ANALIZA RYNKU CERTYFIKACJI SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W LATACH 2006-2009

Monika STOMA

Streszczenie: W pracy przedstawiono istotę i znaczenie informacji oraz jej ochrony we współczesnych przedsiębiorstwach. Zaprezentowano także koncepcję systemu zarządzania bezpieczeństwem informacji, ze szczególnym uwzględnieniem korzyści z wdrożenia systemu w przedsiębiorstwie oraz poddania go certyfikacji przez akredytowaną jednostkę certyfikującą. Podjęto ponadto próbę przeprowadzenia analizy rynku certyfikacji systemów zarządzania bezpieczeństwem informacji w latach 2006-2009 na świecie, ze szczególnym uwzględnieniem krajów europejskich oraz Polski.

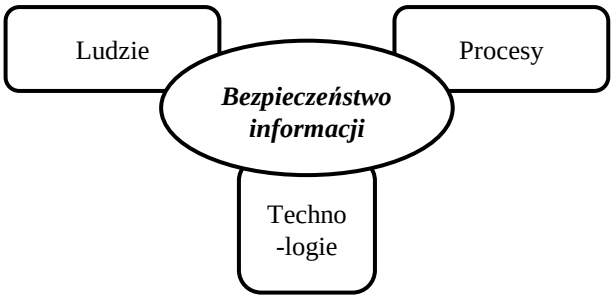
Słowa kluczowe: informacja, system zarządzania bezpieczeństwem informacji, certyfikacja, audit, normy ISO.

1. Informacja i jej bezpieczeństwo we współczesnych przedsiębiorstwach

Współcześnie informacja jest niezwykle istotnym towarem i jednocześnie zasobem w działalności przedsiębiorstw, a także stanowi jeden z najważniejszych czynników sukcesu firm w dynamicznie zmieniającym się otoczeniu biznesowym. Informacja jest więc aktywem, który podobnie jak inne ważne aktywa biznesowe (składniki kapitału przedsiębiorstwa), ma dla przedsiębiorstwa wartość i dlatego należy ją odpowiednio chronić.

Stąd też przedsiębiorstwa zaczynają zwracać uwagę na bezpieczeństwo posiadanych informacji, co oznacza przede wszystkim zachowanie poufności (zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym), integralności (zapewnienie dokładności, wiarygodności i kompletności informacji oraz metod ich przetwarzania) oraz dostępności informacji (zapewnienie że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów, wtedy gdy jest to potrzebne) – tzw. triada CIA (Confidentiality, Integrity, Availability). Można więc stwierdzić, iż bezpieczeństwo informacji należy rozpatrywać wielowymiarowo, biorąc pod uwagę przede wszystkim wielość atrybutów informacji, które podlegają ochronie, ale również wielość form, jakie może przybrać informacja (plik w komputerze, wydruk, zapis tradycyjny lub elektroniczny, rekord w bazie danych, informacja ustna, itd.).

Bezpieczeństwo informacji można zdefiniować również jako systematyczne podejście do zarządzania kluczowymi informacjami firmy w celu zapewnienia ich bezpieczeństwa. Obejmuje ono ludzi, procesy i systemy informatyczne - w dzisiejszych czasach nie można bowiem ograniczać bezpieczeństwa do samych tylko systemów informatycznych, rys. 1 [6].



Rys. 1. Struktura bezpieczeństwa informacji
Źródło: opracowanie własne

Szczególny nacisk na bezpieczeństwo informacji kładą jednak organizacje, dla których ochrona informacji ma zasadnicze znaczenie (np. takie, w których jedną z realizowanych funkcji jest przetwarzanie dużej ilości danych osobowych). Aby więc skutecznie zarządzać bezpieczeństwem informacji w przedsiębiorstwie należy wdrożyć system zarządzania bezpieczeństwem informacji, który powinien stanowić integralną część systemu zarządzania przedsiębiorstwem i być oparty na podejściu wynikającym z ryzyka biznesowego.

2. System zarządzania bezpieczeństwem informacji

Koncepcja systemu zarządzania bezpieczeństwem informacji (*ang. Information Security Management System – ISMS*) opiera się o podejście systemowe zgodnie z cyklem ciągłego doskonalenia Deminga, czyli cyklem PDCA (Plan-Do-Check-Act). Podstawą do jego opracowania stało się założenie, że zjawiska jakościowe mają charakter dynamiczny, a jakością procesów i wyrobów należy sterować w cyklu działań zarządczych i wykonawczych. Dla bezpieczeństwa informacji oznacza to m.in.:

- Planowanie – sformułowanie polityki i zasad zarządzania bezpieczeństwem informacji oraz oszacowanie poziomu ryzyka związanego z przechowywanymi informacjami w przedsiębiorstwie, czyli tworzenie (ustanowienie) systemu zarządzania bezpieczeństwem informacji;
- Realizacja – wdrożenie i funkcjonowanie procedur związanych z minimalizacją ryzyka w odniesieniu do posiadanych informacji;
- Ocena – prowadzenie bieżącego monitoringu realizowanych działań i procedur oraz okresowych przeglądów i auditów wewnętrznych dotyczących systemu zarządzania bezpieczeństwem informacji w zaplanowanych odstępach czasu;
- Działanie – obsługa oraz realizacja działań korygujących i zapobiegawczych doskonalących system zarządzania bezpieczeństwem informacji w przedsiębiorstwie.

Koncepcja systemu zarządzania bezpieczeństwem informacji opiera się o wymagania normatywne zawarte w PN-ISO/IEC 27001:2007 „Technika informatyczna –Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania" [3]. Określa ona przede wszystkim wymagania związane z ustanowieniem, wdrożeniem, funkcjonowaniem, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem systemu

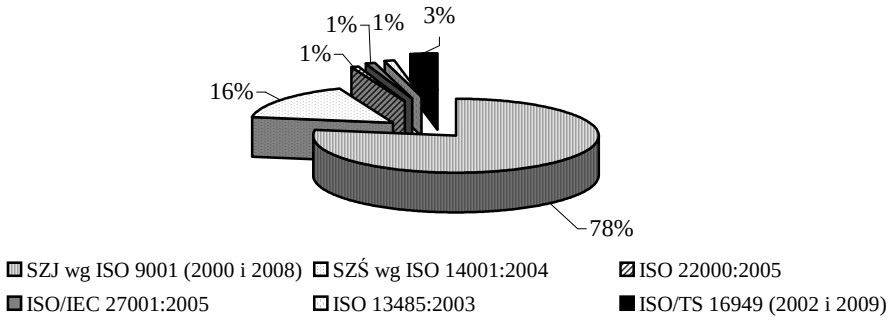
zarządzania bezpieczeństwem informacji. Norma PN-ISO/IEC 27001:2007 w kompleksowy sposób obejmuje więc wszystkie zagadnienia związane z zarządzaniem bezpieczeństwem informacji w przedsiębiorstwie, a zwłaszcza bezpieczeństwo fizyczne, osobowe, teleinformatyczne oraz prawne, czyli umożliwia budowę w przedsiębiorstwie zintegrowanego systemu zarządzania jakością w oparciu o normę ISO 9001 i bezpieczeństwem informacji [2]. Może znaleźć ona zastosowanie we wszystkich organizacjach, niezależnie od ich typu (biznesowe i publiczne), rozmiaru (małe, średnie i duże) i natury prowadzonej działalności (usługowa i produkcyjna). Norma ta stanowi podstawę do certyfikacji systemów zarządzania bezpieczeństwem informacji.

Wdrożenie w przedsiębiorstwie systemu zarządzania bezpieczeństwem informacji może więc przynieść następujące korzyści:

- pozwali określić wymagania przedsiębiorstwa w zakresie bezpieczeństwa,
- pozwoli położyć szczególny nacisk na ochronę informacji i jej znaczenie oraz wartość,
- pozwoli na wzrost świadomości pracowników co do bezpieczeństwa informacji,
- zwiększy zainteresowanie w firmie technologiami informatycznymi (ICT),
- spowoduje prowadzenie analizy i zarządzania ryzykiem, a w konsekwencji próbę minimalizacji ryzyka w odniesieniu do posiadanych lub przechowywanych w przedsiębiorstwie informacji,
- pozwoli na zastosowanie podejścia procesowego i ciągłego doskonalenia w zakresie bezpieczeństwa informacji,
- pozwoli na lepsze dostosowanie się do wymogów przetargowych,
- może pozwolić na podniesienie wydajności, płynności finansowej oraz rentowności przedsiębiorstwa,
- może stać się instrumentem pozwalającym na uzyskanie przewagi nad konkurencją
  i poprawy wizerunku firmy i jej wiarygodności w oczach klientów.

3. Certyfikacja systemów zarządzania bezpieczeństwem informacji w Europie i na świecie

Systemy zarządzania, oparte na normach ISO, od kilku lat cieszą się niesłabnącym zainteresowaniem wśród różnego rodzaju organizacji i przedsiębiorstw. Dzieje się tak głównie z powodu chęci standaryzacji realizowanych działań, czego konsekwencją jest niewątpliwie poprawa ich funkcjonowania. Dotyczy to przede wszystkim systemów zarządzania jakością, opartych na normie ISO 9001, systemów zarządzania bezpieczeństwem żywności (ISO 22000) oraz systemów zarządzania środowiskowego (ISO 14001). Niemniej jednak, również i wymagania normy dotyczącej bezpieczeństwa informacji (ISO/IEC 27001), coraz częściej podlegają certyfikacji (rys. 2).



Rys. 2. Najbardziej popularne systemy zarządzania podlegające certyfikacji – stan na dzień 31.12.2009 r.
Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009"

Zainteresowanie przedsiębiorstw wdrożeniem konkretnych systemów zarządzania, a następnie poddanie ich funkcjonowania certyfikacji, znajduje swoje odbicie w coraz większej liczbie wydanych certyfikatów, zarówno w Polsce, jak i na całym świecie. Jak już wspomniano, od kilku lat, stale wzrasta liczba systemów poddanych certyfikacji, co przedstawiono w tabelach 1-3.

Tab. 1. Liczba wydanych certyfikatów na świecie w odniesieniu do konkretnego systemu zarządzania – stan na dzień 31.12.2007

System zarządzania	Liczba krajów stosujących normę	Liczba wydanych certyfikatów
SZJ wg ISO 9001 (2000 i 2008)	175	951.486
SZŚ wg ISO 14001:2004	148	154.572
ISO 22000:2005	93	4.132
ISO/IEC 27001:2005	**70**	**7.732**
ISO 13485:2003	84	12.985
ISO/TS 16949 (2002 i 2009)	81	35.198

Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2008"

Tab.2. Liczba wydanych certyfikatów na świecie w odniesieniu do konkretnego systemu zarządzania – stan na dzień 31.12.2008

System zarządzania	Liczba krajów stosujących normę	Liczba wydanych certyfikatów
SZJ wg ISO 9001 (2000 i 2008)	176	982.832
SZŚ wg ISO 14001:2004	155	188.815
ISO 22000:2005	112	8.102
ISO/IEC 27001:2005	**82**	**9.246**

ISO 13485:2003	88	13.234
ISO/TS 16949 (2002 i 2009)	81	39.320

Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2008"

Tab. 3. Liczba wydanych certyfikatów na świecie w odniesieniu do konkretnego systemu zarządzania – stan na dzień 31.12.2009

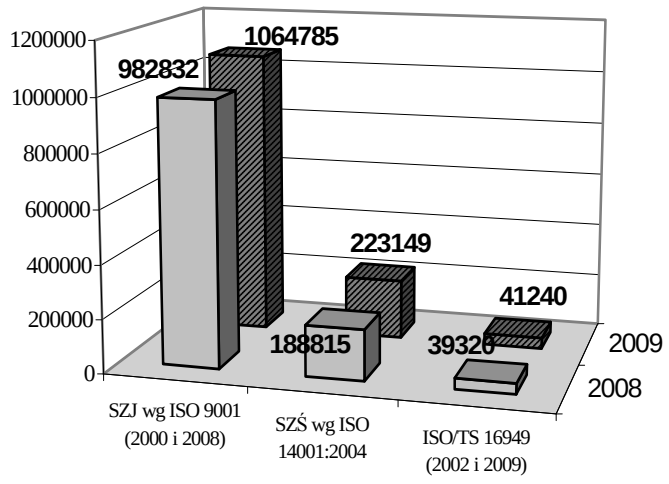
System zarządzania	Liczba krajów stosujących normę	Liczba wydanych certyfikatów
SZJ wg ISO 9001 (2000 i 2008)	178	1.064.785
SZŚ wg ISO 14001:2004	159	223.149
ISO 22000:2005	127	13.881
ISO/IEC 27001:2005	**117**	**12.934**
ISO 13485:2003	90	16.424
ISO/TS 16949 (2002 i 2009)	83	41.240

Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009"

Jak wynika z tabeli 3, na początek 2010 r. najwięcej wydano certyfikatów potwierdzających zgodność wdrożonych systemów zarządzania jakością z wymaganiami zawartymi w normie ISO 9001:2008, bowiem w 178 krajach odnotowano ich aż 1.064.785.

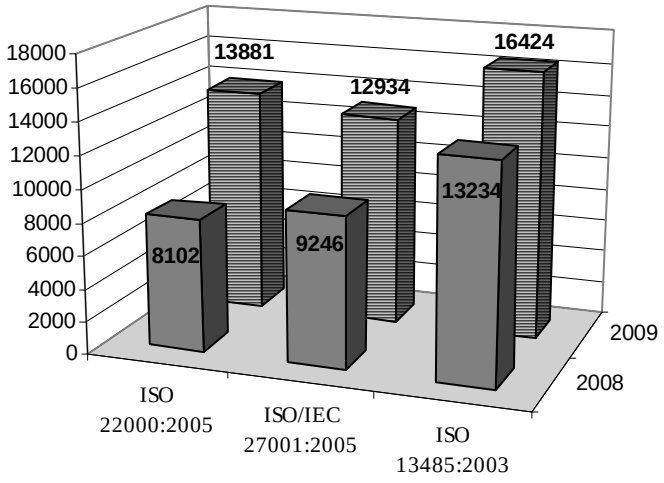
Jeśli chodzi o system zarządzania bezpieczeństwem informacji, spełniający wymagania zawarte w normie ISO/IEC 27001:2005, na dzień 1 stycznia 2010 r. zostało wydanych co najmniej 12.934 certyfikatów w 117 krajach stosujących ww. normę.

Dynamikę wzrostu liczby wydanych na świecie certyfikatów w odniesieniu do różnych systemów zarządzania w latach 2008-2009 przedstawiono na rys. 3 oraz 4.



Rys. 3. Dynamika wzrostu liczby wydanych certyfikatów na zgodność z normą ISO 9001, ISO 14001 i ISO/TS 16949

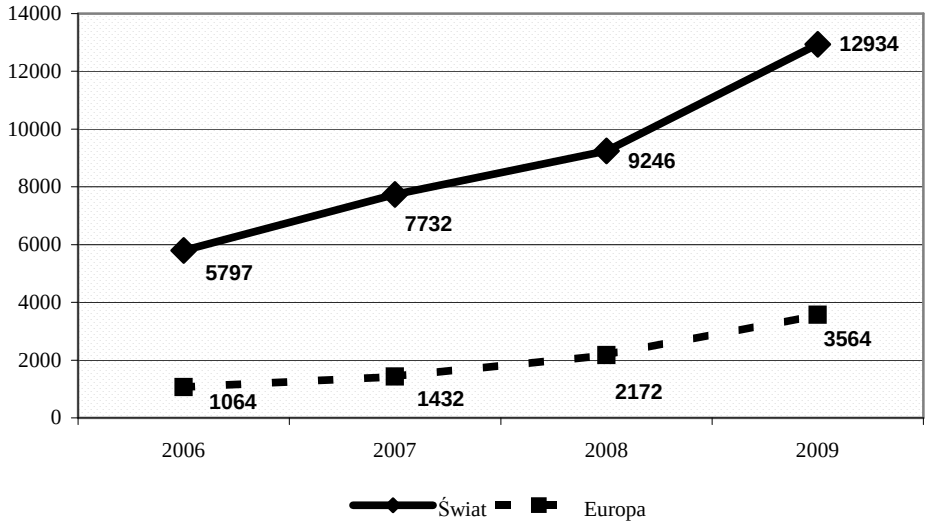
Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009"



Rys. 4. Dynamika wzrostu liczby wydanych certyfikatów na zgodność z normą ISO 22000, ISO 27001 i ISO 13485
Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009"

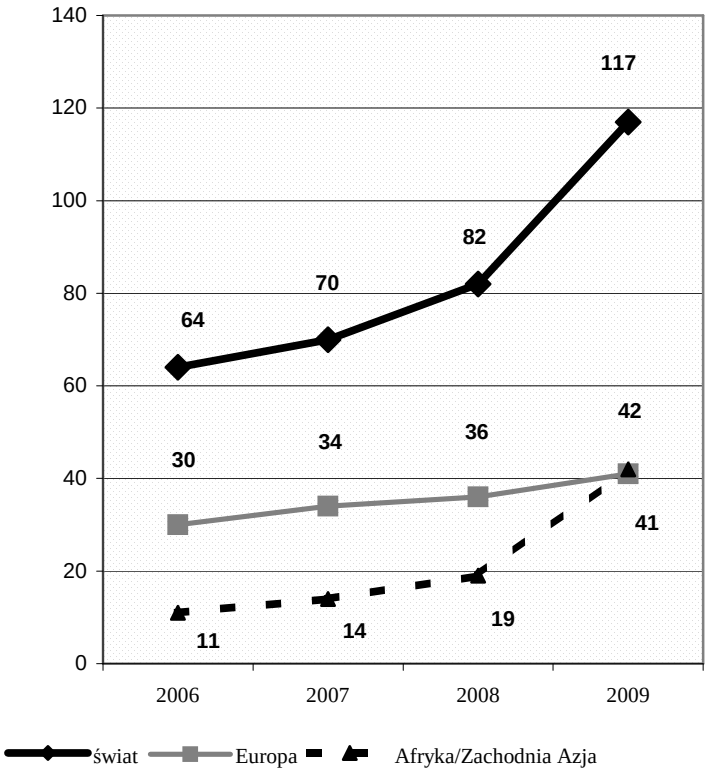
Z danych udostępnionych przez Międzynarodową Organizację Standaryzacji (ISO), przedstawionych na rys. 3 i 4, wynika, iż w 2009 roku, najbardziej widoczny wzrost w ilości wydanych certyfikatów, można było zaobserwować w odniesieniu do systemów zarządzania bezpieczeństwem żywności (ISO 22000). Liczba certyfikatów potwierdzających wdrożenie i funkcjonowanie ww. systemu w przedsiębiorstwach wzrosła bowiem aż o 69% (podczas, gdy do końca 2008 roku wydanych zostało 8.102 certyfikatów na zgodność z normą ISO 22000, to na początek 2010 istniało już aż 13.881 przedsiębiorstw posiadających stosowny certyfikat).

W odniesieniu do systemów zarządzania bezpieczeństwem informacji, wzrost liczby wydanych certyfikatów nie był aż tak spektakularny, jak to miało miejsce w przypadku systemów zarządzania bezpieczeństwem żywności, jednakże był on również znaczący – wskaźnik wzrostu wyniósł bowiem prawie 40% (wzrost z 9.246 certyfikatów na koniec 2008 do 12.934 – na koniec 2009 r.), podczas gdy w 2008 roku, w stosunku do 2007 r. wskaźnik ten wyniósł nieco ponad 20%. Te same informacje, a odnoszące się do krajów i gospodarek europejskich prezentowały się następująco: % wzrost w 2007 roku – 35%, w 2008 r. – 52% i w 2009 r. aż 64% (rys. 5).



Rys. 5. Dynamika wzrostu liczby wydanych certyfikatów na zgodność z normą ISO 27001 w latach 2006-2009 na świecie (ogółem) i w Europie
Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009"

Pomimo kryzysu finansowego, który rozpoczął się w 2007 roku i w latach 2008-2009 rozprzestrzenił się na większość krajów i sektorów w gospodarce światowej, odnotowano nie tylko wzrost liczby wydanych certyfikatów na świecie w odniesieniu do konkretnego systemu zarządzania, ale również liczbę krajów stosujących poszczególne normy. Aktywność w zakresie certyfikacji jednego lub więcej ISO-wskich standardów dotyczących systemów zarządzania w roku 2009 można było zaobserwować w 178 krajach (2008 r. – 176 krajów, 2007 r. – 175 krajów na świecie). Jeszcze wyraźniej widać to w odniesieniu do systemów zarządzania bezpieczeństwem informacji – co zostało zaprezentowane na rys. 6.



Rys. 6. Liczba krajów stosujących i certyfikujących normę ISO 27001
Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009"

Z rys. 6 wynika, iż w 2006 r. 64 kraje stosowały normę ISO 27001, podczas gdy na koniec 2009 odnotowano aż 117 gospodarek światowych, w których przedsiębiorstwa poddały certyfikacji funkcjonujące u nich systemy zarządzania bezpieczeństwem informacji (wzrost o blisko 83%). W Europie sytuacja nie przedstawia się już w tak spektakularny sposób, ale również widoczny jest permanentny wzrost krajów stosujących normę ISO 27001 (w 2006 r. – 30 krajów, w 2009 – 42 kraje; wzrost o 40%). Dla porównania na rys. 6 zaprezentowano również adekwatne dane odnoszące się do gospodarek i krajów w Afryce i Zachodniej Azji – i tak, podczas gdy w 2006 r. jedynie 11 krajów deklarowało stosowanie się do wymagań normy ISO 27001, to w 2009 – ich liczba wzrosła do 41 (prawie 3-krotny wzrost).

Powyższa sytuacja została skomentowana przez samą Międzynarodową Organizację Standaryzacji we wstępie do „The ISO Survey of Certifications", stwierdzając mianowicie, iż tak wysokie wskaźniki dynamiki wzrostu odnoszące się do ilości wydanych certyfikatów na świecie stanowią wyraźny dowód na to, że systemy zarządzania stały się niezbędnymi narzędziami gospodarki światowej i utrzymują swoją atrakcyjność dla organizacji nawet w okresie kryzysu [5].

Jak już wspomniano, od kilku lat można zaobserwować stały wzrost liczby przedsiębiorstw poddających funkcjonujące u nich systemy zarządzania bezpieczeństwem informacji certyfikacji, potwierdzającej zgodność z wymaganiami normy ISO 27001, zarówno biorąc pod uwagę gospodarki wszystkich krajów, jak i gospodarki europejskie. Podczas gdy w 2006 liczba certyfikatów dotyczących systemu zarządzania bezpieczeństwem informacji wydanych w Europie, w odniesieniu do ogólnej liczby wydanych certyfikatów na zgodność z normą ISO 27001, stanowiła jedynie 18,4% to już w 2008 udział ten wzrósł do 23,5%, by w 2009 osiągnąć wartość 27,6%.

W tabeli 4 zaprezentowano 10 krajów, w których na dzień 31.12.2009 r. odnotowano największą liczbę wydanych certyfikatów potwierdzających funkcjonowanie systemów zarządzania bezpieczeństwem informacji na zgodność z wymaganiami normy ISO 27001, natomiast w tabeli 5 – 10 krajów, w których odnotowano największy wzrost liczby wydanych certyfikatów odnoszących się do ww. normy.

Tab. 4. Kraje z największą liczbą wydanych certyfikatów na zgodność z normą ISO 27001 – stan na dzień 31.12.2009 r.

Lp.	**Nazwa kraju**	**Liczba wydanych certyfikatów**
1.	Japonia	5.508
2.	Indie	1.240
3.	Wielka Brytania	946
4.	Tajwan	934
5.	Hiszpania	483
6.	Chiny	459
7.	Rumunia	303
8.	Włochy	297
9.	Republika Czeska	264
10.	Niemcy	253

Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009”

Tab. 5. Kraje z największą dynamiką wzrostu liczby wydanych certyfikatów na zgodność z normą ISO 27001 – stan na dzień 31.12.2009 r.

	Nazwa kraju	**Wzrost liczby wydanych certyfikatów w 2009 r.**
1.	Japonia	1.083
2.	Indie	427
3.	Hiszpania	280
4.	Rumunia	259
5.	Tajwan	232
6.	Chiny	223
7.	Wielka Brytania	208
8.	Republika Czeska	176
9.	**Polska**	**112**
10.	Stany Zjednoczone	84

Źródło: opracowanie własne na podstawie „The ISO Survey of Certifications-2009”

4. Certyfikacja systemów zarządzania bezpieczeństwem informacji w Polsce

Jak już wspomniano, coraz więcej przedsiębiorstw decyduje się na poddanie wdrożonego i funkcjonującego u siebie systemu zarządzania: jakością, bezpieczeństwem żywności, czy też bezpieczeństwem informacji (lub innych), procesowi dobrowolnej certyfikacji przez akredytowaną jednostkę certyfikującą (wydana w połowie lutego 2007 ISO/IEC 27006 „Requirements for bodies providing audit and certification of information security management systems" czyli „Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji" określa wymagania, jakie muszą spełniać jednostki przeprowadzające audyty certyfikacyjne systemów zarządzania bezpieczeństwem informacji) [4]. Dzieje się tak również w Polsce, co znajduje swoje odbicie w różnego rodzaju statystykach.

Po roku 2007 pozycja Polski w zakresie certyfikacji systemów zarządzania, na tle gospodarek światowych i europejskich, dynamicznie wzrasta. Do 2007 roku, jeśli chodzi o ilość wydanych certyfikatów, Polska była, w rankingu ISO, klasyfikowana poza światową dziesiątką. Według opublikowanej 25 października 2010 roku przez Międzynarodową Organizację Normalizacyjną wspomnianej wcześniej ankiety *The ISO Survey of Certifications* [5] Polska została już sklasyfikowana w pierwszej dziesiątce świata na 8 miejscu wśród państw o największym wzroście standardu ISO 9001. W Polsce bowiem, na dzień 1 stycznia 2010 r., 12.707 organizacji posiadało certyfikowany system zarządzania jakością, spełniających wymagania wyspecyfikowane w normie ISO 9001, co oznacza prawie 16% przyrost ilości wydanych certyfikatów w porównaniu do roku poprzedniego.

Jeśli chodzi o standard ISO 22000 – tutaj nasz kraj może pochwalić się najlepszą pozycją w rankingu ogólnoświatowym, bowiem już po raz drugi został sklasyfikowany na 7 miejscu na świecie. Wskazuje to, jak się wydaje, na wysoką dbałość o poziom bezpieczeństwa naszej żywności.

W Polsce system zarządzania bezpieczeństwem informacji cieszy się również w ostatnich latach coraz większym uznaniem. Coraz więcej przedsiębiorstw w Polsce dostrzega konieczność ochrony posiadanych informacji. Osiągnięcie i utrzymanie właściwego poziomu bezpieczeństwa w dzisiejszych czasach, w których nowe zagrożenia pojawiają się praktycznie każdego dnia, nie jest bowiem zadaniem prostym. Niejednokrotnie dochodzi także do zdarzeń niespodziewanych, nieprzewidywalnych które utrudniają lub wręcz uniemożliwiają kontynuację procesów biznesowych. Stąd też polskie firmy coraz częściej decydują się na wdrożenie systemu ISO/IEC 27001.

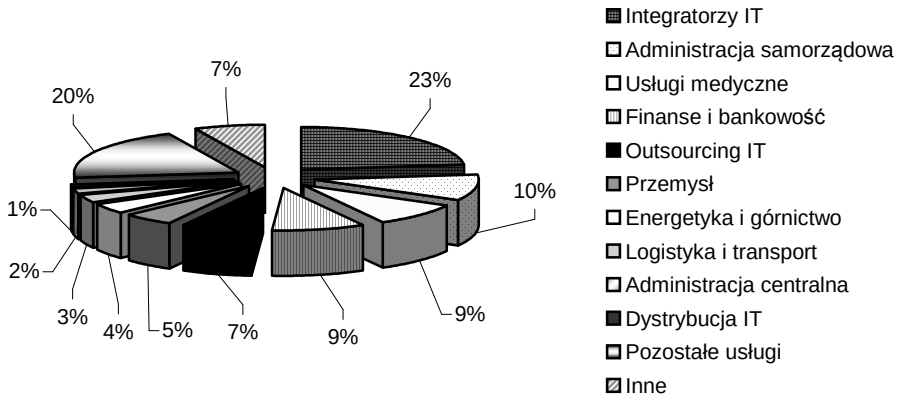
Pierwszy, zakończony sukcesem i potwierdzony certyfikatem audit systemu ISMS, przeszła firma Inforsys Sp. z o.o., ekspert usług outsourcingowych z zakresu masowego przetwarzania dokumentów. Drugi certyfikat, ale pierwszy dla urzędu przyznano Urzędowi Miasta Piotrków Trybunalski, a pierwszym bankiem, który uzyskał certyfikat ISO 27001, jest bank PKO BP [1]. Z kolei w ostatnich miesiącach przyznano co najmniej 3 kolejne certyfikaty: Transition Technologies S.A. (02.09.2011), Biatel BIT S.A. (15.09.2011) oraz Advicom Sp. z o.o. (21.11.2011) – wszystkie firmy z branży IT [7].

Brak jest kompletnych i wiarygodnych danych dotyczących ilości certyfikatów wydanych w Polsce na zgodność z wymaganiami normy ISO 27001. Niektóre źródła mówią o 172 wydanych certyfikatach na koniec grudnia 2011 r. [7] – przytoczony rejestr został przygotowany w oparciu o wiedzę grona specjalistów oraz publicznie dostępne materiały.

Bez względu jednak na niemożność podania konkretnej i dokładnej liczby wydanych w Polsce certyfikatów na zgodność z wymaganiami zawartymi w standardzie ISO/IEC

2700, można powiedzieć, że charakteryzuje się ona tendencją wzrostową, o czym może świadczyć fakt, iż w 2009 r. Polska w rankingu ISO zajęła 9 miejsce (co przedstawiono w tabeli 5), podczas gdy w roku 2008 w ogóle nie była sklasyfikowana w światowej czołówce. W odniesieniu do standardu ISO/IEC 27001 w Polsce nastąpił więc wzrost certyfikacji blisko 2,5 krotny.

Dynamika wzrostu liczby organizacji, które zdobywają powyższe certyfikaty oznacza, że polskie firmy i urzędy mają coraz większą świadomość konieczności ochrony przetwarzanych informacji i sięgają po sprawdzone narzędzia umożliwiające wdrożenie skutecznych zabezpieczeń. Wśród tych organizacji są głównie firmy usługowe oraz zajmujące się nowymi technologiami (głównie informatyczne), które stanowią około 80% wszystkich certyfikowanych firm w Polsce. Strukturę organizacji posiadających certyfikat w odniesieniu do standardu ISO/IEC 27001 wg branż zaprezentowano na rys. 7.



Rys. 7. Organizacje posiadające certyfikowany system zarządzania bezpieczeństwem informacji w Polsce – podział wg branż
Źródło: opracowanie własne na podstawie www.iso27000.pl

Niektórzy eksperci oceniają, że wzrost dynamiki przyrostu procesów certyfikacji wynika z rosnących wymagań biznesowych, prawnych oraz technologicznych. Duży przyrost projektów obejmujących wdrożenie ISO/IEC 27001 obserwuje się także w sektorze administracyjnym, który aktualnie podlega gruntownej modernizacji informatycznej i kultury pracy opartej na technologiach internetowych [www.iso27000.pl].

W najbliższym czasie można spodziewać się dalszych wzrostów liczby certyfikatów ISO/IEC 27001 (systemów zarządzania bezpieczeństwa informacji). Przedsiębiorstwa, a zwłaszcza firmy informatyczne, banki czy urzędy miejskie nie mogą sobie pozwolić na utratę zaufania klientów. To głównie one, jak już wspomniano, są zainteresowane standardami zapewniającymi bezpieczeństwo informacji.

5. Podsumowanie i wnioski

Podsumowując należy stwierdzić, iż informatyzacja w połączeniu z koniecznością przekazywania oraz udostępniania coraz większych ilości danych i informacji wymusi na wielu firmach i organizacjach konieczność nadzorowania bezpieczeństwa informacji. Obecnie trudno jest prognozować, w których sektorach biznesu szerokie zastosowanie znajdzie system zarządzania bezpieczeństwem informacji wdrażany w oparciu o PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania [3]. Można przypuszczać, iż analogicznie, jak dla systemu zarządzania bezpieczeństwem żywności w branży spożywczej, tak i dla systemu zrządzania bezpieczeństwem informacji powstaną doprecyzowane wymagania dla specyficznych sektorów, np. sektora bankowego. Rozwój systemu zarządzania bezpieczeństwem informacji polegający na systematycznym i logicznym podejściu do problemów bezpieczeństwa informacji, w odróżnieniu od wyrywkowego podejścia do naruszeń bezpieczeństwa, został bowiem już zapoczątkowany i rozwija się dynamicznie.

Literatura

1. Bielawa A., System Zarządzania Bezpieczeństwem Informacji według normy ISO/IEC 27001:2005, Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania Nr 1, Wyd. Naukowe Uniwersytetu Szczecińskiego, Szczecin 2008, s. 171-176.
2. Maćkowiak K., Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO/IEC 27001:2005, Boston IT Security Review 4/2007.
3. PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania.
4. PN-ISO/IEC 27006:2009 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.
5. The ISO Survey of Certifications-2009, Geneva 2010.
6. Wrzesiński P., Zarządzanie bezpieczeństwem informacji, Boston IT Security Review 1/2007.
7. www.iso27000.pl.

Dr Monika STOMA
Zakład Logistyki i Zarządzania Przedsiębiorstwem
Katedra Energetyki i Pojazdów
Wydział Inżynierii Produkcji
Uniwersytet Przyrodniczy w Lublinie
20-950 Lublin, ul. Akademicka 13
tel./fax.: (0-81) 531-83-15
e-mail: monika.stoma@up.lublin.pl