ASO.A.5(1)/2015.21-40

CEZARY SZYDŁOWSKI

audytor wewnętrzny, Urząd Wojewódzki w Łodzi,
Wyższa Szkoła Ekonomiczno-Humanistyczna
im. Sz. A. Pieniążka w Skierniewicach

BEZPIECZEŃSTWO INFORMACJI W LOGISTYCE

INFORMATION SECURITY IN LOGISTICS

Streszczenie: Celem artykułu jest przedstawienie podstawowych zagadnień związanych z bezpieczeństwem informacji w procesach logistycznych. Informacja jest bardzo ważnym aktywem niezbędnym do sprawnego realizowania zadań w każdej organizacji. W związku z tym bezpieczeństwo informacji stanowi istotny obszar zarządzania organizacjami. Procesy logistyczne wymagają stałego wsparcia informatycznego w celu przetwarzania danych niezbędnych do realizacji określonych czynności oraz usług logistycznych. Bezpieczeństwo informacji jest zagadnieniem, które będzie nadal się rozwijać wraz z postępem technologicznym oraz rosnącą liczbą użytkowników. Można domniemywać, że również procesy logistyczne będą wymagać ciągłego doskonalenia w obszarze bezpieczeństwa informacji.

Słowa kluczowe: bezpieczeństwo informacji, bezpieczeństwo systemów teleinformatycznych, logistyka

Abstract: This article presents basic issues related to information security in logistics processes. Firstly, the author presents basic issues related to information security in any organization. Moreover, the author shows the areas of information security management in logistic systems. Logistics processes require IT support to process the data necessary to carry out specific tasks. Information security is now a very important area of organizational management. It can be assumed that also the logistics processes will require continuous improvement in the area of information security.

Key words: information security, information security management, logistics

Received: 04.2015

Accepted: 06.2015

WPROWADZENIE

Przepływy dóbr oraz osób realizowane są przez każdą organizację, niezależnie od formy własności czy zakresu jej działania. Logistyka wspiera poszczególne procesy realizowane w przedsiębiorstwach, urzędach oraz w innych podmiotach, jednakże sprawność jej działania jest zależna od efektywnego przepływu informacji. Każda działalność organizacji wymaga od kadry menedżerskiej ciągłego podejmowania szeregu decyzji, których podstawą są aktualne informacje. Logistyka nie może funkcjonować bez skutecznego przepływu informacji. Realizacja każdego zamówienia, zarządzanie stanem magazynowym, czy też fizyczne przemieszczanie określonego dobra wymaga pełnej i aktualnej informacji. Informacja spełnia kluczową rolę w przepływach realizowanych przez logistykę, niekompletna lub nieaktualna informacja może mieć poważne konsekwencje dla prawidłowego przepływu dóbr oraz osób. Wzrost ilości informacji oraz technicznych środków ich przekazywania poza wieloma zaletami powoduje również szereg zagrożeń. Podejmując określone decyzje menedżerowie logistyki chcą mieć pewność, że dane, które otrzymali są wiarygodne, a dostęp do nich posiadają jedynie upoważnione do tego osoby. Aktualnie przepływ informacji odbywa się przede wszystkim poprzez systemy teleinformatyczne. Składanie zamówień przez klientów na realizację określonych procesów logistycznych odbywa się za pomocą narzędzi informatycznych. Zamówienia przesyłane są poprzez sieci teleinformatyczne, które potencjalnie mogą być narażone na nieuprawniony dostęp. Włamanie do sieci przez postronną osobę stanowi duże zagrożenie dla bezpieczeństwa danych przetwarzanych przez systemy informatyczne danej organizacji. Wzrost liczby użytkowników systemów teleinformatycznych poza możliwością pozyskiwania nowych klientów z nich korzystających powoduje również nowe zagrożenia dla bezpieczeństwa informacji. Incydenty dotyczące bezpieczeństwa informacji mogą dotyczyć wszystkich organizacji oraz osób fizycznych. W związku z powyższym stale rośnie rola oraz znaczenie problematyki bezpieczeństwa informacji we wszystkich obszarach działania organizacji.

Bezpieczeństwo informacji stanowi bardzo ważny obszar logistyki, szczególnie w sytuacji stale postępującej informatyzacji procesów logistycznych. Podstawowym celem niniejszego artykułu jest przedstawienie problematyki bezpieczeństwa informacji w obszarze logistyki. Ponadto w publikacji przedstawiono najistotniejsze zagadnienia związane z bezpieczeństwem danych przetwarzanych przez systemy teleinformatyczne w organizacjach. Należy podkreślić, że systemy teleinformatyczne to obecnie podstawowe wsparcie wszystkich procesów logistycznych realizowanych

w nowoczesnych organizacjach. Materiał źródłowy artykułu stanowią aktualnie obowiązujące rozwiązania prawne w zakresie bezpieczeństwa teleinformatycznego, przegląd aktualnej literatury w zakresie bezpieczeństwa informacji w obszarze logistyki oraz analiza obowiązujących Polskich Norm w obszarze bezpieczeństwa systemów informatycznych.

Opracowanie przedstawia bardzo ważną problematykę dla wszystkich organizacji, gdyż problematyka bezpieczeństwa informacji powinna znajdować się w obszarze zainteresowania każdego menedżera.

ROLA INFORMACJI W LOGISTYCE

Informacja odgrywa w każdej organizacji ważną rolę dla podejmowania działań i realizacji bieżących zadań. Również działalność logistyczna wymaga aktualnych oraz wiarygodnych danych. Zakres oraz znaczenie logistyki zmieniało się stosownie do potrzeb i okoliczności, w jakich funkcjonowały i rozwijały się organizacje. Logistyka wspomaga realizację misji oraz celów organizacji. Uogólniając należy uznać, że *„podstawowe znaczenie pojęcia logistyka zostało sformułowane w odniesieniu do wszelkich zadań związanych z przewozami, przeładunkami i magazynowaniem wraz z niezbędnymi do ich wykonywania czynnościami*" [Krawczyk 2011, 156], czyli z magazynowaniem, załadunkiem i wyładunkiem oraz transportem. Logistyka koncentruje się na relacjach pomiędzy poszczególnymi podmiotami w ramach konkretnego łańcucha dostaw. Łańcuch dostaw definiuje się jako *„integrującą filozofię zarządzania całym przepływem w kanale dystrybucji od dostawcy do ostatecznego klienta*" [Coyle, Bardi, Langley 2010, 29]. Wymienione wyżej procesy nie mogą być realizowane w organizacji bez dostępu do aktualnej informacji. Informacje są kluczowane dla bieżącej współpracy w ramach poszczególnych łańcuchów dostaw. Przepływy w łańcuchu dostaw oprócz dóbr obejmują również informacje.

Działalność gospodarcza cechuje się dużą niepewnością, sprostanie przez producenta oczekiwaniom klientów wymaga stałego monitorowania rynku. Aktualne informacje z rynku oraz o kondycji firmy mają strategiczne znaczenie dla podejmowania decyzji przez właścicieli oraz menedżerów. Przedsiębiorstwo potrzebuje dostępu do informacji, przede wszystkim w celu realizacji założonych celów, takich jak:

- *„utrwalenie pozycji rynkowej i przez to uzyskanie przewagi konkurencyjnej,*
- *maksymalizowanie wyniku finansowego w długim horyzoncie czasowym,*

- *wzrost potencjału ekonomicznego,*
- *zwiększenie wartości przedsiębiorstwa dla akcjonariuszy (właścicieli)*" [Skowronek, Sarjusz – Wolski 2008, 44-43].

Powyższe cele nie mogą być zrealizowane bez pozyskania szczegółowych danych w obszarach kluczowych dla działalności przedsiębiorstwa. Realizacja bieżącej produkcji wymaga informacji o zapotrzebowaniu na surowce, półprodukty, podzespoły. Zrealizowanie zamówienia dla klienta poprzedza informacja o zgłaszanym przez niego zapotrzebowaniu. Fizyczne dostarczenie dóbr wymaga choćby informacji o miejscu docelowym dostawy, ilości zamówionych produktów, formie jego opakowania itd. Logistyka zatem zapewnia przedsiębiorstwu niezbędne surowce oraz pozwala dystrybuować wyprodukowane dobra. Przedsiębiorstwa działają w ramach łańcuchów dostaw, które stanowią „*sieć partnerów, którzy w ramach wspólnego działania przekształcają podstawowy surowiec (faza zaopatrzenia) w wyrób gotowy (faza dystrybucji) o określonej wartości dla końcowych nabywców i zagospodarowują zwroty na każdym etapie. Każdy partner w łańcuchu dostaw jest bezpośrednio odpowiedzialny za proces, który podnosi wartość produktu. W ramach tego procesu następuje przekształcenie wkładu w postaci materiałów i informacji w wytwory w postaci dóbr i usług*" [Harrison, Hoek 2010, 23]. Powyższe zależności sprawiają, że logistykę bardzo często rozumie się jako „*metodę zarządzania łańcuchem dostaw w przedsiębiorstwie i pomiędzy przedsiębiorstwami, rozumianą jako planowanie, wdrażanie i kontrolę przepływu produktów wraz z przepływem informacji i finansów*" [Gołembska 2009, 10]. Żaden łańcuch logistyczny nie mógłby skutecznie funkcjonować bez bieżącej informacji. Realizacja każdego zamówienia wymaga wygenerowania danych, które są przekazywane do kontrahentów współpracujących w ramach łańcucha dostaw. Przepływy w procesie zarządzania łańcuchem dostaw obejmują informację jako kluczowy składnik systemu logistycznego organizacji.

Warto w tym miejscu zdefiniować termin informacja oraz dane, rozumiane jako „*rzeczy, fakty, na których można oprzeć się w wywodach*" [Jashapara 2014, 32] lub też jako „*surowe liczby i fakty odzwierciedlające jakiś pojedynczy aspekt rzeczywistości*" [Griffin 2006, 724]. Informację należy interpretować jako „*uporządkowanie danych lub ich przeanalizowanie w jakiś znaczący sposób*" [Stoner, Freeman, Gilbert Jr. 2011, 589]. Każda informacja, żeby mogła być przydatna dla odbiorcy musi być dokładna, istotna oraz aktualna. W celu uniknięcia przeciążenia zbędnymi informacjami przed jej wykorzystaniem należy dokonać wstępnej jej oceny oraz selekcji.

Działania takie zwiększają przydatność informacji dla jej użytkownika. Trzeba dodać, że selekcja oraz ocena informacji pozwala również dokonać wstępnej oceny istoty informacji dla jej odbiorcy. Informacje przepływają w organizacji w ramach przyjętej struktury organizacyjnej. Wykonywanie funkcji kierowniczej w stosunku do podległych członków organizacji nie jest możliwe bez bieżącej wymiany informacji. Relacje takie występują również pomiędzy podmiotami łańcucha dostaw. Informacja wygenerowana w jednej organizacji wywołuje działania w kolejnej.

Informacja w każdej organizacji pozwala podejmować racjonalne decyzje, umożliwia określanie nowych celów, opracowywanie strategii działania itp. Zakres działalności logistycznej w organizacjach jest zależny od struktury oraz zadań i celów jakie realizuje organizacja. Współcześnie logistyka jest w pełni wspomagana przez systemy informatyczne, które pozwalają przetwarzać, generować oraz przechowywać ogromne ilości danych. Systemy teleinformatyczne pozwalają logistyce wspierać poszczególne procesy realizowane przez organizacje. Logistyka nie może być efektywna bez skutecznego przepływu informacji. Informacja stanowi podstawę działań w obszarze logistyki, do których zaliczymy m.in.:

- czynności związane z przemieszczaniem oraz składowaniem dóbr,
- czynności magazynowania oraz składowania dóbr (zarówno niezbędnych do produkcji jak i wyrobów gotowych),
- manipulację materiałami oraz surowcami,
- kontrolowanie i monitorowanie poziomu zapasów,
- realizowanie zamówień klientów,
- opracowywanie prognoz popytu,
- opracowywanie planów produkcji,
- realizację zakupów,
- obsługę klienta,
- logistykę zwrotną (czyli gromadzenie oraz usuwanie odpadów) [Coyle, Bardi, Langley 2010, 69].

Wymienione powyżej działania wymagają stałego dostępu do aktualnych danych. Poszczególne procesy logistyczne wiążą się z generowaniem ogromnej ilości informacji. Przemieszczenie lub składowanie dobra wymaga precyzyjnej informacji o miejscu docelowego składowania i parametrach danego dobra (wadze, wymia-

rach itp.). Ponadto bez dokładnych informacji o specyfice danego dobra nie można określić niezbędnego środka transportu do jego przemieszczenia. Proces składowania oraz magazynowania nieodłącznie powiązany jest z dostępem do bieżących informacji. Niemożliwe jest sprawne zarządzanie stanem magazynowym bez danych o miejscu składowania danego dobra oraz m.in. o jego stanie ilościowym czy terminach przydatności. Gospodarka magazynowa wymaga aktualnych danych o stanach magazynowych poszczególnych dóbr. Wszystkie informacje w tym zakresie przetwarzane są poprzez systemy teleinformatyczne, które zapewniają szybki dostęp do bieżących danych. Kontrolowanie poziomu zapasów w przedsiębiorstwie jest informacją o strategicznym znaczeniu. Stan zapasów determinuje proces produkcji lub świadczy o poziomie sprzedaży konkretnych wyrobów. Generowanie aktualnych informacji wymaga stałego zastosowania nowoczesnych systemów informatycznych pozwalających tworzyć ogromne bazy danych. Przedsiębiorstwa posiadają rozbudowane bazy danych zawierające informacje ze wszystkich obszarów działania organizacji. Przetwarzanie dużych ilości danych powoduje konieczność częstej rozbudowy infrastruktury informatycznej w celu jej dostosowania do zmieniających się potrzeb organizacji.

Zrealizowanie zamówienia danego klienta jest możliwe jedynie po uzyskaniu specyfikacji określającej wymagania konkretnego odbiorcy lub kontrahenta w łańcuchu dostaw. Umożliwiają to systemy teleinformatyczne, dzięki którym możliwe jest szybkie przesyłanie danych dotyczących zamówienia. Wymaga to jednakże integracji systemów informatycznych podmiotów działających w ramach łańcucha dostaw. Proces realizacji zamówienia nieodzownie związany jest z jego obsługą, usprawniają go wyspecjalizowane systemy teleinformatyczne, dzięki którym możliwe jest przysyłanie dużych ilości informacji. Dzięki temu klienci mogą składać zamówienia poprzez globalną sieć teleinformatyczną (Internet). Umożliwia to szybsze złożenie i zrealizowanie zamówienia, ponadto wdrożenie określonych rozwiązań informatycznych daje klientowi możliwość wyboru optymalnego dla niego dobra nie opuszczając siedziby przedsiębiorstwa lub miejsca zamieszkania.

Zwiększanie efektywności przedsiębiorstw wymusiło wdrożenie usprawnień procesów logistycznych również w zakresie przepływu informacji. Usługi logistyczne takie jak przemieszczanie dóbr oraz ich magazynowanie wymaga przetwarzania wielu danych. Informacja jest nieodzownym elementem procesów logistycznych. Zapewnienie usług logistycznych na odpowiednim poziomie wymaga wdrażania

coraz wydajniejszych systemów teleinformatycznych. Dzięki temu możliwe jest przyspieszenie procesu podejmowania decyzji przez menedżerów logistyki. Logistyka na szeroką skalę wykorzystuje najnowocześniejsze rozwiązania w zakresie zarządzania informacją. Przykładowo zarządzanie realizacją usług transportowych wymaga stałego dostępu do bieżących informacji o przemieszczających się pojazdach, ich lokalizacji itd. Aktualną informację w tym zakresie mogą zapewnić jedynie nowoczesne systemy lokalizacji pojazdu oraz śledzenia trasy jego przemieszczania, takie jak GPS, czyli *Global Positioning System*. GPS to satelitarny system umożliwiający wyznaczenie pozycji danego obiektu. System działa dzięki sygnałom wysyłanym przez satelity umieszczone na orbicie Ziemi [Remlein 2009, 160-163]. Wykorzystanie powyższego systemu umożliwia generowanie bieżących informacji o realizacji poszczególnych dostaw dla klientów. Ponadto system dostarcza bieżących informacji o przemieszczaniu się konkretnych pojazdów. System ten usprawnia proces zarządzania flotą pojazdów będących w dyspozycji przedsiębiorstwa.

Logistyka nie mogłaby funkcjonować bez bieżącej informacji. Determinuje ona wszystkie działania w obszarze zarządzania przepływami dóbr i usług, prowadzenia gospodarki magazynowej oraz obsługi klienta. W związku z powyższym duże znaczenie ma wiarygodność i bezpieczeństwo informacji będącej podstawą procesu decyzyjnego.

BEZPIECZEŃSTWO INFORMACJI W LOGISTYCE

Technologie w zakresie generowania, przetwarzania oraz przesyłania informacji znalazły szerokie zastosowanie w logistyce. Konieczność szybkiej wymiany informacji do realizacji zadań logistyki przyczyniła się do wdrożenia wielu nowoczesnych rozwiązań teleinformatycznych. Jednakże postęp technologiczny oraz szerokie wykorzystywanie ogólnie dostępnych sieci teleinformatycznych spowodowało powstanie zagrożeń dla bezpieczeństwa informacji.

Bezpieczeństwo informacji obejmuje wszystkie dane gromadzone oraz przetwarzane w organizacji. Zatem obejmuje ono zarówno nowoczesne systemy teleinformatyczne jak i dane generowane w tradycyjny sposób, np. odręczne notatki. Bezpieczeństwo informacji powinno zagwarantować, aby dane będące w posiadaniu organizacji nie zostały przetworzone w nieuprawniony sposób lub nie zostały udostępnione nieuprawnionym do tego osobom lub podmiotom. Każda informacja generowana w organizacji powinna podlegać ochronie. Oczywiście poziom zastosowa-

nych zabezpieczeń jest zależny od istoty i znaczenia danej informacji dla organizacji. Dane szczególnie wrażliwe dla przedsiębiorstwa muszą być szczególnie chronione. Wdrażanie nowoczesnych systemów bezpieczeństwa informacji wymaga szeregu nakładów finansowych oraz inwestycji. Należy zdawać sobie sprawę, że bezpieczeństwo stanowi znaczący koszt dla organizacji, jednakże ujawnienie danych wrażliwych o firmie może spowodować ogromne straty finansowe oraz wizerunkowe. Każdy klient oraz kontrahent chce mieć pewność, że jego wrażliwe dane podlegają ochronie i nie są narażone na ujawnienie osobom postronnym. W związku z powyższym organizacje obowiązane są chronić bezpieczeństwo danych. System zarządzania bezpieczeństwem informacji musi zagwarantować, że systemy informacyjne wykorzystywane przez organizację zapewniają poufność, integralność oraz dostępność informacji i usług[1]. Poufność systemów teleinformatycznych należy rozumieć jako właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom i podmiotom. Integralność oznacza, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony, natomiast dostępność określa, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym[2]. Bezpieczeństwo informacji obejmuje wszystkie dane przetwarzane w organizacji. Odręcznie sporządzone zestawienie zrealizowanych zamówień może być potencjalnie dla konkurencji równie cenną informacją jak dostęp do bazy klientów.

Procesy logistyczne wymagają przetwarzania bardzo dużej ilości danych. Szerokie wykorzystywanie w logistyce systemów teleinformatycznych poza wieloma zaletami, stanowi również znaczące zagrożenie dla bezpieczeństwa danych. Przykładowo ujawnienie lub kradzież danych dotyczących wymiany dóbr w ramach łańcucha dostaw, stanowi dla konkurencji cenne źródło informacji. Dane generowane w tym procesie mogą świadczyć o kondycji przedsiębiorstwa, jego planach rozwojowych,

[1] Osiągniecie podstawowych wymogów jest możliwe poprzez wdrożenie w organizacji wytycznych zawartych w Polskich Normanach: PN-ISO/IEC 27001, PN-ISO/IEC 20000-1:2007, PN-ISO/IEC 20000-2:2007, PN-ISO/IEC 17799, PN-ISO/IEC 27005, PN-ISO/IEC 24762.

[2] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2012 r., poz. 526 ze zm. § 2.

kanałach dystrybucji itd. Ponadto informacje przekazywane pomiędzy podmiotami mogą być źródłem wiedzy o przyjętych strategiach działania czy też polityce cenowej. Stosowane w logistyce systemy wymiany informacji, systemy zarządzania relacjami z klientami oparte są przede wszystkim na przepływie danych poprzez sieci teleinformatyczne. Praktyka dowodzi, że najbezpieczniejszy jest system teleinformatyczny nie posiadający połączenia ze światem zewnętrznym. Jednakże w powyższym przypadku również istnieje zagrożenie ujawnienia ważnych danych, którym jest użytkownik systemu mający do niego bezpośredni dostęp. Zatem taka sytuacja również wymaga zastosowania odpowiednich zabezpieczeń, w postaci niepowtarzalnych identyfikatorów użytkowników (loginów) oraz rozbudowanego systemu haseł.

Zapewnienie odpowiedniego poziomu bezpieczeństwa informacji procesów logistycznych wymaga przeprowadzenia kompleksowej analizy zagrożeń. Analiza ryzyka w obszarze bezpieczeństwa informacji stanowi podstawę do wdrożenia odpowiednich zabezpieczeń. Najwięcej zagrożeń dla bezpieczeństwa informacji w logistyce związanych jest z systemami teleinformatycznymi, które mają połączenie z globalną siecią Internet. Warto w tym miejscu przedstawić różnicę między bezpieczeństwem teleinformacyjnym a teleinformatycznym. 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 i systemach teleinformatycznych*" [Liderman 2009, 11-12]. Zgodnie z powyższymi definicjami bezpieczeństwo informacji w logistyce obejmuje oba obszary oraz już wcześniej wspomniane tradycyjne formy wymiany danych (odręczne zapiski, fotokopie danych itp.). Logistyka, poza systemami teleinformatycznymi, wykorzystuje również do przepływu informacji inne systemy łączności. Obsługa klienta poza wykorzystaniem systemów informatycznych jest również realizowana, np. w wyniku telefonicznego zgłoszenia zapotrzebowania na daną usługę. Przykładem może być choćby transport osób realizowany na podstawie telefonicznego zgłoszenia klienta. Kolejnym obszarem jest świadczenie pomocy poszkodowanym w ramach systemu ratownictwa medycznego, gdzie system jest uruchamiany przede wszystkim po wpłynięciu zgłoszenia telefonicznego. Również w tych obszarach ważne jest zapewnienie bezpieczeństwa danych generowanych na potrzeby realizacji danych usług. Obecnie rejestracja zgłoszeń telefonicznych w ww. przypadkach odbywa się przy

pomocy systemów teleinformatycznych, które ułatwiają zarządzanie poszczególnymi procesami. Ujawnienie zapisów nagrywanych rozmów z klientami może narazić klientów oraz organizacje na poważne konsekwencje.

Kolejnym ważnym obszarem logistyki, który wymaga wdrożenia nowoczesnych systemów bezpieczeństwa informacji, jest wymiana danych poprzez sieci teleinformatyczne. Wymiana danych pomiędzy kontrahentami odbywa się w większości przypadków poprzez systemy teleinformatyczne. Najwięcej zagrożeń dla bezpieczeństwa danych występuje w ogólnie dostępnej sieci Internet. Rosnąca liczba użytkowników powoduje wzrost zagrożeń dla bezpiecznego przesyłania danych pomiędzy podmiotami. Najczęściej włamania do sieci informatycznych przedsiębiorstw są dokonywane przez tzw. hackerów. Są to osoby lub grupy osób posiadające wysoką wiedzę i umiejętności w zakresie obsługi i użytkowania systemów teleinformatycznych. Posiadane przez nich kwalifikacje i umiejętności pozwalają na omijanie zabezpieczeń stosowanych przez przedsiębiorstwa. Podejmowane przez nich działania mają różny charakter i wiążą się z tzw. *„cyberterroryzmem czyli z przestępstwem o charakterze terrorystycznym popełnionym w cyberprzestrzeni. Cyberprzestrzeń jest definiowana jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne*" [Polityka Ochrony Cyberprzestrzeni ... 2013, 5].

Dynamiczny wzrost ilości zagrożeń dla bezpieczeństwa danych przyczynił się do opracowania szeregu wytycznych oraz norm w tym zakresie. Obowiązujące na całym świecie wytyczne obejmują zarówno zarządzanie bezpieczeństwem informacji jak i zarządzanie procesami informatycznymi w organizacjach. Najbardziej rozpowszechnione są międzynarodowe normy ISO (w Polsce wdrażane jako Polskie Normy przez Polski Komitet Normalizacji). Normy stanowią swoisty katalog wytycznych, które umożliwiają organizacji sprawne zarządzanie procesami. Każda organizacja w oparciu o wskazane w normach wytyczne musi wdrożyć własny system zarządzania bezpieczeństwem informacji. System ten musi uwzględniać specyfikę danej organizacji.

W związku z tym każdy proces logistyczny realizowany przez przedsiębiorstwo powinien zostać poddany szczegółowej analizie pod kątem potencjalnych zagrożeń. Na podstawie analizy ryzyka można opracować wewnętrzne procedury bezpieczeństwa informacji oraz systemów informatycznych. Obecnie nie jest możliwe wdrożenie efektywnego systemu bezpieczeństwa informacji bez skutecznego zarządzania systemami informatycznymi.

Tabela 1. Zestawienie najważniejszych Polskich Norm dotyczących bezpieczeństwa informacji

Lp.	Nazwa Polskiej Normy	Kluczowe obszary i zagadnienia ujęte w normie
1.	Polska Norma PN-ISO/IEC 27001. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji	Norma przedstawia ogólne wytyczne w zakresie możliwego do opracowania i wdrożenia w organizacji modelu systemu zarządzania bezpieczeństwem informacji w organizacjach. Norma przedstawia ogólne założenia związane z procesem planowania, wdrażania, zarządzania i kontrolowania ww. procesu.
2.	Polska Norma PN-ISO/IEC 20000-1:2007 Technika informatyczna. Zarządzanie usługami. Część 1: Specyfikacja	Norma przedstawia ogólne wytyczne w zakresie zintegrowanego podejścia do skutecznego świadczenia klientom usług w obszarze informatyki.
3.	Polska Norma PN-ISO/IEC 20000-2:2007 Część 2: Reguły postępowania.	Norma przedstawia ogólne wytyczne w zakresie wdrożenia w organizacji standardu jakości określonego w normie w obszarze zarządzania usługami informatycznymi.
4.	Polska Norma PN-ISO/IEC 17799 - Technika informatyczna, Techniki bezpieczeństwa, Praktyczne zasady zarządzania bezpieczeństwem informacji	Norma przedstawia ogólne wytyczne w zakresie wdrożenia w organizacji zaleceń dotyczących opracowania i rozwoju skutecznego systemu zarządzania bezpieczeństwem informacji.
5.	Polska Norma PN-ISO/IEC 27005 Technika informatyczna, Techniki bezpieczeństwa, Zarządzanie ryzykiem w bezpieczeństwie informacji	Norma przedstawia ogólne wytyczne w zakresie wdrożenia przez organizacje usystematyzowanego procesie zarządzania ryzykiem w obszarze bezpieczeństwa informacji, ze szczególnym uwzględnieniem systemów teleinformatycznych. Przedmiotowa zawiera wytyczne zgodne dla systemu zarządzania bezpieczeństwem informacji (opisanego w Polskiej Normie PN-ISO/IEC 17799).
6.	Polska Norma PN-ISO/IEC 24762 Technika informatyczna. Techniki bezpieczeństwa. Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.	Norma zawiera ogólne wytyczne w dotyczące eksploatacji systemu zarządzania bezpieczeństwem w obszarze ponownego odtworzenia systemów teleinformatycznych organizacji, które uległy zniszczeniu lub uszkodzeniu w wyniku wystąpienia nieprzewidzianych czynników zewnętrznych (pożaru, powodzi, katastrofy budowlanej, konfliktu zbrojnego, zamachu terrorystycznego itp.). Proces odtwarzania systemów informatycznych organizacji związany jest z tzw. zapewnieniem ciągłości działania organizacji.

Źródło: Opracowanie własne na podstawie Polskich Norm (PN-ISO/IEC 27001, PN-ISO/IEC 20000-1:2007, PN-ISO/IEC 20000-2:2007, PN-ISO/IEC 17799, PN-ISO/IEC 27005, PN-ISO/IEC 24762).

Normy zawierają wskazówki dotyczące zarządzania bezpieczeństwem informacji oraz zarządzania i gospodarowania dostępnymi zasobami teleinformatycznymi organizacji. Wdrażanie wytycznych określonych w normie nie zwalnia kierownictwa organizacji z obowiązku stałego monitorowania zmian oraz zagrożeń w zakresie

bezpieczeństwa informacji. Tylko stałe doskonalenie organizacji oraz szkolenia dla pracowników mogą chronić kluczowe dla organizacji informacje. Polski Komitet Normalizacji opublikował szereg międzynarodowych norm w zakresie bezpieczeństwa informacji i zarządzania systemów teleinformatycznych w organizacjach, zestawienie kluczowych norm zawarto w tabeli 1.

Poza powyższymi normami funkcjonują na świecie również inne wytyczne w zakresie bezpieczeństwa informacji i zarządzania systemami informatycznymi. Jedną z wytycznych są standardy COBIT, opracowane przez IT Governance Institute w Stanach Zjednoczonych [Standardy COBIT 4.1 … http://www.itgi.org]. Standardy „*Control Objectives for Information and related Technology (CobiT), czyli cele kontroli nad technologiami informatycznymi i pokrewnymi, stanowią zbiór dobrych praktyk pogrupowanych w domeny i procesy i prezentujący odpowiednie działania w zrozumiałym i logicznym porządku. Dobre praktyki CobiT odzwierciedlają wspólne stanowisko ekspertów*" [CobiT 4.1 Metodyka …, 5, www.itgi.org]. Powyższe wytyczne zostały opracowane w celu popularyzowania dobrych praktyk w zakresie bezpieczeństwa informacji i zarządzania systemami teleinformatycznymi.

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W LOGISTYCE

Bezpieczeństwo informacji stanowi ważny obszar zarządzania każdą organizacją. Postęp technologiczny oraz wzrost wymiany danych spowodował, że problematyka zabezpieczenia informacji wymaga od właścicieli oraz kierownictwa wdrożenia wielu systemowych rozwiązań w tym zakresie. Każde przedsiębiorstwo indywidualnie musi opracować wewnętrzne regulacje określające zasady bezpieczeństwa informacji obejmujące wszystkie procesy, w tym logistyczne. Poza rozwiązaniami proceduralnymi ważne jest również stosowanie nowoczesnych narzędzi technicznych oraz informatycznych, zapewniających bezpieczeństwo informacji na poziomie istotnym dla firmy.

Zapewnienie bezpieczeństwa informacji w logistyce wymaga od przedsiębiorstwa wdrożenia procedur oraz odpowiednich zabezpieczeń fizycznych i logicznych (systemy dostępu do danych, hasła itp.). Kluczowym elementem systemu bezpieczeństwa informacji jest opracowanie polityki bezpieczeństwa informacji, która powinna zawierać:

- zestawienie budynków, pomieszczeń lub części pomieszczeń, w którym przetwarzane oraz przechowywane są informacje (wykaz biur, magazynów itp.),
- zestawienie zbiorów danych wraz ze wskazaniem konkretnego oprogramowania wykorzystywanego do przetwarzania informacji w procesach logistycznych,
- charakterystykę sposobu wymiany oraz przepływu danych pomiędzy poszczególnymi systemami informatycznymi użytkowanymi przez organizację,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności (rozumianej jako właściwość zapewniającą, że działania danej organizacji mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi) przetwarzanych w organizacji informacji[1].

Opracowanie oraz wdrożenie polityki bezpieczeństwa jest jednym z elementów, prowadzących do zastosowania odpowiednich rozwiązań technicznych i organizacyjnych. Pomocne w tym zakresie mogą być przytoczone wyżej Polskie Normy. Zgodnie z nimi opracowano szereg wytycznych oraz aktów prawnych, które stanowią dla organizacji cenną wskazówkę jak opracować system zarządzania bezpieczeństwem informacji. Opierając się na ogólnie dostępnych wytycznych zawartych w aktach prawnych, można określić minimalne wymagania w zakresie zarządzania bezpieczeństwem informacji. Organizacja, aby wprowadzić skuteczny system bezpieczeństwa informacji powinna:

- wdrożyć system aktualizacji obowiązujących w organizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia oraz pojawiających się zagrożeń dla bezpieczeństwa informacji przetwarzanych w przedsiębiorstwie,
- monitorować stan posiadanego sprzętu oraz oprogramowania wykorzystywanego do przetwarzania informacji w przedsiębiorstwie,

[1] Opracowano na podstawie wytycznych zawartych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz. U. z 2004 r., Nr 100, poz. 1024, § 4.

- prowadzić okresowy przegląd oraz analizę potencjalnych zagrożeń (ryzyk) w zakresie bezpieczeństwa informacji oraz systemów teleinformatycznych w przedsiębiorstwie,
- dążyć do doskonalenia umiejętności oraz kompetencji pracowników zaangażowanych w proces przetwarzania informacji, w celu zapewnienia posiadania przez nich aktualnych uprawnień umożliwiających im skuteczną realizację zadań w zakresie zapewnienia bezpieczeństwa informacji,
- przeprowadzać okresowe szkolenie pracowników firmy przetwarzających dane ze szczególnym uwzględnieniem problematyki zagrożenia bezpieczeństwa informacji oraz skutków naruszenia zasad bezpieczeństwa informacji, w celu minimalizacji potencjalnych zagrożeń dla bezpieczeństwa danych,
- wprowadzać systemy ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- wdrażać skuteczne systemy dostępu do informacji przetwarzanych w firmie,
- wdrożyć procedury prowadzące do ustalenie przyczyn oraz osób odpowiedzialnych za wystąpienie przypadków naruszenia bezpieczeństwa informacji,
- wdrożyć w przedsiębiorstwie skuteczne środki uniemożliwiające nieautoryzowany dostęp do systemów operacyjnych, usług sieciowych oraz aplikacji wykorzystywanych w firmie,
- wdrożyć procedury oraz mechanizmy zapewniające bezpieczną pracę przy mobilnym przetwarzaniu informacji przez pracowników oraz przy pracy na odległość,
- wdrożyć procedury oraz mechanizmy zabezpieczające informacje w sposób uniemożliwiający nieuprawnione jej ujawnienie, modyfikacje, usunięcie lub zniszczenie,
- wdrożyć w umowach serwisowych podpisanych z usługodawcami zapisy gwarantujące organizacji odpowiedni poziom bezpieczeństwa informacji,

- wdrożyć procedury oraz mechanizmy minimalizacji ryzyka kradzieży informacji i urządzeń teleinformatycznych, w tym urządzeń mobilnych,
- wdrożyć procedury oraz mechanizmy zapewniające firmie odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegający przede wszystkim na:
  - bieżącej dbałości o aktualizację użytkowanego w firmie oprogramowania,
  - minimalizowaniu ryzyka utraty informacji w przypadku wystąpienia awarii,
  - ochronie przed błędami, utratą danych, nieuprawnioną modyfikacją danych,
  - stosowaniu mechanizmów szyfrowania danych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
  - zapewnieniu bezpieczeństwa plików systemowych,
  - redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
  - niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
  - kontroli zgodności systemów teleinformatycznych z odpowiednimi normami, wytycznymi i politykami bezpieczeństwa,
- wdrożyć procedury oraz mechanizmy zapewniające bezzwłoczne zgłaszanie incydentów naruszenia w firmie bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
- wdrożyć obowiązek okresowego przeprowadzania audytu bezpieczeństwa informacji oraz systemów teleinformatycznych wykorzystywanych przez przedsiębiorstwo[1].

[1] Opracowano na podstawie wytycznych zawartych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz

Przytoczone powyżej wytyczne dotyczące zarządzania bezpieczeństwem informacji mają także szerokie zastosowanie w logistyce. Menedżerowie logistyki nie mogliby sprawnie zarządzać procesami logistycznymi w przedsiębiorstwie bez dostępu do aktualnych danych. Realizacja poszczególnych czynności w każdym procesie logistycznym (pakowania, magazynowania, kompletacji, przemieszczania dóbr itd.) nie jest możliwa bez pozyskiwania bieżących informacji. Logistyka musi zapewnić szybką realizację dostaw do odbiorcy, zarówno wewnątrz jak i na zewnątrz organizacji. Szerokie wykorzystywanie możliwości handlu elektronicznego sprawia, że logistyka staje się kluczowym usługodawcą dla firm świadczących tego typu usługi. Specyfika e-usług i handlu elektronicznego wymaga, by zamówiony przez klienta produkt był dostarczony odbiorcy w jak najszybszym terminie. Rosnąca ilość sklepów wirtualnych sprawia, że logistyka zwiększa stale swój zakres działania i obsługi podmiotów gospodarczych. Presja czasu, jaka występuje w handlu elektronicznym, przy jednocześnie ograniczonych zasobach może powodować niewłaściwą ocenę danej informacji, szczególnie przy weryfikacji dużych ilości zamówień do realizacji. Generalnie procesy logistyczne mają zapewnić organizacji szybką realizację danego zamówienia oraz dostarczenie aktualnej informacji np. o stanach zapasów. Od szybkości przepływu informacji zależy terminowość oraz jakość realizacji zadań w zakresie logistyki. Problem ten jest również dostrzegalny w zakresie usług przesyłek kurierskich, gdzie wiarygodna informacja determinuje czas realizacji danego zlecenia. Dlatego też bardzo ważne, żeby zabezpieczyć systemy informatyczne przed nieautoryzowanym dostępem lub modyfikacją. Dotyczy to wszystkich usług świadczonych poprzez portale internetowe. Ewentualne włamanie do internetowego serwisu może skutkować utratą danych klientów oraz wprowadzeniem przez hackera modyfikacji, które sparaliżują pracę firmy elektronicznej. W związku z powyższym nowoczesne organizacje inwestują bardzo duże środki finansowe w rozbudowywanie infrastruktury oraz systemów teleinformatycznych. Dbają one również o modernizację istniejących zabezpieczeń przetwarzanych informacji. Pozwala to zminimalizować ewentualne zagrożenia dla bezpieczeństwa danych.

minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2012 r., poz. 526 ze zm., § 20.

Zwiększenie się ilości generowanych informacji w procesach logistycznych oraz ich wymiany pomiędzy uczestnikami łańcuchów dostaw, powoduje konieczność wzmocnienia systemu ochrony danych. Dotyczy to w szczególności systemów korzystających z ogólnie dostępnych sieci teleinformatycznych. Rozwój wspomnianych wcześniej usług świadczonych drogą elektroniczną powoduje konieczność wzmożonej ochrony danych i użytkowników. Należy sobie jednak zdawać sprawę, że nawet najlepsze systemy bezpieczeństwa nie dają całkowitej gwarancji ochrony danych. Zmiany w technologiach informacyjnych postępują na tyle szybko, że organizacje nie zawsze mogą sprostać nowym zagrożeniom w cyberprzestrzeni. Poza tym zawsze istnieje potencjalne ryzyko wystąpienia incydentu związanego z utratą danych spowodowaną działaniem człowieka. Każdy członek organizacji stanowi potencjalne zagrożenie dla bezpieczeństwa informacji. Dlatego też bardzo ważne jest uświadamianie oraz szkolenie pracowników w tym zakresie.

Bardzo ważną rolę w procesie zarządzania bezpieczeństwem informacji w firmie odgrywa zarządzanie zmianą w obszarze systemów teleinformatycznych. Pojawienie się nowych zagrożeń powinno stymulować kierownictwo firmy do podejmowania działań zmierzających do wdrażania nowych rozwiązań adekwatnych do zmian w tym zakresie. Bez takich działań organizacji może zagrażać utrata danych, która może przynieść straty trudne do oszacowania, a może wręcz zaważyć na pozycji rynkowej firmy.

PODSUMOWANIE

Informacje zawsze stanowiły bardzo ważne dobro każdej organizacji. Ochrona danych posiadanych przez przedsiębiorstwo wymaga zastosowania wielu rozwiązań, zarówno metodologicznych jak i technicznych. Bezpieczeństwo informacji w obszarze logistyki powinno być jednym z obszarów zarządzania bezpieczeństwem informacji przedsiębiorstwa. Zmiany techniki przetwarzania i gromadzenia danych powodują nowe zagrożenia w tym zakresie. Zawsze w organizacji istniało ryzyko utraty informacji, jednakże postęp technologiczny, wdrożenie handlu elektronicznego oraz sieć Internet zwiększyło potencjalnie katalog tych zagrożeń. Przed erą rewolucji informatycznej, trudniej było uzyskać dostęp do danych bez fizycznej obecności w siedzibie organizacji. Dynamiczny rozwój Internetu poza wieloma zaletami, przyczynił się także do szerokiego otwarcia nowych „drzwi" do zasobów informacyjnych

przedsiębiorstw. Dzisiaj wystarczy jedynie dostęp do sieci oraz posiadanie odpowiednich umiejętności oraz narzędzi informatycznych, aby dane firmy były dostępne dla niepowołanej osoby. Przyczynia się do tego również wzrost ilości usług świadczonych drogą elektroniczną. Bardzo często Internetowe serwisy stają się przedmiotem ataku hackerów, którzy testują poziom zabezpieczeń stosowanych przez wirtualne firmy.

Logistyka pełni w organizacjach bardzo ważną funkcję, ponieważ zapewnia przepływy dóbr pomiędzy podmiotami. Poszczególne procesy logistyczne nie mogą być realizowane bez skutecznego przepływu informacji. Informacja odgrywa w logistyce kluczową rolę, ponieważ zależy od niej realizacja poszczególnych czynności w określonym miejscu i terminie. Zaplanowanie oraz zrealizowanie dostawy nie byłoby możliwe bez pozyskania danych potrzebnych do przygotowania i dostarczenia dobra w wyznaczonym terminie w określone miejsce. Zwiększająca się ilość przedsiębiorstw korzystających z zewnętrznych usług logistycznych powoduje konieczność zwiększania skuteczności przepływu informacji. Nieuprawniony dostęp do danych generowanych przy realizacji jakiejkolwiek usługi logistycznej (magazynowania, transportu, pakowania itp.) może mieć poważne konsekwencje dla firm współpracujących w łańcuchu dostaw. Każda taka sytuacja stanowi bowiem poważne zagrożenie dla funkcjonowania przedsiębiorstwa, dlatego też bardzo ważne jest wdrażanie skutecznych i nowoczesnych systemów bezpieczeństwa informacji.

Bezpieczeństwo informacji w logistyce wymaga zastosowania wielu rozwiązań organizacyjnych i technicznych stosowanych na całym świecie. Wypracowane wytyczne oraz normy dotyczące bezpieczeństwa informacji są uniwersalne i mogą być wdrażane w każdej organizacji. Oczywiście ich wdrożenie będzie zależne od specyfiki realizowanych zadań oraz liczby podmiotów i użytkowników systemu. Zaniechanie działań w tym zakresie nie zapewni skutecznej ochrony danych przetwarzanych przez organizację.

Bezpieczeństwo informacji jest zagadnieniem, które będzie nadal się rozwijać wraz z postępem technologicznym oraz rosnącą liczbą użytkowników. Należy zakładać, że również procesy logistyczne będą wymagać ciągłego doskonalenia w obszarze bezpieczeństwa informacji. Bez działań w tym zakresie organizacje będą zawsze narażone na nieuprawniony dostęp do danych, ich modyfikację lub wręcz na utratę informacji [Dziekański 2012].

SPIS LITERATURY

CobiT 4.1 Metodyka, Cele kontrolne. Wytyczne zarządzania. Modele dojrzałości, USA 2007, IT Governance Institute, s. 5, www.itgi.org

Coyle J. J., E.J. Bardi, C.J. Langley, *Zarządzanie logistyczne*, PWE, Warszawa 2010.

Dziekański P., *Informacja jako dobro ekonomiczne będące źródłem przewagi konkurencyjnej*, s. 387-403 [w:] M.G. Woźniak (red. nauk.), Nierówności społeczne a wzrost gospo-darczy, Zeszyt 24, Uniwersytet Rzeszowski, Katedra Teorii Ekonomii i Stosunków Międzynarodowych.

Gołembska E., *Logistyka w gospodarce światowej*, C.H. Beck, Warszawa 2009.

Griffin R. W., *Podstawy zarządzania organizacjami*, wyd. 2, PWN, Warszawa 2006.

Harrison A., R. van Hoek, *Zarządzanie logistyką*, PWE, Warszawa, 2010 r.

Jashapara A., *Zarządzanie wiedzą*, wyd. 2, PWE, Warszawa 2014.

Krawczyk S., *Logistyka w przedsiębiorstwie* [w:] S. Krawczyk (red.), *Logistyka. Teoria i praktyka cz. 1*, Difin, Warszawa 2011.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2009.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 23 czerwca 2013.

Polska Norma PN-ISO/IEC 17799 - Technika informatyczna, Techniki bezpieczeństwa, Praktyczne zasady zarządzania bezpieczeństwem informacji, Polski Komitet Normalizacji, Warszawa 2007.

Polska Norma PN-ISO/IEC 20000-1:2007 Technika informatyczna. Zarządzanie usługami. Część 1: Specyfikacja, Polski Komitet Normalizacji, Warszawa 2007.

Polska Norma PN-ISO/IEC 20000-2:2007 Część 2: Reguły postępowania. Polski Komitet Normalizacji, Warszawa 2007.

Polska Norma PN-ISO/IEC 24762 Technika informatyczna. Techniki bezpieczeństwa. Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie, Polski Komitet Normalizacji, Warszawa, maj 2010.

Polska Norma PN-ISO/IEC 27001. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, Polski Komitet Normalizacji, Warszawa 2007 r.

Polska Norma PN-ISO/IEC 27005 Technika informatyczna, Techniki bezpieczeństwa, Zarządzanie ryzykiem w bezpieczeństwie informacji, Polski Komitet Normalizacji, Warszawa, marzec 2010.

Remlein P., *Systemy łączności bezprzewodowej w logistyce* [w:] J. Długosz, *Nowoczesne technologie w logistyce*, PWE, Warszawa 2009.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,Dz. U. z 2004 r., Nr 100, poz.1024.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2012 r., poz. 526 ze zm.

Skowronek Cz., Sarjusz – Wolski Z., *Logistyka w przedsiębiorstwie*, PWE, Warszawa 2008.

Stoner J. A. F., Freeman R. E.,. Gilbert Jr. D. R, *Kierowanie*, PWE, Warszawa 2011.