PAŁĘGA Michał[1]

System zarządzania bezpieczeństwem informacji ISO/IEC 27001 w działalności logistycznej

WSTĘP

Działalność na rynku usług logistycznych wiąże się z fizycznym przepływem towarów oraz towarzyszącą mu wymianą informacji. Na podkreślenie zasługuje fakt, iż procesy te zdecydowanie różnią się między sobą. Proces przemieszczania dóbr z miejsca ich wytworzenia do miejsca ich potencjalnej konsumpcji ma zmaterializowaną postać, można go zobaczyć oraz wycenić. W przypadku transmisji informacji jest to nie możliwie. Niemniej jednak zarządzanie przepływem informacji w organizacji jest niezmiernie ważnym zagadnieniem. Bowiem, od sprawnie funkcjonującego systemu informacyjnego w dużym stopniu zależy powodzenie misji przedsiębiorstwa [1,3,9]. Dlatego też nadrzędnym celem każdej organizacji, w tym przede wszystkim przedsiębiorstw świadczących usługi logistyczne powinna być szczególna troska o bezpieczeństwo informacji oraz technologii informatyczno – komunikacyjnej, która je gromadzi, przetwarza oraz dystrybuuje [10].

Organizacje będące świadome znaczącej roli bezpieczeństwa i ochrony informacji w procesach realizacji misji i celów, obsługi klienta, a w konsekwencji budowania przewagi konkurencyjnej na rynku poszukują najlepszych, światowych rozwiązań w tym zakresie. Z pomocą przychodzi tutaj międzynawowych standard ISO/IEC 27001: 2005, stanowiący zbór zaleceń, wymagań oraz dobrych praktyk, których zaimplementowanie do systemu bezpieczeństwa informacji gwarantuje jego niezawodność, a dla klientów, dostawców i osób trzeci organizacji jest świadectwem dbałości o zachowanie wysokiej jakości wymienianej informacji.

Celem niniejszego artykułu jest zwrócenie uwagi czytelnika na koncepcję systemu zarządzania bezpieczeństwem informacji opartego na identyfikacji zagrożeń oraz analizie ryzyka, ukierunkowanego na ustanawianie, wdrażanie, eksploatację, monitorowanie, utrzymanie i doskonalenie bezpieczeństwa informacji, poddawanego certyfikacji przez akredytowaną jednostkę certyfikującą. Ponadto w opracowaniu dokonano przeglądu rejestru certyfikatów ISO/IEC 27001: 2005 przyznawanych organizacjom w Polsce, ze szczególnym uwzględnieniem przedsiębiorstw działających w sektorze logistyka i transport.

1. POJĘCIE I ISTOTA BEZPIECZEŃSTWA INFORMACJI

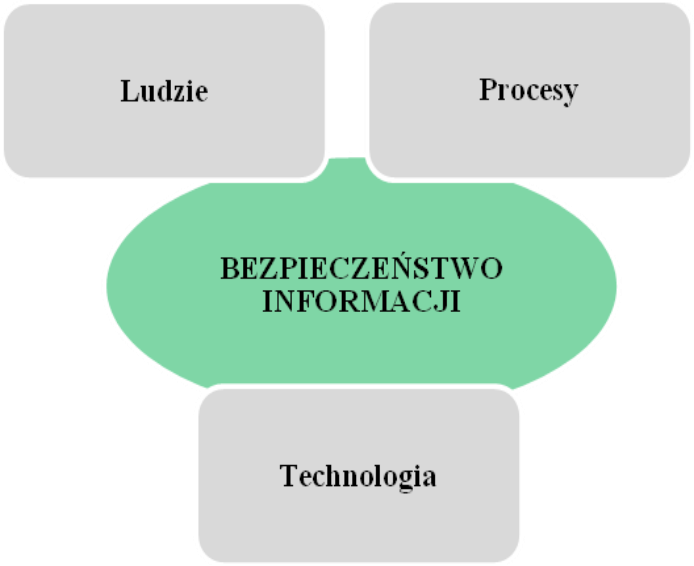
Pojęcie bezpieczeństwa informacji, zgodnie z literaturą przedmiotu definiowane jest jako zbiór przedsięwzięć, mających na celu ochronę informacji, ważnego elementu współczesnego systemu gospodarczego, jakim jest instytucja bądź organizacja gospodarcza, zapewniający jego efektywne i niezawodne funkcjonowanie. Zgodnie z prezentowanymi w piśmiennictwie treściami informację uznaje się za bezpieczną, wówczas gdy zagwarantowane są wszystkie atrybuty jej bezpieczeństwa: poufność (*confidentiality*), spójność (*integrity*), dostępność (*availability*), rozliczalność (*accountability*), autentyczność (*authenticity*), niezaprzeczalność (*non-repunddation*) i niezawodność (*reliability*) [6,10]. Wobec powyższego bezpieczeństwo informacji należy rozmieć wielowymiarowo, uwzględniając nie tylko wielość atrybutów informacji, podlegających ochronie, ale także różnorodność form ich występowania (np. w postaci pliku danych, wydruku, zapisu w formie elektronicznej i tradycyjnej, rekordu w bazie danych czy wiadomości przekazywanej ustnie). Charakterystykę poszczególnych atrybutów bezpieczeństwa przybliżono w tabeli 1.

[1] Politechnika Częstochowska, Wydział Inżynierii Produkcji i Technologii Materiałów, Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa

Tab. 1. Atrybuty bezpieczeństwa informacji [6,8]

Poufność - zapewnienie, że informacja nie jest udostępniania bądź ujawniana osobom podmiotom i procesom nieuprawnionym	**Integralność** - oznacza precyzyjność, dokładność oraz kompletność informacji	**Dostępność** - zakłada możliwość autoryzowanego wykorzystania danych i informacji w pożądanym czasie
Autentyczność - zapewnienie, że tożsamość podmiotu bądź zasobu jest zgodna z deklarowaną (dotyczy to użytkowników, procesów, systemów, a nawet instytucji)	**Rozliczalność** - wiąże się z jednoznacznym przypisaniem określonego zakresu działań do jednemu podmiotowi	**Niezawodność** - oznacza stałe, spójne zamierzone zachowania oraz skutki

Bezpieczeństwo informacji można także definiować jako systematyczne podejście do zarządzania kluczowymi informacji instytucji bądź podmiotów gospodarczych w celu zagwarantowania racjonalnego poziomu ich bezpieczeństwa. Obejmuje ona ludzi, procesy oraz technologię – obecnie nie można bowiem ograniczać się do bezpieczeństwa danych gromadzonych i przetwarzanych w systemach informatycznych [6,10]. Strukturę bezpieczeństwa informacji prezentuje rys. 1.



Rys. 1. Model systemu bezpieczeństwa informacji [6]

Problematyka bezpieczeństwo informacji w dzisiejszym świecie dotyczy praktycznie wszystkich podmiotów rządowych i komercyjnych (w tym m.in. przedsiębiorstw, banków i instytucji finansowych, jednostek rządowych i samorządowych, służby zdrowia czy organizacji non – profit). Wszystkie funkcjonujące na rynku organizacje zobligowane są do skutecznego zarządzania bezpieczeństwem informacji. Wobec powyższego wiele z nich poszukuje odpowiednich wytycznych w tym zakresie. Odpowiedź na tę potrzebę może stanowić system zarządzania zgodny z ISO 27001, który umożliwia zarządzanie bezpieczeństwem informacji w sposób kompleksowy i usystematyzowany, oparty na podejściu wynikającym z ryzyka biznesowego.

2. SYSTEM ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Zgodnie z definicją zawartą w normą ISO/IEC 17799 system zarządzania bezpieczeństwem informacji należy rozumieć jako „część całościowego systemu zarządzania, opracowana na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji" [7]. Wobec powyższego celem zapewnienia racjonalnego poziomu bezpieczeństwa informacji organizacje gospodarcze oraz

instytucje zmuszone są niejako stosować w ramach opracowanej i przyjętej polityki bezpieczeństwa podejście procesowe, co wiąże się z identyfikacją zagrożeń oraz realizacją wielu przedsięwzięć, które angażują określone zasoby i wymagają właściwego zarządzania ukierunkowanego na proces, czyli transformację wektorów wejścia w wektory wyjścia [6]. Ponadto podejście procesowe do systemu zarządzania bezpieczeństwem informacji wymaga także koncentracji na następujących kwestach:

- zrozumieniu wymagań bezpieczeństwa informacji w organizacji;
- wdrożeniu i użytkowaniu zabezpieczeń w celu należytego zarządzania ryzykiem;
- nadzorowaniu efektywności i skuteczności ISMS;
- ciągłemu doskonaleniu w oparciu o rzeczywiste, obiektywne pomiary.

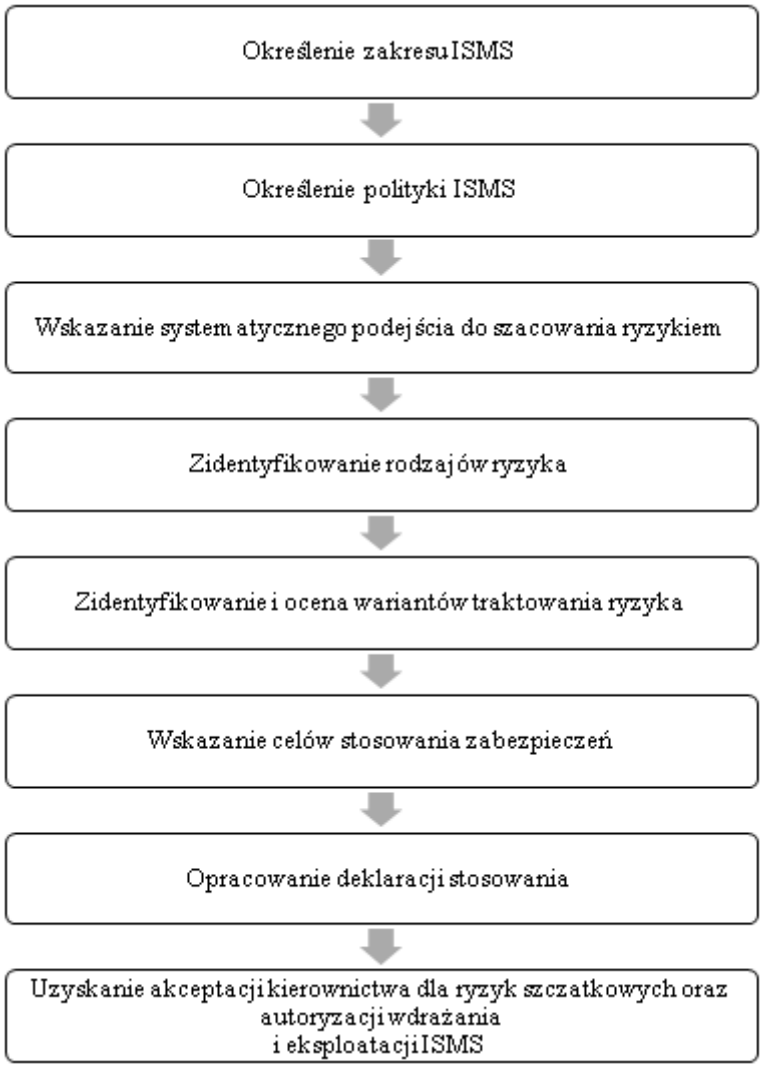
System zarządzania bezpieczeństwem informacji (ISMS) bazuje na dwóch zasadniczych standardach o charakterze międzynarodowym. Zalicza się do nich:

- ISO/IEC 17799: 2005 – norma stanowiąca zbiór wytycznych, zaleceń, dobrych praktyk w zakresie utworzenia i utrzymania ISMS;
- ISO/IEC 27001: 2005 – norma zawierająca zestaw niezbędnych wymagań, jakim organizacja jest zobligowana sprostać, ubiegając się o certyfikat ISMS.

Obejmuje on swoim zakresem strukturę organizacyjną, politykę, zakres odpowiedzialności, zasady, procedury, procesy oraz zasoby. Postuluje się, aby podjęcie decyzji związanej z implementacją systemu zarządzania bezpieczeństwem informacji wynikało z określonych potrzeb oraz założonych celów biznesowych organizacji i przedsiębiorstwa, a także z wymagań obejmujących sferę bezpieczeństwa.

2.1. Ustanawianie ISMS

Ustanawianie sprawnie działającego ISMS wiąże się z koniecznością systematycznego podejścia, które powinno uwzględniać kilka następujących po sobie procesów. Poszczególne jego etapy prezentuje rys. 2.



Rys. 2. Etapy ustanawiania ISMS [5,8]

Kolejnym etapem we wdrażaniu i ustanawianiu ISMS jest identyfikacja ryzyka, która polega na wskazaniu zasobów oraz przypisaniu do nich zagrożeń, podatności oraz skutków wystąpienia niebezpieczeństwa.

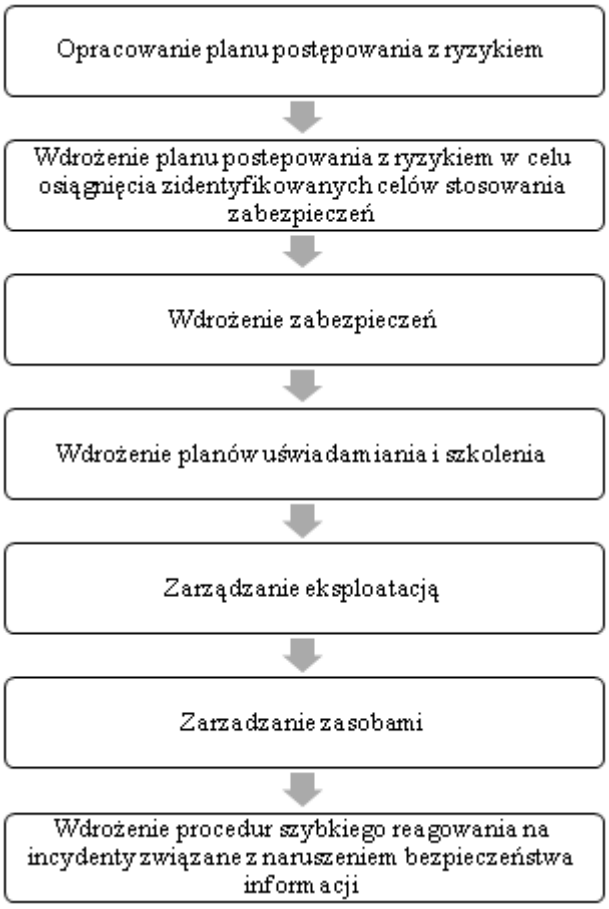
Norma definiuje również konieczność analizy i oceny ryzyka. Odbywa się to poprzez [4]:
- wyznaczenie strat i szkód wynikających z naruszenie bezpieczeństwa informacji w organizacji;
- określenie realnego prawdopodobieństwa wystąpienie niekorzystnego zdarzenia;
- oszacowanie poziomu wyznaczonych rodzajów zagrożeń;
- ustalenie, czy ryzyko jest na poziomie akceptowalnym.

Kolejnym wymaganiem dyktowanym przez normę w zakresie ISMS jest identyfikacja oraz ocena wariantów traktowania ryzyka. Wyróżnia się następujące możliwości [4,5]:
- wdrożenie stosownych zabezpieczeń;
- unikanie ryzyka;
- akceptowanie ryzyka;
- transfer ryzyka (np. na ubezpieczyciela).

Wszystkie zabezpieczenia, które trzeba bezwzględnie wdrożyć w ramach ISMS określone zostały w załączniku A do normy – należy jednak mieć na uwadze, iż ich lista nie jest kompletna i w szczególnych przypadkach może zaistnieć konieczność zastosowania dodatkowych zabezpieczeń. Zestawienie wszystkich zaimplementowanych zabezpieczeń wraz z uzasadnieniem ich wyboru należy określić w tzw. deklaracji stosowania ISMS.

2.2. Wdrażanie i eksploatacja ISMS

Wdrożenie i eksploatacja ISMS, zgodnie z wymogami zawartymi w nomie koncentruje się na kilku podstawowych działaniach. Ich zakres został przedstawiony w sposób graficzny na rys. 3.



Rys. 3. Zasady wdrażania i eksploatacji ISMS [5,8]

Przedstawione na schemacie działania są bardzo ogólne, jednakże wyznaczają strategiczne kierunki aktywności związane z zarządzaniem bezpieczeństwem informacji w oparciu o międzynarodowy standard ISO 27001.

2.3. Monitorowanie i przegląd

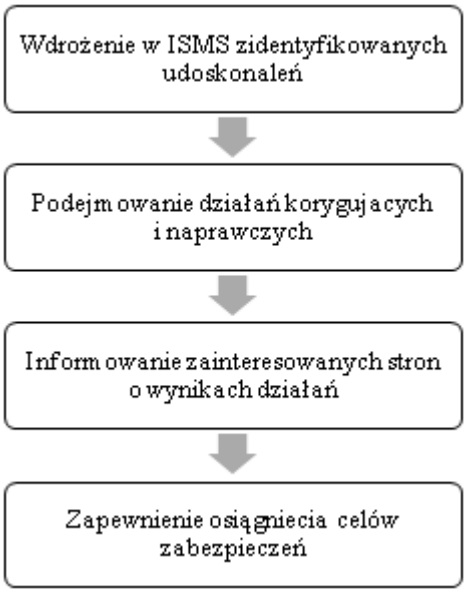
W ramach systemu zarządzania bezpieczeństwem informacji monitorowanie i przegląd ISMS polega przede wszystkim na [4,5]:

- realizacji procedur szybkiego reagowania w sytuacji wystąpienia incydentu naruszenia bezpieczeństwa informacji;
- dokonywaniu systematycznych pomiarów efektywności ISMS (z uwzględnieniem zgodności z polityką i celami oraz przeglądów zabezpieczeń) biorąc pod uwagę wyniki z audytów bezpieczeństwa;
- przeprowadzaniu przeglądów poziomu ryzyka szczątkowego i akceptowalnego, uwzględniając przy tym zachodzące zmiany w obrębie stosowanej technologii, założonych celów biznesowych, zidentyfikowanych zagrożeń oraz obowiązujących w danym czasie uregulowań prawnych;
- wykonywaniu regularnych audytów wewnętrznych ISMS z ustaloną częstotliwością działań;
- dokonywaniu przeglądów ISMS przez kierownictwo organizacji – przynajmniej raz w roku.

Zgodnie z normą zasadniczym celem przeprowadzonych przeglądów jest weryfikacja zakresów systemu oraz identyfikacja następujących zmian. Ponadto w oparciu o dokonywany monitoring i przegląd należy aktualizować plany bezpieczeństwa i dopasowywać je do aktualnych potrzeb i wymagań systemu [4,5].

2.4. Utrzymanie i doskonalenie ISMS

Otrzymanie przez organizację certyfikatu systemu zarządzania bezpieczeństwem informacji narzuca konieczność przestrzegania przez nią określonych zasad, wskazanych w normie. Jedną z nich jest utrzymanie i doskonalenie ISMS, których realizacja obejmuje klika podstawowych działań. Ich zakres został przedstawiony na rys. 4.



Rys. 4. Zasady prawidłowego utrzymania i doskonalenia ISMS [5,8]

3. CERTYFIKACJA SYSMETMU ZARZĄDZANIE BEZPIECZENSTWEM INFORMACJI ISO/IEC 27001: 2007 W DZIAŁALNOŚCI LOGISTYCZNEJ

Współczesne przedsiębiorstwa, zarówno polskie, jak i zagraniczne coraz większą wagę przywiązują do poziomu bezpieczeństwa informacji. Jakość świadczonych usług obecnie nie przejawia się tylko i wyłącznie zapewnieniem satysfakcji i zadowolenia odbiorców, ale także przyjętymi przez organizację procedurami zarządzania związanymi z ochroną powierzanych, gromadzonych i przetwarzanych informacji. Z tego też względu wzrasta liczba przedsiębiorstw i instytucji zainteresowanych wdrażaniem systemu zarządzania bezpieczeństwem informacji. Dowodem na zastosowanie w tym obszarze światowych standardów i dobrych praktyk jest posiadanie przez organizację certyfikowanego systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001: 2005.

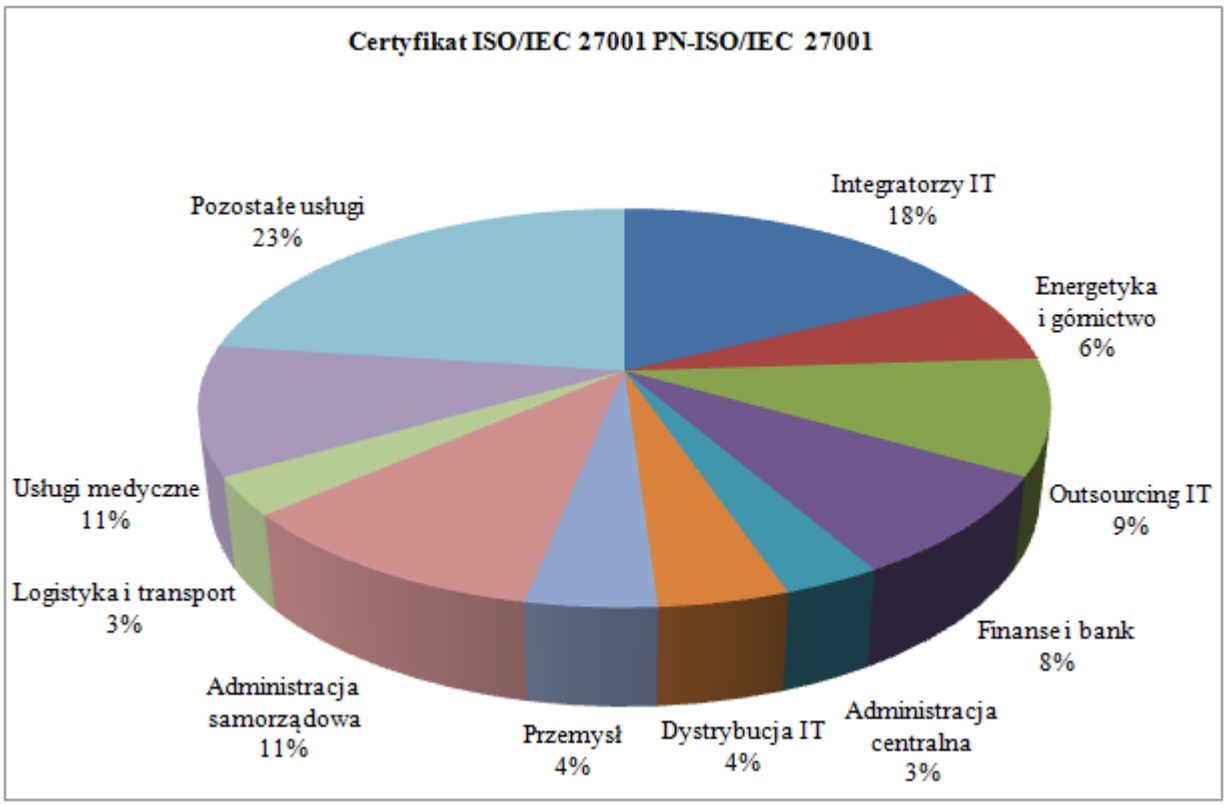
Podmioty ubiegające się o certyfikację ISMS zobligowane są do zbudowania efektywnego systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami normy, stanowiącego jego podstawę. W normie określonych zostało 36 celów oraz 136 zabezpieczeń [8]. Na podkreślenie zasługuje fakt, iż dozwolone są wyłącznie, z uwagi na specyficzne uwarunkowania funkcjonowania określonej jednostki gospodarczej. W oparciu o oszacowane ryzyko przedsiębiorstwo samo decyduje, jakiego rodzaju zabezpieczenia zaimplementuje do swojej struktury. Istnieje również możliwość zastosowania dodatkowych zabezpieczeń, nie uwzględnionych w normie [4].

W procesie akredytowanej certyfikacji, jednostki certyfikujące oceniające zgodność oraz skuteczność systemu zarządzania bezpieczeństwem informacji poszukują dowodów, na to, że organizacja zdolna jest zagwarantować bezpieczeństwo trzech podstawowych cech informacji, (tj. poufność, spójność oraz dostępność).

Jednostki, którym przyznano certyfikat zgodności z normą ISO/IEC 27001, mogą „reklamować się" jako organizacje przywiązujące najwyższą wagę do wartości bezpieczeństwa informacji poprzez wdrożenie niezbędnych środków ostrożności przeciwdziałających takim zagrożeniom jak: nieuprawniony dostęp czy nieautoryzowana modyfikacja.

Niezwykle istotną kwestią jest zapewnienie właściwego poziomu bezpieczeństwa informacji w działalności usług logistycznych. Logistyka, jak podaje jedna z definicji to fizyczny przepływ towarów, ale to także towarzyszący mu przepływ ogromnej ilości różnego typu informacji. Uwzględniając dodatkowo fakt, że firmy logistyczne coraz częściej wspomagają się w swojej działalności nowoczesną technologią informatyczno – komunikacyjną niezbędnym jest tworzenie niezawodnych systemów zabezpieczania informacji. Zagwarantowanie bezpiecznego zarządzania informacją jest fundamentem nowoczesnego zarządzania łańcuchem dostaw, ale także wpływa na proces kształtowania zaufania i pozytywnych relacji pomiędzy firmą logistyczną a jej odbiorcami, a w konsekwencji determinuje pozycję konkurencyjną przedsiębiorstwa na rynku.

Praktyka gospodarcza pokazuje jednak, iż nie wszystkie podmioty logistyczne podzielają tego typu teorię, czego dowodzą dane zamieszczone na rys. 5, prezentujące rejestr certyfikatów ISO/IEC 27001 przyznanych organizacjom w Polsce, z podziałem według branż [11].



Rys. 5. Rejestr certyfikatów ISO/IEC 27001 przyznawanych organizacjom w Polsce, z podziałem według branż [11].

Z zebranych danych wynika bowiem, iż w Polsce jednie 3% przedsiębiorstw działających w sektorze Logistyka i Transport posiada świadectwo doskonale zorganizowanego systemu zarządzania bezpieczeństwem informacji, zgodnego z międzynarodowym standardem ISO/IEC 27001 – podobnie jak w przypadku organizacji należących do administracji centralnej. Największy odsetek przedsiębiorstw wdrażający ISMS zgodny z ISO/IEC 27001 przypada branżom zdefiniowanym jako pozostałe usługi (23%) oraz integratorzy IT. Fakt ten może dowodzić, iż w polskiej gospodarce nadal panuje przekonanie, że bezpieczeństwo informacji to domena głównie informatyki. Należy jednak mieć nadzieję, iż w niedalekiej przyszłość świadomość organizacji w Polsce w zakresie konieczności kształtowania bezpiecznych warunków gromadzenia, przetwarzania oraz przepływu informacji będzie wzrastać, co będzie przekładać się również na liczbę posiadanych certyfikatów ISO/IEC 27001 przez przedsiębiorstwa i instytucje reprezentujące różne gałęzie gospodarki, w tym także sektor usług logistycznych [11].

W tabeli 2 zaprezentowano zbiorcze zestawie przedsiębiorstw z branży Logistyka i Transport, których systemy zarządzania bezpieczeństwem informacji spełniły wymagania zawarte w normie ISO/IEC 27001, co potwierdzone zostało w procesie akredytowanej certyfikacji.

Tab. 2 Rejestr certyfikatów ISO/IEC 27001 przyznawanych organizacjom w Polsce z branży Logistyka i Transport [11]

Lp.	Organizacja	Liczba pracowników	Data przyznania	Akredytacja	Standard
1.	Genpact	100-250	2012-10-15	✓	ISO/IEC 27001
2.	LeasePlan Fleet Management Polska Sp. z o. o.	do 100	2011-04-25	✓	ISO/IEC 27001
3.	PKP CARGO SERVICE Sp. z o. o.	brak danych	2012-11-23	✓	PN-ISO/IEC 27001
4.	Sadi Polska Agencja Celna Sp. z o.o.	brak danych	2008-07-07	✓	ISO/IEC 27001
5.	Schenker Sp. z o. o.	1000-5000	2006-12-21	✓	ISO/IEC 27001
6.	Siódemka S.A.	250-1000	2008-01-28	✓	ISO/IEC 27001

Z analizy danych zamieszczonych w tab. 2 wynika, że Schenker Sp. z o.o. była pierwszą firmą na polskim rynku usług logistycznych, która zdecydowała się na certyfikację systemu zarządzania bezpieczeństwem informacji, zgodnego z ISO/IEC 27001. Jak możemy przeczytać na stronie internetowej Spółki zapewnienie bezpieczeństwa w całym łańcuch świadczonych usług logistycznych, w tym również bezpieczeństwa i ochrony aktywów informacyjnych jest jednym z jej priorytetów. Spółka szczególną troskę przywiązuje do dbałości o poufność informacji, odpowiednie zabezpieczenie danych swoich klientów przed niekontrolowanym wyciekiem oraz dobry poziom komunikacji na linii firma-klient [2].

PODSUMOWANIE

Sukcesy rynkowe przedsiębiorstw od zawsze skorelowane były z jakością świadczonych usług czy oferowanych produktów. Nie mniej jednak znaczenie jakości uległo zasadniczej transformacji. Jakość współcześnie nie oznacza już tylko zagwarantowania satysfakcji czy zachwycenia klienta oferowanymi dobrami bądź usługami, ale dotyka wielu różnych aspektów związanych z zarządzaniem organizacją. W przypadku działalności firm logistycznych, niewątpliwie wartością wysoko cenioną przez ich klientów i kontrahentów z pewnością są m.in. procedury związane z ochroną i bezpieczeństwem przetwarzanych i wymienianych informacji.

Organizacje, aby zachowywać zdolność do przetrwania i rozwoju zmuszone są nieustannie reagować na zachodzące w ich otoczeniu zmiany. Taka sytuacja powoduje, iż coraz więcej podmiotów gospodarczych wdraża bądź deklaruje konieczność wdrożenia systemu zarządzania bezpieczeństwem informacji [4,9]. Światowym standardem, stanowiącym zbiór wymagań, zaleceń oraz dobrych praktyk w tej dziedzinie jest norma ISO/IEC 27001: 2005.

Z zaprezentowanych w niniejszym opracowaniu danych wynika, że liczba certyfikacji systemu zarządzania bezpieczeństwem informacji zgodnych z normą ISO/IEC 27001 przyznawanych organizacjom w Polsce (w tym z sektora logistyka i transport) jest niewielka. Nie świadczy to jednak o tym, iż organizacje nie wykorzystują rozwiązań w niej zawartych jako wzorca do budowania własnego systemu bezpieczeństwa informacji. Opór organizacji przed procesem certyfikacji często wynika z jego złożoności oraz nadmiernych nakładów finansowych. Należy jednak mieć na uwadze, iż priorytetem w omawianym obszarze zarządzania nie jest to, czy organizacje poddają certyfikacji swój system zarządzania bezpieczeństwem informacji, a kompleksowa ochrona zasobów informacyjnych i systemów je przetwarzających przed zagrożeniami, które w dzisiejszym świecie przybierają coraz to bardziej wyrafinowane formy.

Streszczenie

Informacje niewątpliwie pełnią znaczącą rolę w sektorze logistycznym oraz stanowią ważny element w procesie osiągania przewagi konkurencyjnej przedsiębiorstwa. Dlatego też istnieje potrzeba zbudowania w organizacji odpowiedniego systemu gwarantującego ochronę informacji przed zagrożeniami. W niniejszym artykule opisano podejście do zarządzania bezpieczeństwem informacji z wykorzystaniem normy ISO/IEC 27001. Przedstawiono w nim również wyniki analiz akredytowanej certyfikacji ISMS w sektorze usług logistycznych.

Information security management system ISO/IEC 27001 in the logistics enterprise

Abstract

Undoubtedly, the information play a very important role in logistics sector and are important asset while increasing the competitiveness by the companies. Therefore, it's necessary to construct appropriate system in organization, which guarantee information security before threats. In this article describes the way of approach to information security management in companies in accordance with ISO/IEC 27001 norm. Article presents results of analysis accredited certifications ISMS in logistics sector.

BIBLIOGRAFIA

1. Borowiecki R., Czekaj J., *Zasoby informacyjne w ograniczaniu ryzyka gospodarczego*, Wyd. Dom Organizatora, Toruń 2011.
2. http://dbschenker-csr.pl/pl/raport-spoleczny-obszary/klienci/bezpieczenstwo-informacji
3. Kot S. (red.), Nowe kierunki rozwoju logistyki, Wyd. Politechnika Częstochowska, Częstochowa 2008.
4. Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.
5. Molski M., Łacheta M., *Przewodnik audytora systemów informatycznych*, Wyd. Helion, Gliwice 2007.
6. Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Wyd. AON, Warszawa 2010.
7. PN-ISO/IEC 1779:2007. *Praktyczne zasady zarządzania bezpieczeństwem informacji*, Wymagania, PKN, Warszawa
8. PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji, Wymagania, PKN, Warszawa
9. Prauzner T., *Prawo a bezprawie w Internecie*, [w:] Prace Naukowe Akademii im. Jana Długosza w Częstochowie, Tom IV, Wyd. AJD, red. A. Gil, Częstochow 2009, s. 297-302.
10. Prauzner T., *Technologia informacyjna – wybrane problemy społeczne*, [w] Edukacja-Technika-Informatyka nt: „*Wybrane problemy edukacji informatycznej i informacyjnej*", Rocznik Naukowy Nr 3/2012 cz.2, red. dr hab. prof. UR Walat W., Wyd. FOSZE, Rzeszów 2012 , s.39-45.
11. www.iso27000.pl