyczne.

Kolejny wniosek wynikający z badań dotyczy skali zagrożeń. Najdotkliwiej przedsiębiorstwa odczuwają zagrożenia z powodu niestabilnej gospodarki, polityki płacowej i podatkowej, zmian w ustawach emerytalnych i zawirowań demograficznych.

Celowa i przypadkowa działalność człowieka także przynosi zakłócenia w funkcjonowaniu systemów logistycznych.

Mniejsze problemy związane z bezpieczeństwem logistycznym stwarzają zmiany klimatyczne, zła lokalizacja infrastruktury magazynowej i drogowej czy zdarzenia związane z niezadowoleniem pracowników, dostawców i klientów.

Istotnym i ważnym elementem dotyczącym bezpieczeństwa logistycznego jest ujęcie tej tematyki w planowaniu strategicznym rozwoju przedsiębiorstwa oraz podejmowanie długofalowej współpracy z podmiotami zewnętrznymi.

Przemyślane i zaplanowane działania pozwalają odpowiednio wcześnie przygotować bazę zabezpieczeń logistycznych, przeprowadzać systematyczne szkolenia personelu, przygotować rezerwową infrastrukturę i zapasy na wypadek sytuacji kryzysowej, zatrudnić profesjonalne firmy ochroniarskie, ustalić formy kontaktu z policją, strażą pożarną, strażą miejską i administracją samorządową.

Jednak nawet najlepiej opracowane plany nie dają pełnej gwarancji ich skutecznej realizacji z powodów zagrożeń nagłych i niemożliwych do przewidzenia. Ponadto w praktyce występują często problemy z wczesnym wykrywaniem zagrożeń mimo sprawnego monitoringu. Niejednokrotnie trudno przewidzieć zasięg i skalę zagrożenia ani określić jego konsekwencje, dlatego opracowanie efektywnego modelu przeciwdziałania skutkom zagrożeń stanowi główne wyzwanie bezpieczeństwa w logistyce.

Profesjonalnie opracowane plany strategiczne uwzględniające monitorowanie i identyfikację zagrożeń, określenie przewidywanej częstotliwości ich wystąpienia, prawdopodobieństwo pojawienia się oraz spodziewane straty pozwalają na odpowiednie przygotowanie sił i środków, na neutralizację negatywnych skutków i pełną realizację zamierzonych zadań w ramach systemu logistycznego, zabezpieczającego określony podmiot.

## Nowoczesne rozwiązania technologiczne wykrywania i eliminacji zagrożeń bezpieczeństwa występujących w logistyce

Wyzwania współczesnej logistyki w dziedzinie bezpieczeństwa obywateli wymagają kompleksowego współdziałania różnych instytucji państwowych i prywatnych, organów administracji rządowej i samorządowej oraz organizacji pozarządowych. W obliczu zagrożeń bezpieczeństwa obywateli w sektorze logistycznym należy dostosować metody i narzędzia pracy oraz system kierowania i zarządzania uwzględniający konieczność dysponowania nowoczesnym, specjalistycznym sprzętem technicznym i informacyjnym.

Działania związane z bezpieczeństwem obywateli skupiają się na procesach informacyjno-decyzyjnych ratownictwa i zarządzania kryzysowego oraz prognozowaniu zagrożeń z wykorzystaniem systemów i urządzeń wspomagających ich monitorowanie, identyfikację i przeciwdziałanie. W celu skutecznej realizacji podejmowanych przedsięwzięć w tym obszarze konieczne jest ciągłe i systematyczne doskonalenie technologii wykrywania i rozwoju zagrożeń, poszukiwanie nowatorskich rozwiązań i innowacji.

Technologie z zakresu bezpieczeństwa w logistyce rozwijają się w dwóch obszarach: bezpieczeństwa technicznego i bezpieczeństwa osobowego. Bezpieczeństwo techniczne dotyczy przede wszystkim projektowania i budowy oraz właściwej eksploatacji obiektów i infrastruktury logistycznej i odnosi się

do wszystkich dziedzin logistyki, czyli zaopatrzenia, produkcji i dystrybucji oraz związanym z nimi transportem, spedycją, magazynowaniem i utylizacją.

Bezpieczeństwo osobowe dotyczy bezpośredniego bezpieczeństwa osób związanych z logistyką, obejmuje stałe monitorowanie, wczesną identyfikację i efektywne przeciwdziałanie zagrożeniom bezpieczeństwa obywateli oraz skuteczne kierowanie ewentualnymi działaniami ratowniczymi i szybkim reagowaniem kryzysowym.

Zapewnienie bezpieczeństwa w obu obszarach opiera się na zastosowaniu nowoczesnych technologii zdefiniowanych przez Ministerstwo Obrony Narodowej pod nazwą: *Polskie priorytety w obszarach europejskich badań na rzecz bezpieczeństwa i walki z terroryzmem*.

Obejmują one wskazania do stosowania innowacyjnych technologii w zakresie:

- powszechnej wiedzy o zagrożeniach bezpieczeństwa;
- ochrony systemów sieciowych;
- przeciwdziałania terroryzmowi, w tym bioterroryzmowi;
- zarządzania kryzysowego,
- integracji systemów informacyjnych i łączności.

W każdym z tych obszarów wytypowane zostały priorytetowe technologie stosowane w systemach bezpieczeństwa. Należy zauważyć, że polskie priorytety technologiczne są zbieżne z priorytetami technologicznymi Europejskiej Agencji Obrony (EDA) i Programem Ramowym Unii Europejskiej, co powinno ułatwić współpracę w tym zakresie z organizacjami europejskimi i pozwoli pozyskać fundusze unijne na ten cel.

Innowacyjne technologie wspomagające utrzymanie bezpieczeństwa obejmują m.in. czujniki (sensory), urządzenia pomiarowe i systemy monitorowania bezpieczeństwa obiektów i środowiska naturalnego oraz automatyzację zarządzania kryzysowego. Podstawowym elementem struktury każdego systemu monitorowania jest czujnik (sensor, detektor), który decyduje o pozostałych modułach i podzespołach urządzenia. Czujniki takie są wykorzystywane w logistyce transportu i magazynowania, szczególnie substancji chemicznych i spożywczych, w których ważne jest wczesne wykrywanie niekorzystnych zmian oraz w transporcie, gdzie istotną rolę odgrywają czujniki sygnalizujące przekroczenie prędkości czy nadmierne zbliżanie się do przeszkody.

Kolejną grupą urządzeń stosowanych w systemach monitorowania są kamery telewizyjne światła dziennego, kamery niskiego poziomu oświetlenia, kamery termowizyjne i noktowizory. Mają one zastosowanie w bezpieczeństwie logistyki przeznaczonej do wykrywania substancji niebezpiecznych czy szkodliwych dla zdrowia i życia umieszczonych w magazynach czy materiałach przewożonych w kontenerach, ładowniach statków czy samolotów.

Istotnym składnikiem monitoringu bezpieczeństwa jest w miarę ujednolicony **system pobierania, przesyłania i analizy danych oraz ewidencjonowania zebranych wyników pomiarów**. Pomiarów dokonują automatyczne sieci monitoringu i przesyłają zakodowane informacje do ośrodka, w którym dane te zostają rozkodowane, zweryfikowane i zapamiętane w komputerowych bazach danych. Systemy informatyczne w postaci komputerowych baz danych w połączeniu z geograficznymi systemami informacyjnymi (GIS) umożliwiają wizualizację danych na mapach tematycznych, co sprzyja szybkiemu wykrywaniu miejsc zagrożeń.

Posiadanie efektywnych systemów wykrywania i analizy zagrożeń bezpieczeństwa w logistyce może dawać gwarancję odpowiednio wczesnego informowania o przewidywanym i aktualnym zagrożeniu i umożliwia zastosowanie odpowiednich środków ochrony.

Nowoczesna infrastruktura logistyczna wyposażona jest w szereg instalacji alarmowych oraz technicznych systemów zapewniających bezpieczeństwo jej funkcjonowania. Należą do nich różnorakie systemy bezpieczeństwa, m.in.:

- *system przeciwpożarowy*, system napadowo-włamaniowy, system kontroli dostępu, system telewizji dozorowej;
- *system bezpieczeństwa zasobów komputerowych*, system bezpieczeństwa transmisji danych, system ochrony fizycznej urządzeń teleinformatycznych;
- *system sterujący automatyką budynków*, jak na przykład klimatyzacją, pracą wind, oświetleniem, zasilaniem w podstawowe media (*www.zaawansowane technologie*);
- *system zarządzania bezpieczeństwem budynków* – BMS (*Building Management System*), gwarantuje dostarczanie technicznych narzędzi zarządzania bezpieczeństwem i komfortem pracy w budynku, w warunkach codziennej eksploatacji i w sytuacjach awaryjnych.

Ważnym elementem bezpieczeństwa w logistyce jest ochrona infrastruktury transportowej i przewozów. Wobec współczesnych zagrożeń bezpieczeństwa

konieczne jest zastosowanie nowoczesnych środków ochrony, w tym urządzeń do wczesnego wykrywania potencjalnych zagrożeń.

Najbardziej znane sposoby zapewnienia bezpieczeństwa w transporcie to skanowanie ładunków, elektroniczne plomby, inteligentne kontenery, monitorowanie i śledzenie ładunków (Biernikiewicz, 2008, s. 493).

Nowoczesne **skanowanie ładunków** zasadniczo różni się od tradycyjnej, fizycznej kontroli. Polega na użyciu skanerów wykorzystujących promieniowanie gamma, rentgenowskie lub wiązki neutronów do przeglądania zawartości ładunku pojazdów, nawet będących w ruchu. Jest nieinwazyjne, szybsze i dokładniejsze od sposobów tradycyjnych. Mogą zdalnie wykryć zagrożenia w postaci ukrytych ładunków wybuchowych czy prześwietlić przejeżdżające pojazdy.

Innym zabezpieczeniem są **elektroniczne plomby** do zamknięcia kontenera przewożącego towary, w sposób uniemożliwiający jego otwarcie przez osoby nieuprawnione. Próby mechanicznego otwarcia skutkują wysyłaniem sygnału o włamaniu i szybkiej identyfikacji kontenera. Obok plomb jednorazowego czy wielokrotnego użytku istnieją obecnie wysoko zaawansowane technologicznie urządzenia do rejestrowania otwarcia drzwi kontenera umieszczane w jego wnętrzu. Połączenie tej technologii z wykorzystaniem GPS i łączności satelitarnej umożliwia monitorowanie położenia przesyłki przez komunikowanie się z serwerem centralnym.

**Inteligentne kontenery** to kolejna forma zapewnienia bezpieczeństwa w logistyce transportu. Kontenery takie wyposażone są w szereg urządzeń i czujników pozwalających na monitorowanie zachodzących zmian środowiskowych (np. temperatury czy wilgotności) i alarmujących o nieuprawnionej próbie otworzenia drzwi. Bardziej zaawansowane technologie zastosowane w inteligentnych kontenerach umożliwiają poznanie zawartości kontenera, danych nadawcy i odbiorcy, położenie i zboczenie z trasy, czas przybycia do miejsca przeznaczenia oraz inne szczegółowe dane o przewożonym ładunku. Stosowane w transporcie inteligentne kontenery przynoszą wymierne korzyści dla przedsiębiorstwa produkcyjnego czy handlowego, m.in. znaczne zmniejszenie liczby kradzieży, skrócenie czasu transportu oraz poprawę bezpieczeństwa łańcuchów dostaw.

Do sprawnego zarządzania łańcuchem dostaw logistycznych konieczna jest możliwość systematycznego **monitorowania i śledzenia przesyłanych ładunków**. Ma to niebagatelne znaczenie szczególnie podczas przewożenia

towarów niebezpiecznych i wartościowych oraz produktów wrażliwych. Zadanie to jest możliwe do wykonania dzięki nowoczesnej technologii RFID (*Radio-Frequency Identification)*. Jest to technika wykorzystująca fale radiowe do przesyłania danych oraz zasilania elektronicznego układu, stanowiącego etykietę obiektu przez czytnik, w celu identyfikacji obiektu. Specjalne urządzenia zwane tagami, zawierające układy elektroniczne z zakodowanymi danymi i anteną odbiorczo-nadawczą, przymocowuje się do przewożonych przedmiotów. Zapis i odczyt danych odbywa się zdalnie z pomocą fal radiowych przy użyciu czytnika RFID wraz z anteną. Metoda ta jest wykorzystywana w logistyce do wykrywania, śledzenia i monitorowania obiektów z dużą dokładnością. Jako jeden ze składników nowoczesnego systemu informatycznego może automatycznie identyfikować obiekty i na podstawie odczytanych informacji, podejmować odpowiednie działania. Przy połączonym wykorzystaniu RFID z GPS/GSM (*Global Positioning System/Global System for Mobile Communications*) oraz inteligentnych kontenerów w logistyce podnosi się skuteczność działań, oszczędza czas pracy, obniża koszty i znacznie zwiększa bezpieczeństwo obiektów i osób.

Szczególną pieczą otaczany jest **transport towarów podwójnego zastosowania** (*dual use products*), czyli takich, które mogą być użyte zarówno do celów cywilnych, jak i wojskowych. Przykładami takich towarów są np. niektóre serwery, komputery i skanery, niektóre turbosprężarki i pompy, substancje chemiczne, metale i stopy itd. Ze względu na specyficzne właściwości takich towarów zostały wprowadzone międzynarodowe regulacje ograniczające obrót nimi. Do takich ograniczeń należy m.in. konieczność uzyskania stosownego zezwolenia na wywóz tych towarów z kraju czy też obowiązek informowania odpowiednich organów państwowych o zamiarze przywozu tych towarów do kraju. Restrykcje zostały wprowadzone w celu ochrony bezpieczeństwa wewnętrznego poszczególnych państw, zwalczanie terroryzmu oraz zapobieganie rozprzestrzeniania broni masowego rażenia (Najgebauer, 2012).

Zastosowane są także szczególne środki ostrożności i ochrony oraz zasady bezpieczeństwa przy transporcie towarów i przepływie informacji (technologii), dotyczących ich produkcji lub użytkowania. Te specyficzne informacje to dane technologiczne (plany, wykresy, tabele, projekty, nośniki, dyski) lub formy pomocy technicznej (podręczniki, instrukcje, materiały szkoleniowe, wskazówki eksploatacyjne i inne).

Kolejnym ważnym obszarem w bezpieczeństwie logistyki, który wymaga wdrożenia nowoczesnych systemów bezpieczeństwa informacji, jest **ochrona przepływu danych**. Obecnie w większości przedsiębiorstw wymiana informacji między kontrahentami czy składanie zamówień określonych usług logistycznych odbywa się przede wszystkim przez **systemy teleinformatyczne**. Zamówienia przesyłane przez sieci teleinformatyczne potencjalnie mogą być narażone na dostęp nieuprawnionych osób. Każde włamanie do urządzeń teleinformatycznych przez osoby postronne stanowi zagrożenie dla bezpieczeństwa przesyłanych informacji.

Wraz ze wzrostem liczby osób korzystających z sieci teleinformatycznych wzrasta zagrożenie ich bezpieczeństwa. Ujawnienie danych dotyczących zasobów danego przedsiębiorstwa czy organizacji, jego planów strategicznych, kanałów dystrybucji, zamówień, informacji o polityce cenowej i płacowej i innych planach rozwojowych stanowi doskonałe źródło informacji dla firmy konkurencyjnej. Stosowane obecnie w logistyce systemy wymiany informacji czy systemy zarządzania relacjami z klientami oparte są przede wszystkim na przepływie danych przez sieci teleinformatyczne i teleinformacyjne. Różnice między bezpieczeństwem teleinformatycznym i teleinformacyjnym wyjaśnia definicja podana przez Krzysztofa Lidermana (Liderman, 2009, s. 11). **Bezpieczeństwo teleinformacyjne** obejmuje „zakres form wymiany, przechowywania i przetwarzania informacji, ograniczonego do technicznych środków łączności (przez telefony stacjonarne i komórkowe, radiostacje, sieci i systemy komputerowe). **Bezpieczeństwo teleinformatyczne** dotyczy informacji przesyłanych, przechowywanych i przetwarzanych w sieciach systemach teleinformatycznych".

Najczęściej włamania do sieci informatycznych przedsiębiorstw są dokonywane przez osoby posiadające szeroką wiedzę i doskonałe umiejętności w zakresie obsługi i użytkowania systemów teleinformatycznych pozwalające na omijanie zabezpieczeń stosowanych przez przedsiębiorstwa. Podejmowane przez nich działania wiążą się z tzw. **cyberterroryzmem**, „czyli z przestępstwem o charakterze terrorystycznym, popełnionym w cyberprzestrzeni. Cyberprzestrzeń jest definiowana, jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jest przestrzenią otwartego komunikowania się za pośrednictwem połączonych komputerów i powiązań informatycznych pracujących na całym świecie" (www.słownikinternetowy.pl).

Podobnie jak inne działy gospodarki, logistyka, a w szczególności transport, są również objęte siecią cyberprzestrzeni, niezbędną do prawidłowego funk-

cjonowania i zarządzania posiadanymi zasobami rzeczowymi i informacyjnymi. Obecnie obserwuje się dynamiczny rozwój nowoczesnych technik i technologii w tej dziedzinie. Powstają nowe systemy i narzędzia, niejednokrotnie mogące zastępować pracę człowieka.

Swoistym ewenementem zabezpieczenia logistycznego jest **sztuczna inteligencja** (AI – *Artificial Intelligence*), powstała w wyniku badań nad stworzeniem maszyn o inteligencji dorównującej lub przewyższającej inteligencję wybitnych jednostek ludzkich, z szerokimi możliwościami komunikowania się z człowiekiem, opartymi na bazie pojęć i faktów z języka naturalnego nawet ze zdolnością wnioskowania. Termin ten wprowadził do nauki John McCarthy, amerykański informatyk, który w 1956 roku po raz pierwszy użył określenia *artificial inteligence* na konferencji w Dartmouth, podsumowującej badania w tej dziedzinie.

Polscy uczeni także włączyli się w nurt badań poświęconych temu problemowi. Już w 1979 roku Andrzej Dziurnikowski w swoich artykułach wyjaśniał pojęcie sztucznej inteligencji. Według niego „sztuczna inteligencja obejmuje wszelkie badania dotyczące aspektów związanych z problemami inteligencji, prowadzone metodami realizacji technicznej lub teoretycznych rozwiązań wykorzystujących formalizm matematyczny" (Dziurnikowski, 1979).

Kilka lat później Jarosław Olejniczak podał inną definicję tej technologii: „sztuczna inteligencja, to zespół środków informatyki, które ułatwiają nabywanie i wykorzystywanie wiedzy wynikającej z odtwarzania okoliczności, doprowadzających do znanych skutków, w celu określenia czynników i działań niezbędnych dla spowodowania skutków pożądanych" (Olejniczak, 1991).

Jan J. Mulawka zaś określa sztuczną inteligencję „jako dziedzinę informatyki dotyczącą metod i technik wnioskowania symbolicznego, przez komputer oraz symbolicznej reprezentacji wiedzy stosowanej podczas takiego wnioskowania" (Mulawka, 1996).

Jak wynika z przytoczonych definicji, sztuczna inteligencja ma szeroką gamę możliwości, które mogą być wykorzystane w różnych dziedzinach logistyki, z bezpieczeństwem włącznie. Na przykład w transporcie **drony monitorujące transportowanie towarów**, obserwujące terminale przeładunkowe czy centra logistyczne mogą przekazywać obrazy do systemu rozpoznawczego twarzy czy mowy i natychmiast zostanie zaalarmowany dział odpowiedzialny za bezpieczeństwo danego odcinka.

Istnieją już rozwiązania rozpoznające samopoczucie człowieka po wyrazie twarzy, co stwarza możliwość szybkiej oceny kondycji, np. kierowcy transpor-

tu czy magazyniera mającego wpływ na powierzony towar. Urządzenia oparte na sztucznej inteligencji potrafią rozmawiać z człowiekiem, mogą naśladować cechy ludzkiego umysłu w rozwiązywaniu konkretnych problemów, być m.in. wykorzystywane w cyberprzestrzeni do ochrony antywirusowej. Przyszłością sztucznej inteligencji będą coraz doskonalsze rozwiązania polegające na nienadzorowanych systemach uczących, które będą mogły samodzielnie analizować olbrzymie ilości danych i szukać wyjaśnienia problemów niedostrzegalnych dla człowieka.

Norbert Biedrzycki, ekspert IT, przewiduje dynamiczny rozwój tej dziedziny informatyki. Przede wszystkim skupia się na trzech nowych technologiach: **myślące komputery** (*cognitve computing*), **uczenie się maszyn** (*machine learning*) i **rozumienie języków naturalnych** (*natural language understanding)*.

Do grona myślących komputerów dołączą niebawem komputery kwantowe, mające wielokrotnie większe możliwości przetwarzania danych niż obecnie użytkowane komputery o systemach binarnych. Myślące komputery oparte na działaniu sieci neutronowych będą mogły przewidywać zjawiska i modelować systemy transakcyjne tak istotne w logistyce sprzedaży. Innym nowym trendem IT są maszyny rozumiejące języki naturalne, nie tylko reagujące na polecenia głosowe, lecz także posiadające umiejętność czytania tekstów skomplikowanych, raportów czy wykresów. Tego typu komputery mogą stać się niezbędnym narzędziem w polityce ochrony i bezpieczeństwa logistyki przedsiębiorstw i instytucji.

*Z t*echnologią sztucznej inteligencji ściśle związane jest pojęcie ***chatbotów***. Po raz pierwszy nazwa ta została użyta w 1994 roku przez dr. Michaela Mauldina, amerykańskiego matematyka i informatyka. Słowo *bot* pochodzi od *robot* – urządzenia samodzielnie wykonującego zaprogramowane działania. W uproszczeniu *bot* jest programem komputerowym mającym zastąpić człowieka w wykonywaniu jakiejś czynności. Rozwojem botów zajmuje się głównie **botyka**, nowy dział nauki, wykorzystujący wiedzę o modelowaniu oraz symulowaniu zachowań w celu tworzenia cyfrowych postaci. Jednym z botów jest *chatterbot*, program komputerowy sprawiający wrażenie inteligentnego, którego zadaniem jest prowadzenie konwersacji przy użyciu języka naturalnego bądź **interfejsu tekstowego** (Koszemba-Wiklik, Machnik-Słomka, 2018).

Jednym z ważnych kanałów obecnej komunikacji międzyludzkiej i komunikacji między firmami i klientami jest *czat*. Automatyzacja takiej komunikacji

następuje przez **chatboty**. Chatbot jest programem opartym na regułach oraz wykorzystaniu technologii **AI**, z którym użytkownik komunikuje się za pośrednictwem interfejsu, czatu (Koszemba-Wiklik, Machnik-Słomka, 2018). Chatboty potrafią obsługiwać różne aktywności: odpowiadać na zapytania klientów, rekomendować produkty, dokonywać rezerwacji, robić zamówienia, informować o promocjach itp. Technologia chatbotów jest wykorzystywana w firmach do usprawnienia relacji z klientami i szybkiego wewnętrznego komunikowania się. Ponadto ta technologia gwarantuje pełną i skuteczną ochronę przepływu informacji i poufność danych, co jest cenione wśród przedsiębiorców walczących o hegemonię na rynku.

Z kolei **blockchain** to rozproszona baza danych, która zawiera stale rosnącą ilość informacji (*rekordów*), pogrupowanych w bloki i powiązanych ze sobą w taki sposób, że każdy następny blok zawiera oznaczenie czasu (*timestamp*), kiedy został stworzony oraz linkdo poprzedniego bloku, będący zaszyfrowanym „streszczeniem" (*hash*) jego zawartości (Piech, 2016). Zastosowanie tej technologii odpornej na cyberataki może całkowicie zmienić formy bezpieczeństwa w logistyce, nie tylko usprawniając przepływ dokumentacji, lecz także przede wszystkim stwarzając ochronę danych. Technologia *blockchain* jest doskonałym zabezpieczeniem zawartych umów, zleceń czy zamówień, jako niepodatna na awarie systemów komputerowych. Największymi zaletami zautomatyzowanych umów są szybkość ich zawierania i finalizowania, bezpieczeństwo danych, mniejsza podatność na ludzkie błędy oraz redukcja pośredników. Płatności w technologii *blockchain* są czymś w rodzaju certyfikacji zasad uczciwego handlu, przejrzystego i wolnego od nierzetelnych transakcji, a przede wszystkim bezpiecznego. Ponadto koszty operacji kupna-sprzedaży czy transportu są nieporównywalnie niższe od tradycyjnych, gdyż technologia *blockchain* oparta na zakodowanej strukturze kryptograficznej nie potrzebuje żadnej instytucji pośredniczącej i weryfikującej dane z transakcji.

*Kolejnym nowoczesnym rozwiązaniem technologicznym stosowanym m.in. w logistyce transportu i zaopatrzenia jest* **chmura obliczeniowa** lub „przetwarzanie w chmurze" (*cloud computing*). Istnieje wiele definicji tego pojęcia formułowanych przez teoretyków i praktyków z obszaru technologii informatycznych. Jedna z nich, moim zdaniem, najbardziej komunikatywna, określa *cloud computing* jako model umożliwiający powszechny, wygodny, udzielany na żądanie dostęp za pośrednictwem sieci do wspólnej puli możliwych do konfi-

guracji zasobów przetwarzania (np. sieci, serwerów, zasobów przechowywania, aplikacji i usług), które można szybko dostarczyć i uwolnić przy minimalnym wysiłku zarządzania lub działania ze strony usługodawcy (Mell, Grance, 2011). Można przyjąć, że zadaniem *cloud computing* jest dostarczanie zainteresowanym klientom za pośrednictwem internetu („chmura") usług obliczeniowych, takich jak serwery, magazyny, bazy danych, sieci, oprogramowania, analizy itp. Firmy oferujące te usługi obliczeniowe są nazywane dostawcami chmury i zazwyczaj pobierają opłaty za usługi chmury obliczeniowej w zależności od użycia (podobnie jak dostawcy energii elektrycznej lub wody).

Intensywny wzrost liczby zagrożeń dla bezpieczeństwa informacji spowodował konieczność opracowania szeregu zarządzeń, wytycznych i norm w tym zakresie. Normy stanowią zbiór wytycznych, umożliwiających przedsiębiorstwu sprawne i efektywne zarządzanie procesami. Na podstawie wytycznych zamieszczonych w określonych normach przedsiębiorstwo powinno wdrożyć **własny system zarządzania bezpieczeństwem informacji**. Najbardziej rozpowszechnione są międzynarodowe normy ISO, które w Polsce wdrażane są przez Polski Komitet Normalizacji. Normy te dotyczą systemu zarządzania bezpieczeństwem informacji i podają praktyczne zasady jego stosowania, zarządzania usługami oraz zarządzania ryzykiem w bezpieczeństwie informacji.

Szczególnie restrykcyjne przepisy dotyczą obrotu towarami podwójnego stosowania. W Polsce obrót tymi towarami i technologią podwójnego zastosowania jest regulowany przepisami Unii Europejskiej i ustawą z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa. W każdym kraju Unii Europejskiej bezpośrednie zastosowanie ma rozporządzenie Rady (WE) nr 428/2009 z dnia 5 maja 2009 r. ustanawiające wspólnotowy system kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Rozporządzenie to wprowadza m.in. listę towarów podwójnego zastosowania weryfikowaną rokrocznie. Specjalnej kontroli i ochronie poddawane są technologie służące do produkcji, rozwoju oraz użytkowania tych towarów. Wskazane jest, aby przedsiębiorstwa dokonujące transferów kontrolowanej technologii wdrożyły stosowne procedury mające na celu wprowadzenie ścisłego nadzoru nad transferem tych technologii. Należy również wprowadzić identyfikację transferów, które mogą być kontrolowane oraz uzyskać stosow-

ne zezwolenia. Procedury takie służą ograniczeniu ryzyka dokonania transferu bez stosownego zezwolenia, a więc zwiększeniu ich bezpieczeństwa.

Zaprezentowane rozwiązania i technologie nie wyczerpują tematu dotyczącego wykrywania i eliminacji zagrożeń bezpieczeństwa występujących w logistyce. W tej dziedzinie obserwuje się szybki postęp zarówno w doskonaleniu form i metod oraz innowacyjnych rozwiązań ochrony osób i mienia, jak i rozwój technologiczny w zakresie unowocześniania istniejących urządzeń wzmacniających bezpieczeństwo i tworzenie nowoczesnych, wysoko specjalistycznych urządzeń z wykorzystaniem zdobyczy nauki i techniki szczególnie z dynamicznie rozwijających się technologii informatycznych.

## Podsumowanie

Rozpatrzone w artykule zagrożenia bezpieczeństwa w logistyce i sposoby przeciwdziałania im nie wyczerpują tematu. Wobec dynamicznego rozwoju logistyki i jej roli w każdej dziedzinie gospodarki nie jest możliwe, aby w gruntowny sposób przedstawić wszystkie aspekty i dylematy tej problematyki. Jednak nawet tak wybiórcze ukazanie kwestii bezpieczeństwa logistycznego pokazuje wagę wyzwań, jakie stoją przed zainteresowanymi podmiotami. Przedstawiona została złożoność kwestii zapewnienia bezpieczeństwa w łańcuchach dostaw logistycznych oraz podejmowane działania w związku z realizacją tych zamierzeń. Zaprezentowano różnego rodzaju rozwiązania problemu ochrony osób i mienia oraz bezpieczeństwa przy realizacji usług logistycznych. Ponadto wymienione zostały korzyści wynikające ze stosowania wytycznych, procedur, norm i zabezpieczeń stosowanych w logistyce, a szczególnie w transporcie: skrócenie czasu transportu, uproszczenie procedur celnych, możliwość lokalizacji ładunku, odtworzenia trasy przemieszczenia oraz wpływania na zachodzące w czasie przewozu zmiany i nieprawidłowości. Zwrócono również uwagę na innowacyjny charakter stosowanych urządzeń monitorujących i ich wielostronne wykorzystanie w różnych obszarach działalności. W dobie wzrastającego znaczenia internetu na plan pierwszy wysuwa się bezpieczeństwo informacyjne, które odgrywa kluczową rolę w wielu dziedzinach życia. Żadne procesy logistyczne nie mogą być realizowane bez skutecznego przepływu informacji. Od szybkiego i prawidłowego przepływu informacji zależy realizacja poszczególnych działań logistycznych w przedsiębiorstwie. Zaplanowanie i zrealizowanie dostawy nie byłoby możliwe bez pozyskania danych potrzebnych do przygotowania i dostarczenia towaru

w wyznaczonym terminie w określone miejsce. Ciągle rosnąca liczba przedsiębiorstw korzystających z zewnętrznych usług logistycznych wymaga zwiększenia skuteczności przepływu informacji. Zagrożenie tego przepływu przy realizacji jakiejkolwiek usługi logistycznej może mieć negatywne konsekwencje dla przedsiębiorstwa i firm z nim współpracujących. Dlatego priorytetowe staje się wdrażanie skutecznych i nowoczesnych systemów bezpieczeństwa informacji, a to wymaga ciągłego doskonalenia pracowników i tworzenia warunków sprzyjających poszukiwaniom rozwiązań innowacyjnych.

W dzisiejszych czasach bezpieczeństwo w łańcuchu dostaw logistycznych coraz bardziej zyskuje na znaczeniu. Wynika to przede wszystkim z globalizacji form działania i szybkiego rozwoju technologii, które wpływają na dostęp do dóbr, czas prowadzonych transakcji i możliwości związanych z dostawą i dystrybucją produktów, które mogą być prowadzone z różnych części świata. Zasięg systemów logistycznych zatem coraz bardziej się poszerza, a tym samym zwiększa się ryzyko prowadzonych działań przez firmę. Wielkiego znaczenia nabiera więc nowoczesne, skuteczne zarządzanie bezpieczeństwem procesów logistycznych w przedsiębiorstwach. Zarządzanie bezpieczeństwem w logistyce obejmuje zestaw zharmonizowanych działań podejmowanych w sytuacji zagrożeń lub zakłóceń wymierzonych na zasoby logistyczne w celu zmniejszenia lub wyeliminowania zagrożenia (Szymonik, 2011). Dzięki prawidłowo zorganizowanemu zarządzaniu czynności transportowe i magazynowanie, realizacja zamówień, zaopatrywanie w części, obsługa klienta, planowanie, prognozowanie popytu, przepływ informacji, kontrola zapasów, czynności manipulacyjne, lokalizacja zakładów produkcyjnych, usługowych i składów, procesy zaopatrzeniowe, pakowanie, obsługa zwrotów oraz gospodarowanie odpadami przebiegają i funkcjonują niezawodnie. W tym celu w każdym przedsiębiorstwie czy organizacji powinny być wdrożone procedury dotyczące zarządzania bezpieczeństwem w logistyce, by tym samym zapewnić bezpieczną i niezawodną realizację zaplanowanych zadań.

## Bibliografia

*Biała Księga Bezpieczeństwa Narodowego*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

Biernikowicz W., Smal T. (2008). *Nowe standardy bezpieczeństwa na rynku przewozów kontenerowych,* [w:] Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa, ISSN 1899-3524.

Biernikowicz W. (2009). *Wykorzystanie technologii RFID do monitorowania ładunków w łańcuchu dostaw,* „Logistyka", nr 2, wersja elektroniczna CD Nr 2.

Bobrow D., Haliżak E., Ziemba R. (1997). *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*. Warszawa: Wydawnictwo Fundacji Stosunków Międzynarodowych.

Bógdoł-Brzezińska A., Gawrycki M.F. (2003). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa: Oficyna Wydawnicza ASPRA-JR.

Ciborowski L. (1999). *Walka informacyjna*. Toruń: Wydawnictwo Europejskiego Centrum Edukacyjnego.

Doktryna logistyczna SZ RP DD/4, Sztab. Gen. Warszawa 2004.

Dziurnikowski A. (1979). *Nie ma jednolitej definicji*, „Informatyka", nr 3.

Dziurnikowski A., Gliński M., Szewczyk A. (1979). *Na trzy głosy,* „Informatyka", nr 3.

Flasiński M. (2011). *Wstęp do sztucznej inteligencji*. Warszawa: Wydawnictwo PWN.

Goban-Klas T., Sienkiewicz P. (1999). *Społeczeństwo informacyjne: szanse, problemy, zagrożenia.* Kraków: Wydawnictwo Fundacji Postępu Komunikacji.

Jałowiec T. (2014). *Logistyczne wymiary systemu bezpieczeństwa państwa*, „Logistyka", nr 5.

Jedynak P., Teczke J., Wyciślak S. (2001). *Zarządzanie ryzykiem w przedsiębiorstwach zorientowanych międzynarodowo*. Kraków: Wydawnictwo Księgarnia Akademicka.

Kasperski M. (2003). *Sztuczna Inteligencja*. Gliwice: Wydawnictwo Helion.

Kifner T. (1999). *Polityka bezpieczeństwa i ochrony informacji*. Gliwice: Wydawnictwo Helion.

Krasuski A. (2018). *Chmura obliczeniowa. Prawne aspekty zastosowania*. Warszawa: Wydawnictwo Wolters Kluwer Polska.

Koszembar-Wiklik M., Machnik-Słomka J. *Zastosowanie narzędzi sztucznej inteligencji na uczelniach na przykładzie chatterbotów,* https://www.polsl.pl/Wydzialy/ROZ/ZN/Documents/z%20105/13%20Koszembar-Wiklik,%20Machnik-S%C5%82omka.pdf (dostęp: 21 marca 2018 r.).

Liderman K. (2000). *Bezpieczeństwo informacji w systemach informatycznych.* Warszawa: Wydawnictwo WSISiZ.

Liderman K. (2009). *Analiza ryzyka i ochrona informacji w systemach komputerowych.* Warszawa: Wydawnictwo PWN.

Matwiejczuk R. (2013). *Kompetencje logistyki w zarządzaniu przedsiębiorstwem*, [w:] J. Brzóska, J. Pyka (red.), *Nowoczesność przemysłu i usług w warunkach kryzysu i nowych wyzwań,* Towarzystwo Naukowe Organizacji i Kierownictwa, Oddział w Katowicach.

Mell P., Grance T. (2011 september). *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf) (dostęp: 21 marca 2018).

Mateos A., Rosenberg J. (2012). *Chmura obliczeniowa. Rozwiązania dla biznesu*. Gliwice: Wydawnictwo Helion.

Mougayar W. (2016). *The Business Blockchain: Promise*, Practice, *and Application of the Next Internet Technology.*

Mulawka J.J. (1996). *Systemy ekspertowe*. Warszawa: Wydawnictwo WNT.

Najgebauer A. (2012). *Technologie podwójnego zastosowania*. Warszawa: Wydawnictwo Wojskowej Akademii Technicznej.

*Olejniczak* J.J. (1991). *Sztuczna inteligencja a filozoficzne perspektywy*, „Problemy", nr 6 (538).

Piech K. (red). *Leksykon pojęć na temat technologii blockchain oraz kryptowalut Strumień* „Blockchain i Kryptowaluty" programu „Od papierowej do cyfrowej Polski" (https://mc.gov.pl/files/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf, (dostęp: 8.11.2016).

Skowronek Cz., Sarjusz-Wolski Z. (2008). *Logistyka w przedsiębiorstwie*. Warszawa: Wydawnictwo PWE.

Sienkiewicz P. (2007). *Teoria i inżynieria bezpieczeństwa systemów*, „Zeszyty Naukowe AON" nr 1 (66).

Sienkiewicz P. (2015). *Teoria i inżynieria systemów*, [w:] *Inżynieria systemów bezpieczeństwa*. Warszawa: Wydawnictwo PWE.

Szymonik A. (2011). *Logistyka w bezpieczeństwie i bezpieczeństwo w logistyce*, „Logistyka", nr 2.

Szymonik A. (2011). *Logistyka w bezpieczeństwie*. Warszawa: Wydawnictwo Difin.

Szymonik A. (2011). *Organizacja i funkcjonowanie systemów bezpieczeństwa.* Warszawa: Wydawnictwo Difin.

Szymonik A. (2011). *Zarządzanie bezpieczeństwem gospodarczym w systemie bezpieczeństwa narodowego. Aspekty logistyczne*. Łódź: Wydawnictwo Politechnika Łódzka.

Szymonik A. (2014). *Bezpieczeństwo systemów logistycznych*, „Gospodarka Materiałowa i Logistyka", nr 5.

Szymonik A. (2015). *Bezpieczeństwo systemu logistycznego w nowoczesnym zarzadzaniu.* Warszawa: Wydawnictwo Difin.

Tapscott D., Tapscott A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Wydawnictwo Penguin Books Ltd.

## Źródła internetowe

Słownik internetowy, http://www.i-slownik.pl/1,323,*cyberprzestrzen.html* (dostęp: 14 października 2018).

Stec P. (2017). *Ochrona pracodawcy przed nieuczciwą konkurencją ze strony pracownika*, www.valor.pl. *10.X*.www.uwm.edu.pl/mkzk/upload/../39zaawansowane_technologie_monitorowania1, (dostęp: 11 października 2017)