S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 1 ss. 85–112 ROK 2016

ISSN 2543–7321

Marcin Olkiewicz

Politechnika Koszalińska
Koszalin
marcin.olkiewicz@tu.koszalin.pl

SYSTEM ZARZĄDZANIA DETERMINANTĄ BEZPIECZEŃSTWA INFORMACJI W DZIAŁALNOŚCI GOSPODARCZEJ

MANAGEMENT SYSTEM AS A DETERMINANT OF INFORMATION SECURITY MANAGEMENT IN BUSINESS

***Zarys treści*:** Bezpieczeństwo informacji stanowi coraz większe wyzwanie dla przedsiębiorców, gdyż rynkowe zapotrzebowanie na informacje o odpowiedniej jakości jest bardzo duże i ciągle wzrasta. Rosnąca świadomość możliwości utraty informacji niejawnych wymusza na organizacjach podejmowanie często radykalnych działań mających zagwarantować bezpieczeństwo lub zminimalizować ryzyko. Dlatego coraz częściej do sektorów ochrony informacji kwalifikuje się między innymi następujące obszary: danych osobowych, fizycznego i przemysłowego bezpieczeństwa (procesy tworzenia, grupowania, przechowywania i dystrybuowania informacji), teleinformatyczne (obejmujące systemy informatyczne, narzędzia zabezpieczające, przedmioty rejestrujące) oraz logistyczne. Praca skupia się na identyfikacji procesowego zarządzania bezpieczeństwem informacji według znormalizowanych systemów zarządzania stosowanych w organizacjach lub instytucjach różnych branż oraz obszarów funkcjonowania gospodarki. Działania takie są szczególnie istotne dla zwiększania przewagi konkurencyjnej oraz zapewnienia bezpieczeństwa kraju. Wykorzystywanie międzynarodowych znormalizowanych standardów, między innymi takich jak ISO 9001, ISO 27001, PN-ISO/IEC 24762:2010, AQAP, przestrzeganych w 176 krajach na świecie, daje poczucie gwarancji i bezpieczeństwa klientom, społeczeństwu, interesariuszom rynku oraz pozwala zapewnić stabilny i zrównoważony rozwój.

***Słowa kluczowe*:** sklasyfikowane informacje, rola informacji, bezpieczeństwo, jakość systemu zarządzania, aktywność ekonomiczna

***Key words*:** classified information, the role of information, security, quality management system, economic activity

1. Wprowadzenie

Rozwój gospodarki światowej wraz ze zwiększeniem świadomości, potrzeb oraz oczekiwań klientów spowodowały uwydatnienie ważności informacji. Treść informacji, a także jej cechy, w szczególności rzetelność, przydatność, aktualność, są dobrem konsumpcyjnym, o które zabiega wiele firm. W praktyce uważa się takie zjawisko za naturalne, oparte na zasadach czystej konkurencji, tj. im bardziej wartościowa (przydatna) informacja – tym wyższa jej cena. Takie przekonanie potwierdza się z punktu widzenia ekonomicznego i prawnego, gdzie informacja jest towarem, którego wartość rynkowa wynika z zawartych w nim treści (danych). W tym znaczeniu oznacza ona towary (dobra informacyjne) lub usługi (informacyjne) niezbędne w gospodarce, polityce, kulturze, życiu codziennym[1]. Oznacza to, że pewien zasób informacji, najczęściej rynkowo-gospodarczych, można kupić oraz odpowiednio wykorzystać w walce konkurencyjnej, zwiększając swoją pozycję rynkową. Jest to więc pewnego rodzaju strategiczny produkt, regulujący różne mechanizmy społeczno-gospodarcze. Należy pamiętać, że na rynku występuje niezliczona ilość informacji, które są pozyskiwane w różny sposób (czasami niezgodnie z obowiązującym prawem), a następnie udostępniane lub oferowane do nabycia. Jednocześnie z punktu widzenia skutku, jaki może wywołać informacja, istotny staje się podział informacji na jawną[2] (udostępnianą wszystkim zainteresowanym) i niejawną (udostępnianą nielicznym podmiotom).

Determinuje to konieczność odpowiedniego zabezpieczania oraz zarządzania informacją jawną, a w szczególności niejawną. Każda informacja, podobnie jak inne dobro (produkt), podlega procesowi tworzenia oraz przetwarzania, uzyskując ostateczny wymiar, co powoduje, że występują różnego rodzaju zagrożenia mogące zmniejszyć jej wartość oraz jakość. W tym celu należy zaopatrzyć się w odpowiednie narzędzia ochrony informacji, do których zaliczyć można między innymi system zarządzania bezpieczeństwem informacji.

Poniższe opracowanie dotyczyć będzie identyfikacji możliwości zabezpieczania, ochrony informacji niejawnej poprzez celowe systemowe zarządzanie. Świadomość możliwości utraty informacji oraz jej wykorzystania przez inne podmioty zwiększa konieczność stosowania odpowiednich obostrzeń, narzędzi zabezpieczających, ograniczających ryzyko wystąpienia takich sytuacji i narażenia podmiotu na utratę potencjalnych korzyści lub ponoszenia dodatkowych kosztów.

2. Informacja niejawna w działalności gospodarczej

Informację, wedle definicji interdyscyplinarnej, trudno jednoznacznie zinterpretować[3], uznawana jest za zbiór danych (właściwości) przedstawionych w taki spo-

---

[1] M. Chyliński, *Informacja i zarządzanie informacją w działalności samorządowej*, „Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie" 2014, nr 69, s. 121.

[2] Z. Malara, *Przedsiębiorstwo w globalnej gospodarce: wyzwania współczesności*, Warszawa 2006, s. 127.

[3] W. Flakiewicz, *Pojęcie informacji w technologii multimedialnej*, Warszawa 2005; G. Harmon, *The measurement of information*, „Information Processing and Management" 1984, no. 1–2; E. Kałuszyńska,

sób, że ma znaczenie i kreuje pewną wartość, a także za niezbędne źródło wiedzy wykorzystywanej w codziennym życiu. Informacja stanowi zatem wiedzę potrzebną do określania i realizacji zadań służących osiąganiu celów organizacji[4]. Przydatność informacji uwarunkowana jest od jej jakości, parametru określającego cechy[5] informacji, do których zalicza się: aktualność, kompletność i spójność, rzetelność (wiarygodność), dostępność, porównywalność oraz dokładność. Coraz częściej dodatkowym parametrem jakości uznawana jest kosztowność, tzn. jak wysokie trzeba ponieść koszty, aby otrzymać pożądaną informację. Prawidłowe funkcjonowanie i zarządzanie organizacją, zasobem ludzkim, krajem, uzależnione jest od jakości informacji.

Do głównych atrybutów jakości informacji należy zaliczyć[6]:

- relewancję (*relevance*) – jest to kluczowy komponent oceny jakości informacji. Istotne jest tu pytanie, czy dostarczona informacja odpowiada na zapotrzebowanie odbiorcy (nabywcy). Jeśli tak nie jest, to odbiorca oceni informację jako nieadekwatną, niezależnie od posiadania przez informację pozostałych atrybutów;
- dokładność (*accuracy*) – atrybut ten uznaje się za oczywisty, a w praktyce informacja używana w różnych celach wymagać będzie różnych stopni dokładności. Jest też możliwe, że informacja będzie zbyt dokładna, zbyt precyzyjna i będzie przekraczać zdolności pojmowania odbiorcy;
- aktualność (*timeliness*) – atrybut ten jest w oczywisty sposób zmienny. Zależy on nie tylko od tempa powstawania nowych informacji, które wypierają informacje dostępne dotychczas, ale także od szybkości przetwarzania nowych informacji i dostarczania ich do odbiorcy (nabywcy);
- kompletność (*completeness*) – niekompletna informacja może być dla odbiorcy myląca, a stopień kompletności informacji jest również zrelatywizowany do jej nabywcy. Podobnie jak jest w przypadku zbyt dużej dokładności informacji, także nadmierna kompletność może przekraczać zdolności pojmowania odbiorcy;
- koherencja (*coherence*) – atrybut koherencji polega na tym, jak dobrze poszczególne informacje wspierają się wzajemnie i są ze sobą spójne. Niekoherencja może być spowodowana występowaniem elementów nierelewantnych, mylących lub formalnie niejednoznacznych, co może powodować odrzucenie informacji przez odbiorcę. Chociaż informacja może być autentycznie niekoherentna, to niekoherencja zwykle wskazuje na błędy w dokładności lub aktualności;
- odpowiedniość formatu (*format*) – problem dotyczy sposobu prezentacji informacji jej nabywcy. Dwoma czynnikami odpowiedniości formatu są forma prezentacji i kontekst interpretacji. Odpowiedniość formatu jest także zależna od odbiorcy i sposobu użycia informacji;

Wiedza i informacja, [w:] *Informacja a rozumienie*, red. M. Heller, J. Mączka, Warszawa 2005; J. Gleick, *Informacja*, Kraków 2012.

[4] B. Nogalski, B.M. Surawski, *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, [w:] *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona. Wybrane problemy teorii i praktyki*, red. R. Borowiecki, M. Kwieciński, Kraków 2003, s. 205.

[5] R.W. Griffin, *Podstawy zarządzania organizacjami*, Warszawa 2004, s. 725–726.

[6] J. Boruszewski, *Jakość i wiarygodność informacji w infobrokerstwie*, „Lingua ac Communitas" 2012, vol. 22, s. 244–245.

- dostępność (*accessibility*) – informacja powinna być dostępna dla odbiorcy zawsze, gdy zaistnieje taka potrzeba. Dostępność jest atrybutem komplementarnym względem aktualności. Niedostępna informacja aktualna lub dostępna informacja, która straciła na aktualności, nie spełnia potrzeb informacyjnych odbiorcy (nabywcy);
- kompatybilność (*compatibility*) – jakość informacji nie zależy tylko od jakości tej informacji samej w sobie, lecz także od tego, jak może być ona powiązana z innymi informacjami i jako taka dostarczona do odbiorcy;
- bezpieczeństwo (*security*) – atrybut ten ma dwa aspekty: ochronę informacji przed dostępem dla niepowołanych osób oraz ochronę informacji przed naturalnymi katastrofami. Informacja, która nie jest odpowiednio chroniona, może nie budzić zaufania i jej potencjał może nie być w pełni wykorzystany;
- ważność, wiarygodność (*validity*) – informacja jest ważna, jeśli może być zweryfikowana jako prawdziwa i spełnia odpowiednie standardy odnoszące się do dokładności, aktualności, kompletności i bezpieczeństwa.

Każdy podmiot gospodarczy dąży do uzyskania informacji o istotnej jakości. Wykorzystanie informacji o niskiej jakości, a także informacji niejawnej w niepożądany sposób może mieć wpływ na destabilizację podmiotów gospodarczych. Dlatego zapewnienie najwyższej jakości informacji ma znaczący wpływ na efektywny i skuteczny proces decyzyjny, ograniczający lub minimalizujący istnienie ryzyka[7], a także ochronę przed tworzeniem propagandy, plotek oraz nieracjonalnych działań. Plotki, pogłoski, a nawet pomówienia są efektem pracowniczej dezinformacji lub braku pełnej wiedzy (informacji) na określony temat w organizacji. Jest to częste zjawisko, które dotyczy przede wszystkim zasobów ludzkich oraz finansów. W przypadku niejasnego przepływu informacji lub jej braku obawy pracowników narastają, dlatego konieczne jest sformalizowanie postępowania przekazu informacji oraz dostępności. Szczególnie przy informacjach niejawnych brak jasnego sposobu postępowania może spowodować poważne konsekwencje dla pracownika bezpośrednio związanego z dostępem do informacji i samej organizacji.

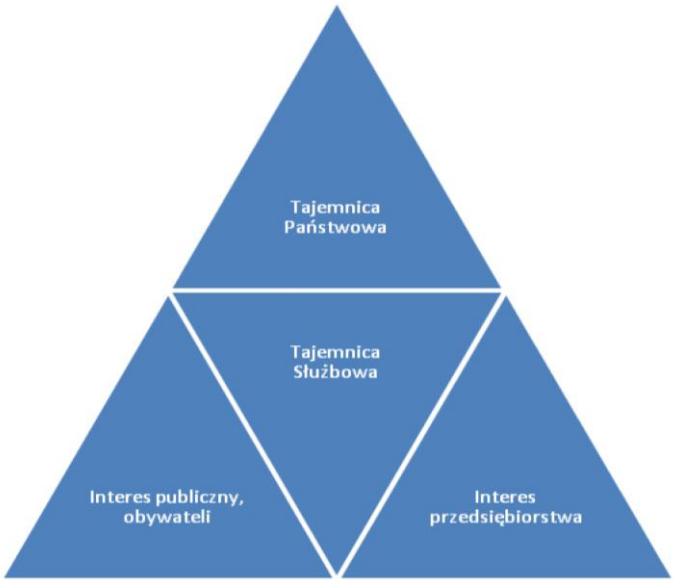
Na potrzeby niniejszego opracowania przyjmuje się definicję informacji niejawnej jako zbiór danych, które poprzez udostępnienie osobom nieuprawnionym spowodują lub mogą spowodować szkody bezpośrednie lub pośrednie dla kraju, organizacji lub osoby. Ustawa o ochronie informacji niejawnych[8] określa przedmiot ochrony informacji niejawnych jako tajemnicę państwową i tajemnicę służbową, tworząc pewnego rodzaju hierarchię informacji niejawnych (ryc. 1). Tajemnica państwowa stanowi informację niejawną, której niepowołane ujawnienie może spowodować zagrożenie dla kraju lub jego interesów albo wyrządzić znaczącą szkodę. Natomiast tajemnica służbowa dotyczyć będzie pozostałych informacji niejawnych mogących negatywnie oddziaływać na akcjonariuszy rynku, tj. interes publiczny, w tym także obywateli oraz podmioty gospodarcze.

Ustawa także precyzuje rodzaje informacji niejawnych objętych tajemnicą państwową (załącznik 1 ustawy) oraz podział na „ściśle tajne", „tajne" oraz „zastrzeżo-

[7] K. Szczepańska, *Metody i techniki TQM*, Warszawa 2009, s. 58–59.
[8] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228).

ne" i „poufne". Każda klauzula określa wymagania i zalecenia do sposobów postępowania nie tylko w sferze zabezpieczeń informacji niejawnych, ale także z zakresie podmiotów przetwarzających (jednostek organizacyjnych, tajnych kancelarii itp.) informacje, sposobów przekazywania, dopuszczania, monitorowania, archiwizowania itd. Za informację niejawną, z punktu widzenia tajemnicy służbowej stanowiącej interes akcjonariuszy rynku, możemy uznać każdą informację, która nieuprawnienie ujawniona staje się „dobrem handlowym" w zakresie tajemnicy przedsiębiorcy lub przedsiębiorstwa.

Do głównych grup takich informacji zaliczyć należy między innymi: dane osobowe, informacje handlowe, techniczno-technologiczne, bankowe, skarbowe, sądowe itd. Innymi słowy, dotyczące prowadzonych działalności gospodarczych lub państwowych.



Ryc. 1. Hierarchia ochrony informacji niejawnej
Fig. 1. The hierarchy of protection of classified information

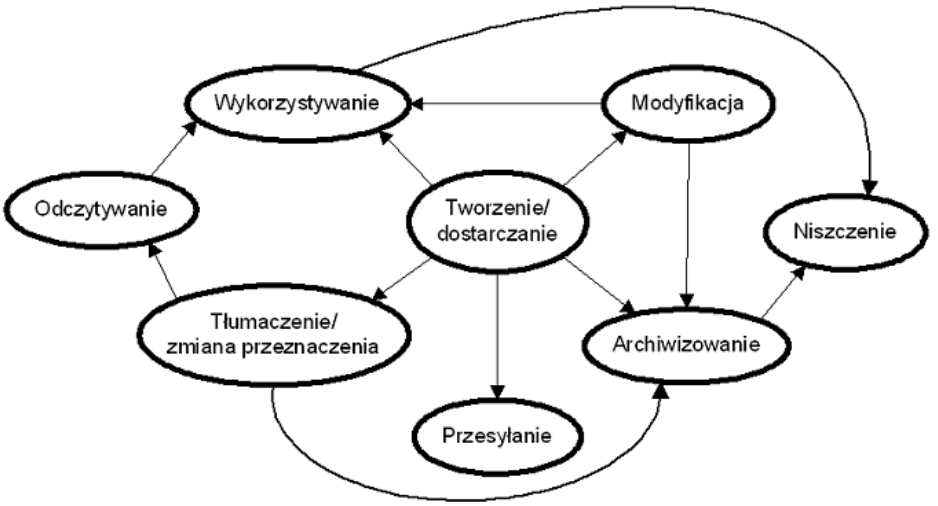
Źródło: opracowanie własne na podstawie: B. Iwaszko, *Ochrona informacji niejawnych w praktyce*, Wrocław 2012, s. 11–32.

3. Procesowe zarządzanie informacją niejawną w organizacji

Współczesne organizacje funkcjonują w ramach procesowego zarządzania. Wynika to z podejmowania ciągłych działań prorozwojowych, ukierunkowanych na jakość, mających na celu zwiększenie konkurencyjności oraz skuteczności organizacji, popartych analizą danych rynkowych[9].

[9] J. Majchrzak-Lepczyk, *Safety in the context of logistics and marketing support*, [w:] *Bezpieczeństwo w procesach globalizacji – dziś i jutro*, t. 1, red. Z. Grzywna, Katowice 2013, s. 387–397.

Działania analityczne związane z procesem identyfikacji oraz oceną zagrożeń w obszarze informacji występujące w organizacji i jej otoczeniu wymuszają jednocześnie wdrożenie odpowiednich czynności ograniczających i eliminujących takie zjawiska. Zagrożenia informacyjne mogą się pojawiać, gdyż transformacja informacji, tzn. cyklu jej życia, jest złożona, co prezentuje rycina 2.



Ryc. 2. Procesy przetwarzania informacji
Fig. 2. Information processing

Źródło: A. Adamczyk, R. Renk, J. Radziulis, W. Hołubowicz, *Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania*, „ORACLE'owe PLOUG'tki" 2005, nr 36, s. 160.

Celem działań w zakresie eliminacji (ochrony i zapewnienia bezpieczeństwa informacji) pojawiających się zagrożeń w przedsiębiorstwie jest osiągnięcie poziomu organizacyjnego oraz technicznego, który umożliwi m.in.:

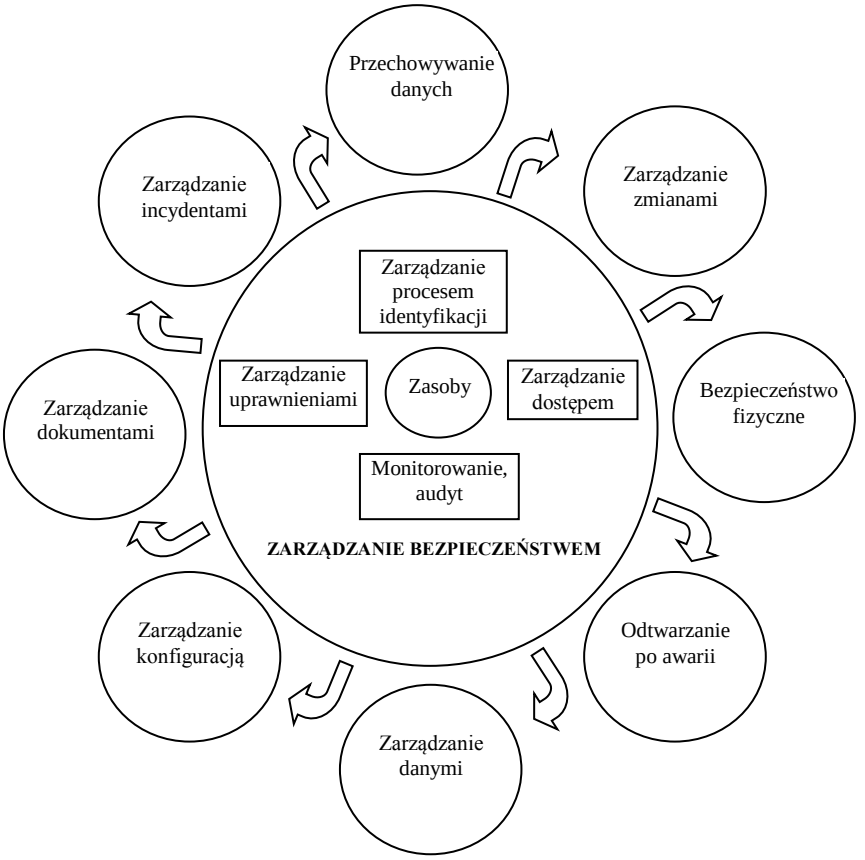
- zachowanie poufności informacji chronionych,
- integralność informacji chronionych i jawnych oraz dostępność do nich,
- osiągnięcie wymaganego poziomu bezpieczeństwa przetwarzanych informacji,
- maksymalne ograniczenie występowania zagrożeń bezpieczeństwa informacji,
- poprawne oraz bezpieczne funkcjonowanie systemów przetwarzania informacji,
- gotowość do podejmowania działań w sytuacjach kryzysowych[10].

Wzrost znaczenia informacji niejawnych wynikających z interesów różnych podmiotów, tj. państwa, instytucji wojskowych, samorządowych, podmiotów gospodarczych oraz publicznego zaufania, spowodował konieczność zastosowania (opracowania oraz wdrożenia) mechanizmów regulujących między innymi: sposoby rejestracji,

[10] M. Kowalewski, A. Ołtarzewska, *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego*, „Telekomunikacja i Techniki Informacyjne" 2007, nr 3–4, s. 4.

zabezpieczania, przechowywania, przekazywania oraz dostępu do tego typu informacji.

Początkowym etapem regulującym postępowanie z takimi informacjami był kodeks karny. Należy jednak stwierdzić, że to działanie dało tylko narzędzie, które nie było do końca doskonałe. Dlatego wraz z rozwojem świadomości oraz konieczności poszerzania obszarów zabezpieczenia zaczęto podejmować działania dążące do stworzenia takich narzędzi, które pozwolą wypracować odpowiednie mechanizmy nadzoru, funkcjonujące w sposób ciągły (ryc. 3), z możliwością ich procesowego doskonalenia. Takie określenie sposobu postępowania (procesowe działanie) nosi synonim zarządzania ukierunkowanego na jakość, tj. jakość informacji niejawnej.



Ryc. 3. Procesowe zapewnienie bezpieczeństwa informacji
Fig. 3. Process to provide information security

Źródło: A. Adamczyk, R. Renk, J. Radziulis, W. Hołubowicz, *Klasyfikacja informacji i danych*…, s. 161.

Efektem takiego podejścia do zarządzania informacją są sposoby postępowania jasno określone przez okólniki, instrukcje, zarządzenia, spójne również z ustawą

o ochronie informacji niejawnych[11]. Z punktu widzenia procesu zarządzania informacją niejawną ustawa wskazuje sposoby klasyfikowania, organizowania ochrony wraz z dostępem, przetwarzania, monitoringu stanu zabezpieczenia, ochrony w systemach teleinformatycznych, fizycznego zabezpieczenia oraz ochrony. Ponadto wymusza na podmiotach określony sposób postępowania, a w niektórych przypadkach bezpieczeństwo przemysłowe, gwarantujące bezpieczeństwo informacji, a także osoby odpowiedzialne za nadzorowanie prowadzonych działań. Aby sprawnie nadzorować (monitorować) działania bezpieczeństwa i rozwoju oraz kierować nimi, organizacje wspomagają się systemami zarządzania spełniającymi krajowe, a także często międzynarodowe standardy.

4. Systemy zarządzania kształtujące bezpieczeństwo informacji

Współczesne podejście do zarządzania opiera się na wysokiej jakości: systemach informatycznych (źródła pozyskiwania informacji), procesach działania poszczególnych komórek struktury organizacyjno-funkcjonalnej (stadium tworzenia i przetwarzania informacji), a także planach działania od strategicznych do operacyjnych (ukierunkowanie zasobów informacyjnych).

Odpowiednia strategia ukierunkowana na bezpieczeństwo ma na celu zapewnienie spokoju (m.in. funkcjonowania, bytu, podejmowania i realizowania działalności, w tym także gospodarczych) lub stworzenie bezpiecznych warunków, zaufania gwarantującego możliwość prawidłowej pracy oraz rozwoju. Organizacje, aby osiągnąć ten stan, ponoszą koszty związane z dostosowaniem się do takiego „komfortowego funkcjonowania" opartego na zarządzaniu informacją (wiedzą), gdyż zdają sobie sprawę z zagrożeń zwiększających ryzyko porażki[12].

W takim rozumieniu ukierunkowanego zarządzania należy przyjąć, że punktem wejścia jest informacja, a wyjścia – bezpieczna informacja. Cały proces przeobrażania obarczony jest ryzykiem możliwości spowodowania szkody[13], dlatego w ramach odpowiedniego zarządzania organizacje wspomagają się formalnymi lub nieformalnymi systemami zarządzania ukierunkowanymi na jakość.

Sformalizowania określonych sposobów postępowania, zwanych inaczej standaryzacją[14], zaczęto na dużą skalę dokonywać od 2000 roku. Wówczas zaczęły powstawać projakościowe systemy zarządzania opracowywane przez Międzynarodową Organizację Normalizacyjną (ISO – International Standard Organization), które stały się federacją krajowych organizacji normalizacyjnych o zasięgu światowym. Istnieją również niesformalizowane (niepodlegające certyfikacji) systemy zarządzania, wspie-

---

[11] Ustawa z dnia 5 sierpnia 2010 r.…

[12] A. Kister, *Użyteczność informacyjna rachunku kosztów innowacji*, [w:] *Kreatywność i przedsiębiorczość w projakościowym myśleniu i działaniu*, t. I, red. E. Skrzypek, Lublin 2009, s. 13–20.

[13] Najczęściej rozróżnia się szkody w kategoriach: **zamierzone** jako zaplanowane z premedytacją, **losowe wewnętrzne** niezamierzone, spowodowane przez pracowników poprzez zaniedbania, błędy itp. oraz **losowe zewnętrzne** wynikające z otaczającego środowiska naturalnego, w tym także klęski żywiołowe.

[14] Szerzej: M. Olkiewicz, *Podstawy zarządzania jakością. Wybrane aspekty*, Koszalin 2008.

rające również działania projakościowe, które są często uważane za koncepcje lub filozofie, np. TQM (*Total Quality Management* – Kompleksowe Zarządzanie Jakością).

4.1. Koncepcja systemowego zarządzania jakością

W nowoczesnej gospodarce coraz bardziej wyłania się konieczność kompleksowego podejścia do zarządzania informacją wynikająca między innymi z potrzeby posiadania informacji o określonej jakości. Jest to istotne, gdyż w otoczeniu gospodarczym istnieje ogromna ilość danych, różnych sposobów zdobywania i rozpowszechniania informacji, i innych elementów zwiększających niebezpieczeństwo utraty lub przetwarzania informacji niejawnych.

Przedsiębiorstwa nastawione projakościowo na odpowiednie zarządzanie informacją, a w szczególności zapewnienie bezpieczeństwa informacji, mogą zastosować system oparty na koncepcji TQM[15]. Koncepcja TQM skoncentrowana wyłącznie na obszarze informacyjno-informatycznym stworzy system TIQM (*Total Information Quality Management*) ukierunkowany na skuteczność, efektywność i bezpieczeństwo zarządzania informacją. Będzie on funkcjonował w ramach kompleksowego działania obejmującego: identyfikację i analizę wymagań, ocenę jakości uzyskiwanej informacji, prognozowanie kosztów braku jakości, minimalizację i eliminację źródeł powstawania przyczyn oraz kreowanie i wdrożenie odpowiedniego sposobu postępowania projakościowego.

Kompleksowe zarządzanie jakością informacji w przedsiębiorstwach opierać się może na sformalizowanych i niesformalizowanych systemach postępowania opartych na międzynarodowych standardach. Niezależnie od stosowanego sposobu zarządzania organizacją przedsiębiorcy w ramach TIQM muszą polegać na:

- orientacji na klientów,
- orientacji na procesy,
- orientacji na informacje,
- zachowaniach prewencyjnych,
- ciągłym doskonaleniu.

Orientacja na klientów wewnętrznych ma na celu wykreowanie nowego modelu środowiska pracy przy jednoczesnej zmianie stanu świadomości pracowników (zarówno liniowych, jak i kadry kierowniczej oraz zarządczej) poprzez szkolenia lub uświadamianie i objaśnianie, jak również procesu przekształceń stosunków pracy ukierunkowanych na zmianę kultury organizacji. Orientacja na klienta zewnętrznego natomiast musi opierać się głównie na odpowiednim kształtowaniu relacji, potrzeb, satysfakcji itd. W głównej mierze do danych osiąganych z tego obszaru będą zaliczane informacje m.in. o jakości zdefiniowanych modeli danych, pomiarach jakości danych, aktualności, kompletności, dokładności, użyteczności. Działania ukierunkowane na zarządzanie procesami muszą być rozwijane na wszystkich płaszczyznach organizacji, tj. płaszczyźnie operacyjnej, technologicznej, kontrolnej, planistycznej, badawczej, de-

[15] Szerzej o TQM: J. Łunarski, *Zarządzanie jakością. Standardy i zasady*, Warszawa 2012, s. 450–490; W.M. Grudzewski, I.K. Hejduk, *Metody projektowania systemów zarządzania*, Warszawa 2004, s. 12–54; J.J. Dahlgaard, K. Kristensen, G.K. Kanji, *Podstawy zarządzania jakością*, tłum. L. Wasilewski, Warszawa 2000.

terminującej skuteczność oraz efektywność prowadzanych zmian. Postępowania procesowe mogą być mniej lub bardziej sformalizowane m.in. poprzez instrukcje postępowania, procedury, regulaminy czy choćby dobre praktyki. Ma to w efekcie stworzyć pewien ciągły sposób wykonywania czynności (wzorzec, standard postępowania) zgodny z założeniami i zamierzonymi efektami[16]. Bezpieczeństwo informacji w ramach procesowych działań będzie osiągane poprzez konieczność budowania i doskonalenia m.in. aplikacji IT, narzędzi pomiaru jakości, zabezpieczeń systemowych i sprzętowych, baz danych.

Monitoring bezpieczeństwa informacji, w tym także niejawnych, powinien opierać się na zachowaniach prewencyjnych, wspomaganych przez jasno określony (świadomy, odpowiedzialny, wyszkolony itd.) czynnik ludzki, a także system/-y wczesnego ostrzegania[17]. Kompleksowa „ochrona" jakości informacji wymaga działań rozwojowych we wszystkich obszarach i procesach organizacji, dzięki czemu organizacja lepiej dostosowuje się do oczekiwań rynku, zmniejsza ryzyko słabych stron organizacji i zagrożeń pojawiających się w cyberprzestrzeni, zwiększa poziom bezpieczeństwa oraz strefę ochronną.

Zarządzanie w ramach TQM oparte na wskazanych obszarach musi dotyczyć działań projakościowych z zakresie informacji i całościowego funkcjonowania organizacji. Nie można odseparować sfery informacji od sfery zarządzania, dlatego integracja wysiłków skierowana na jeden czynnik będzie miała swoje odzwierciedlenie w drugim obszarze.

Jedynie połączenie starań może gwarantować osiągnięcie sukcesu poprzez:

- stały monitoring jakości informacji (kontrolę, analizę i doskonalenie danych uzyskiwanych, przetwarzanych oraz przekazywanych);
- przejrzyste, skuteczne i zrozumiałe procedury postępowania zwiększające rolę jakości informacji (wzmocnienie znaczenia pracowników, akredytację bezpieczeństwa w dostępności itd.);
- wzmocnienie czynnika jakości informacji w biznesowej sferze organizacji (monitorowanie i eliminowanie ryzyka, kreowanie odpowiedniej polityki IT oraz bezpieczeństwa informacji);
- rozwijanie zasobów infrastrukturalnych i rzeczowych (w ramach IT) gwarantujących właściwe postępowanie ukierunkowane na kształtowanie jakości informacji.

4.2. Systemy zarządzania wspomagające stosowanie bezpieczeństwa informacji[18]

4.2.1. ISO 31000 – Zarządzanie ryzykiem

Ryzyko jest nieodłącznym elementem życia społeczno-gospodarczego, m.in. funkcjonowania, kształtowania bytu oraz rozwoju przedsiębiorstw, a także gospodarstw domowych lub samego społeczeństwa.

---

[16] B. Bober, *Rola standardów w procesie podejmowania decyzji o wyborze procedur szpitalnych*, red. E. Skrzypek, Lublin 2008.

[17] B. Bober, *Zastosowanie sieci neuronowych w modelowaniu ryzyka szpitalnego*, [w:] *Uwarunkowania jakości życia w społeczeństwie informacyjnym*, red. E. Skrzypek, Lublin 2007.

[18] Opracowano między innymi na podstawie informacji zawartych normach oraz w bazach informacji PKN (Polskiego Komitetu Normalizacyjnego).

W literaturze przedmiotu ryzyko definiowane jest różnorodnie, m.in. jako:[19]

- stan umysłu człowieka, jeżeli ulega on zmianie, to zmienia się również ryzyko. Ryzyko istnieje wtedy, gdy podmiot ma świadomość jego istnienia (ujęcie psychologiczne), ryzyko można mierzyć za pomocą prawdopodobieństwa,
- niepewność związana z przyszłymi wydarzeniami lub wynikami decyzji,
- zagrożenie nieosiągnięcia zamierzonego zysku wynikające z posiadania niepełnej informacji,
- potencjalne wahania oczekiwanego dochodu,
- sytuacja, w której przyszłych warunków gospodarowania nie można przewidzieć z całą pewnością, a znany jest jej rozkład ich prawdopodobieństwa. Ryzyko występuje nawet wówczas, gdy tylko jeden z czynników sytuacji nie jest znany, a istnieje prawdopodobieństwo jego wystąpienia,
- zjawisko obiektywne – dotyczy realnych zjawisk gospodarczych, mających związek z instrumentem zagrożenia (niebezpieczeństwa) wynikającego ze zmienności (skali i dynamiki zmian) po stronie popytu, działalności konkurencji, warunków kooperacji, działań regulacyjnych państwa (podatków, ulg). Jest także zjawiskiem subiektywnym, gdyż jest uwarunkowane stanem wiedzy o procesach gospodarczych.

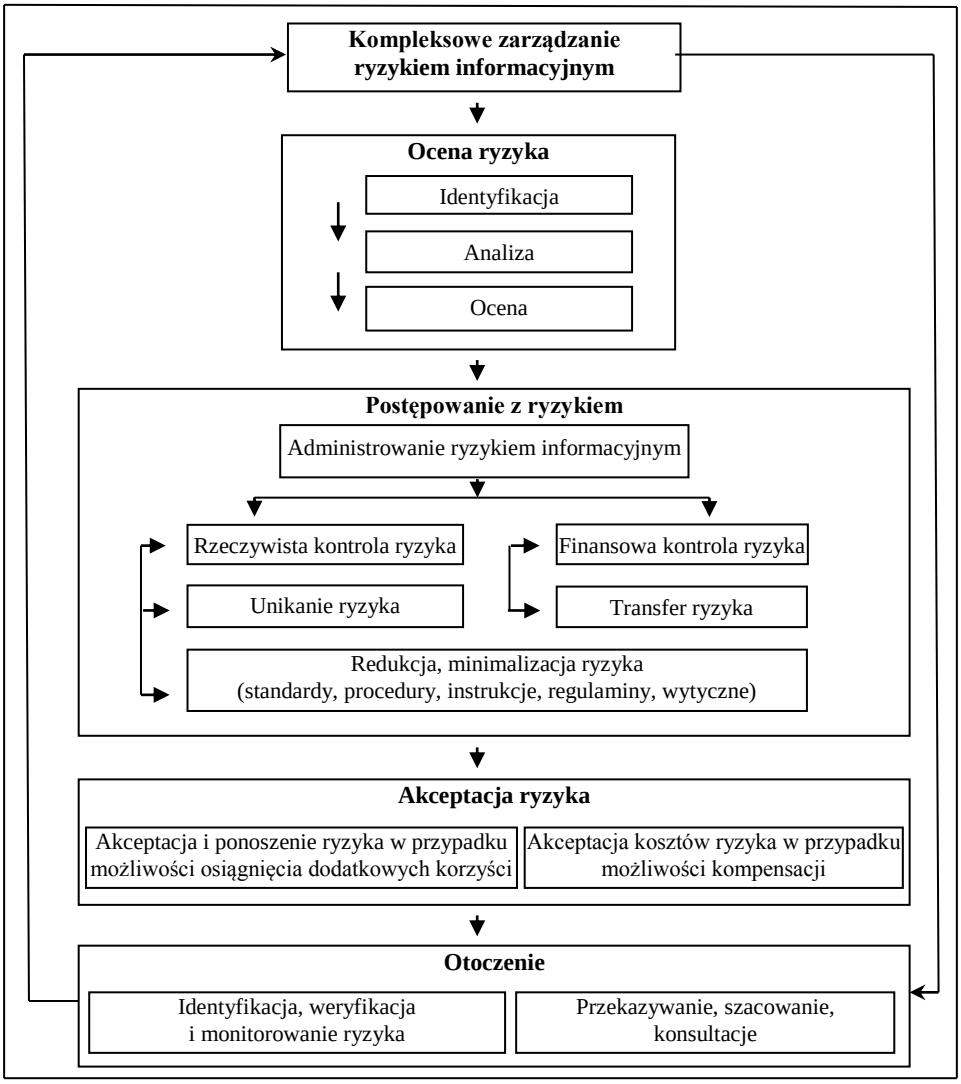
Analizując powyższe definicje, należy stwierdzić, że ryzyko jako stan zagrożenia może być wywołane przez uzyskane informacje. Oznacza to, że sposób przekazywania (uzyskiwania, zdobywania) informacji, a także jej zawartość (jakość), może doprowadzić do błędnych decyzji, efektem czego będzie zwiększenie ryzyka prowadzonej działalności (wykonywanych lub planowanych czynności). Dlatego ważnym elementem funkcjonowania każdego podmiotu, w celu osiągnięcia zamierzonego efektu, jest odpowiednie zarządzanie ryzykiem, w tym przypadku ryzykiem informacyjnym.

Zarządzanie ryzykiem informacyjnym nie jest prostym działaniem. Jego problematyczność ukazuje model kompleksowego zarządzania ryzykiem informacyjnym (rys. 4), który na etapie postępowania z ryzykiem stosuje systemowe rozwiązania poprzez wykorzystanie procedur postępowania zawartych w standardach, m.in. ISO 31000.

Norma ISO 31000:2009, *Zarządzanie ryzykiem – Zasady i wytyczne*, jest uniwersalnym standardem możliwym do wdrożenia w każdej organizacji różnych branż, który określa zasady, zakres oraz sposoby zarządzania ryzykiem i jego oceny. Wszystko oparte jest na zarządzaniu procesowym w celu lepszej, skuteczniejszej możliwości integracji systemów oraz zdolności do ciągłego doskonalenia gwarantującego realizację zamierzeń (lub zwiększającego prawdopodobieństwo osiągnięcia celów). System zarządzania ryzykiem według ISO 31000 ukierunkowany na zasób informacyjny ma na celu lepszą identyfikację i ocenę zarówno wewnętrznych, jak i zewnętrznych zagrożeń, a także stworzyć podwaliny pod możliwości opracowania wytycznych lub konkretnych sposobów postępowania, kontroli (nadzoru), zabezpieczeń, a także monitoringu obrotu informacjami jawną i niejawną. Działanie podmiotów w ramach tego systemu pozwoli zidentyfikować i zrozumieć ryzyko determinujące sposób po-

[19] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, Warszawa 2010, s. 34–35.

stępowania, ograniczające prawidłowe funkcjonowanie lub rozwój, a także utwierdzi w przekonaniu, że systemowe rozwiązanie lub ograniczanie ryzyka prowadzą do bezpieczniejszego, efektywniejszego i skuteczniejszego zarządzania informacją oraz całą organizacją. Koszty związane z zastosowaniem systemu ograniczającego występowanie ryzyka są znaczące dla organizacji, ale z punktu widzenia oceny bezpieczeństwa informacyjnego jest to inwestycja o szybkim zwrocie gwarantująca jednocześnie zwiększenie konkurencyjności.



Ryc. 4. Model kompleksowego zarządzania ryzykiem informacyjnym
Fig. 4. Model comprehensive risk management information

Źródło: opracowanie własne na podstawie normy ISO 31000.

4.2.2. ISO 20000 – System zarządzania usługami informatycznymi

Współczesne podejście do zarządzania obejmuje stały nadzór nad doskonaleniem procesów zarządzania opartych na odpowiednich zasobach. Zasoby informacyjne ściśle powiązane są z systemami informatycznymi, często nazywanymi narzędziami pracy, niezbędnymi w osiąganiu celów organizacji.

Systemy informatyczne stały się więc nieodłącznym źródłem informacji zarówno wewnętrznych, jak i zewnętrznych. Dlatego ochrona danych (informacji) stała się tak ważnym elementem każdego systemu zarządzania.

Analizując powszechność stosowania systemów informatycznych, należy wskazać, że występują w organizacji w różnych postaciach, np. jako:

- system monitoringu wejść i wyjść pracowników,
- oprogramowania urządzeń mobilnych typu: komputery, laptopy, palmtopy itd.,
- specjalistyczne oprogramowania typu: bazy danych (klientów, statystyczne, osobowe itd.) oprogramowanie dla pracowników poszczególnych komórek organizacyjnych, tj. księgowości, płac, kadr, planowania, magazynu, prawników itd.,
- program dostępu do Internetu, aplikacji społecznościowych itd.,
- systemy logistyczne.

Dlatego bardzo istotnym elementem dla przedsiębiorcy jest korzystanie z bezpiecznych usług lub narzędzi informatycznych gwarantujących bezpieczeństwo informacji, które wsparte wytycznymi normy ISO 20000, ma zagwarantować doskonalenie jakości usług IT oferowanych i dostarczanych potencjalnym klientom lub dać taką możliwość. Norma skierowana jest do podmiotów branży informatycznej i określa wytyczne sposobów postępowania w ramach procesowego działania, które miałoby uregulować funkcjonowanie wszystkich obszarów wykorzystujących zasoby informatyczne gwarantujące bezpieczeństwo pracy oraz wysoką jakość oferowanych usług. System zarządzania oparty na normie PN-ISO/IEC 20000-1:2014-01 dzięki odpowiednim sposobom nadzorowania ograniczać ma powstawanie ryzyka oraz potencjalnych zagrożeń poprzez identyfikację, analizę, zarządzanie i raportowanie procesów IT. Efektywność oraz skuteczność systemu uzależnione będą od odpowiedniego zarządzania tą sferą, tj. budżetowania, aktualizacji danych, rozbudowy systemów informatycznych o nowe moduły, zwiększania poziomów zabezpieczeń, konfiguracji na potrzeby zaspokojenia pragnień klienta lub zapotrzebowania rynku itd.

Analiza certyfikacji systemu ISO 20000 wskazuje, że standard ten wpisuje się w formę wspierającą działania projakościowe ukierunkowane na bezpieczeństwo informacji, gdyż w okresie 2007–2012 poddało się ocenie zewnętrznej 12 podmiotów, z czego 10 przedsiębiorstw – w ostatnich dwóch badanych latach.

Dzięki określeniu w normie sześciu najważniejszych obszarów – wymagań dotyczących systemu zarządzania usługami, projektowania i przekazania nowych lub zmienionych usług, procesu dostarczania usług, procesów związków (powiązań), rozwiązań i kontrolnych – wskazano wykorzystanie biznesowe stosowane przez podmioty:

- świadczące lub planujące świadczyć usługi IT,
- wymagające spójnego podejścia wszystkich swoich dostawców usług,

- wykazujące możliwości zarządcze IT (zdolność do projektowania, przekazywania, dostarczania i doskonalenia usług) zapewniające pewien standard zgodny z oczekiwaniami klienta,
- rozwijające usługi w zakresie skutecznego monitorowania, dokonywania pomiarów i doskonalenia jakości usług oraz zarządzania nimi,
- w których IT stanowi element biznesowy (proces biznesowy podlegający ciągłemu doskonaleniu) przynoszący określone korzyści ekonomiczne,
- dobrowolnie poddające się weryfikacji oferowanej jakości (wykonywanej przez niezależną jednostkę certyfikującą).

Analizując standard ISO 20000, możemy dojść do wniosku, że prawidłowe zarządzanie bezpieczeństwem informacji w organizacji pośrednio uzależnione jest od naszych wymagań stawianych podmiotom dostarczającym usługi IT, a także sposobów systemowego zabezpieczania się w ramach wykorzystywanych systemów informatycznych.

4.2.3. ISO 22301 – System zarządzania ciągłością biznesu

Standard ISO 22301:2012 zastąpił brytyjski BS 25999-2:2007 w zakresie zarządzania ciągłością działania. Świadome zarządzanie oparte na standardzie ISO 22301 może mieć zastosowanie we wszystkich organizacjach różnych branż w ramach jednego systemu lub integracji systemowej. Zarządzanie bezpieczeństwem informacji w ramach systemu zarządzania według normy ISO 22301:2012 stanowić ma gwarancję osiągania celów i funkcjonowania organizacji w sytuacjach krytycznych lub kryzysowych.

Zarządzanie ciągłością działania (*Business Continuity Management* – BCM) ma zapewnić możliwość świadczenia usług o określonym poziomie jakości, w sytuacjach wystąpienia zaburzeń zakłócających, w ramach procesowego działania, co gwarantowałoby prawidłowe funkcjonowanie organizacji. System zarządzania oparty na normie ISO ma na celu zwiększenie możliwości organizacji m.in. w zakresie:

- wiedzy o występujących zagrożeniach,
- walki poprzez skuteczniejszy proces decyzyjny,
- efektywniejszych i skuteczniejszych działań prewencyjnych,
- finansowania działań zapobiegawczych,
- odpowiedniego planowania strategicznego,
- sformalizowania oraz sparametryzowania sposobów postępowania i reagowania.

Ingerencja systemu w różnych obszarach ma za zadanie zminimalizować determinację niekorzystnych zjawisk, zdarzeń, zawirowań, klęsk żywiołowych, katastrof oddziaływających na realizację procesów, co oznacza tym samym, że ingeruje w sposób ograniczania ryzyka i minimalizacji negatywnych skutków. Budowanie pewnego rodzaju „parasola ochronnego" (odporności systemowej) organizacji ma przeciwdziałać lub podejmować takie działania, które zagwarantują w ciągły sposób osiąganie celów, utrzymanie lub podwyższanie jakości oferowanych usług, kreowanie odpowiedniego wizerunku przedsiębiorstwa oraz marki, a także podnoszenie wartości firmy. Oznacza to, że system zarządzania ciągłością biznesu ma wskazywać drogę doskonalenia

działań (poprzez odpowiednie procedury, instrukcje itd.) związanych z funkcjonowaniem i rozwojem organizacji, w której ważnym, determinującym elementem jest jakość informacji. Badania wykazały, że standard ten wpisuje się w formę wspierającą działania ukierunkowane na bezpieczeństwo informacji, gdyż w okresie 2008––2010 certyfikat uzyskało 5 podmiotów w ramach ISO 22301:2012.

System zarządzania ciągłością biznesu jednocześnie wpisuje się w rodzinę norm ISO, a w szczególności obszar normy ISO 9001, przez co konieczne są m.in. następujące zadania:

- określenie polityki, strategii i celów zapewniających ciągłość działania i rozwoju,
- zidentyfikowanie, ocena i sformalizowanie procesowego zarządzania,
- identyfikacja i minimalizacja ryzyka i niepewności,
- kreowanie odpowiednich relacji z kooperantami, pracownikami i klientami,
- ciągłe doskonalenie wszystkich obszarów organizacji, a w szczególności tych, które mają bezpośredni wpływ na działania podejmowane w sytuacjach kryzysowych,
- monitorowanie i rejestrowanie sytuacji krytycznych oraz podejmowanych działań zapobiegawczych i koordynacyjnych z uwzględnieniem oceny sprawności, skuteczności, aktualności systemu bezpieczeństwa (najczęściej informatycznego),
- stworzenie „systemu" szybkiego reagowania powiązanego z modułem oceny zagrożenia oraz prognozowania możliwości wystąpienia takiego niebezpieczeństwa.

Podsumowując, należy stwierdzić, że systemowe zarządzanie ciągłością biznesu według normy ISO 22301:2012 ma poprzez odpowiednie narzędzia gwarantować, również w sytuacjach zagrożeń wewnętrznych i zewnętrznych, poprawne wykonywanie i rozwój procesu biznesowego, kreującego wartość organizacji. Brak natomiast odpowiednich identyfikacji i analizy zagrożeń prawidłowego zarządzania informacją, w szczególności niejawną, może spowodować błędne określenie narzędzi ochrony informacji.

4.2.4. ISO 24762 – Technika informatyczna – techniki bezpieczeństwa

Norma PN-ISO/IEC 24762:2010 zawiera wytyczne dotyczące ochrony informacji, w ramach usług technologii komunikacyjnej. W szczególności dotyczy obszaru odzyskania danych komunikacyjnych sprzed katastrofy (ang. *ICT Disaster Recovery*, ICT DR), które są głównymi determinantami zarządzania ciągłością działania – zarządzania ciągłością biznesu (BCM), mającymi również zastosowanie w *in-house* i *outsourced* przez podmioty dostarczające usługi IT.

Międzynarodowa norma ma na celu wspomaganie systemu zarządzania organizacją w obszarze bezpieczeństwa informacji w okresach kryzysu zewnętrznego i wewnętrznego, zapewniając dostępność komunikacyjną poprzez procesowe działania.

Wdrażając ten standard, organizacje będą zdolne do wprowadzenia mechanizmów ochronnych do ich infrastruktury teleinformatycznej, która pozostaje istotna dla kluczowej działalności. Zostanie w ten sposób uzupełnione ich zarządzanie ciągłością

funkcjonowania (by lepiej radzić sobie z tymi rodzajami ryzyka, które mogą przerwać działalność organizacji) oraz zarządzanie bezpieczeństwem informacji (by skuteczniej chronić poufność, integralność i dostępność informacji). Zgodnie z tym standardem zarządzanie ciągłością działania jest częścią ogólnego procesu zarządzania ryzykiem w organizacji i obejmuje:

- zidentyfikowanie potencjalnych zagrożeń, które mogą spowodować znaczący wpływ na działanie organizacji, wraz z określeniem powiązanych rodzajów ryzyka;
- dostarczenie ram do uodporniania procesów biznesowych na zdarzenia kryzysowe;
- dostarczenie zdolności, zasobów, procesów, sposobów postępowania w celu zapewnienia skutecznej reakcji na katastrofy i awarie[20].

Procesowe działanie w ramach stosowania systemu ISO 24762 wymusza:

- określenie wymagań dla wdrożenia, eksploatacji, monitorowania oraz utrzymania usług i udogodnień techniczno-technologicznych ICT DR;
- identyfikację i określenie możliwości, które zewnętrzni dostawcy usług ICT DR powinni mieć, oraz jakie stosować praktyki, aby zapewnić bezpieczeństwo podstawowego środowiska pracy i ułatwić działania naprawcze (*recovery efforts*),
- stosowanie wytycznych wyboru miejsca odzysku (*recovery site*),
- stosowanie wytycznych dla dostawców usług ICT DR w ramach ciągłego doskonalenia swoich usług ICT DR.

Oznacza to, że międzynarodowy standard zawiera wskazówki dotyczące wdrożenia, testowania i realizacji poszczególnych elementów przywracania stanu sprzed katastrofy, a w szczególności są to wskazówki dotyczące[21]:

- wdrażania, funkcjonowania, monitorowania oraz utrzymywania niezbędnych zasobów i usług koniecznych do przywrócenia stanu sprzed katastrofy (np. wdrożenie systemu informowania pracowników o zagrożeniu lub wymaganie o możliwości ręcznego otwierania drzwi elektronicznych od wewnątrz);
- mechanizmów przywrócenia stanu sprzed awarii systemów teleinformatycznych organizacji;
- wymagań, których spełniania należy oczekiwać od dostawców usług związanych z przywracaniem po katastrofie;
- wyboru centrum awaryjnego (np. uwzględnianie takich czynników, jak stabilność organizacji, dobra infrastruktura) i wymagań w stosunku do organizacji oferujących tego typu usługi.

Z przedstawionych danych wynika, że stosowanie procesowego zarządzania w bezpieczeństwie informacji jest istotne, determinuje możliwość powiązania międzynarodowych norm (rodziny norm ISO 20000, tj. ISO 20000-1 – System zarządzania usługami informatycznymi, ISO 22301 – System zarządzania ciągłością biznesu, ISO 24762 – Technika informatyczna – Techniki bezpieczeństwa; z normą ISO 9001 – System zarządzania jakością) w jedną systemową całość gwarantującą bezpieczeństwo informatyczne przedsiębiorstwa.

---

[20] *Norma ISO 24762*, www.centrum.bezpieczenstwa.pl/index.php/standardy-othermenu-16/1064-iso-24762 (dostęp: 24.10.2014).

[21] Tamże.

4.2.5. ISO 9000 – Zarządzanie jakością

Współczesne systemy zarządzania ukierunkowane na jakość poruszają różne jej aspekty oraz określają standardy działania, gdyż obejmują swoim zasięgiem całą organizację, a nie tylko jej poszczególne (jednostkowe) obszary. Najbardziej rozpoznawalny i rozpowszechniony na świecie jest system zarządzania jakością z rodziny ISO 9000, który opisuje całokształt funkcjonowania i rozwoju organizacji. Dlatego system zarządzania jakością interpretuje się jako zbiór wzajemnie powiązanych lub wzajemnie oddziaływających elementów niezbędnych do ustanowienia polityki i celów, osiągania tych celów oraz kierowania organizacją (zasobem ludzi i infrastrukturą, z przypisaniem odpowiedzialności, uprawnień i powiązań) i jej nadzorowania w odniesieniu do jakości[22].

Ewolucja systemu zarządzania jakością według ISO 9000 spowodowała osiągnięcie standardu, który nastawiony jest na doskonalenie procesów organizacyjnych zaspokajających potrzeby i zwiększających satysfakcję potencjalnego klienta.

Niektórzy w swych poglądach idą dalej, twierdząc, że jest to pewnego rodzaju „koncepcja projektowania i usprawniania systemów działania, w której doskonalony układ przedstawiony jest jako zbiór następujących części składowych: funkcja systemu, wejście, wyjście, sekwencja kroków przekształcenia wejść w wyjścia (proces), otoczenie systemu, wyposażenie i zasoby ludzkie”[23]. Należy jednak pamiętać, że sformalizowany system zarządzania jest na tyle uniwersalny, że może funkcjonować we wszystkich organizacjach różnych branż, niezależnie od formy prawnej czy wielkości przedsiębiorstwa oraz zakresu i obszaru działania. Do norm z rodziny ISO 9000 należą:

- ISO 9000:2015 – System zarządzania jakością – Podstawy i terminologia,
- ISO 9001:2015 – System zarządzania jakością – Wymagania,
- ISO 9004:2009 – System zarządzania jakością – Wytyczne doskonalenia funkcjonowania,
- ISO 19011:2011 – Wytyczne dotyczące auditowania systemów zarządzania jakością i/lub zarządzania środowiskowego.

Należy podkreślić, że dążenie do doskonałości występuje również w ujęciu tej grupy norm, gdyż były już nowelizowane czterokrotnie, a następna aktualizacja nastąpiła w 2015 r. Ciągłe doskonalenie norm powoduje, że organizacje coraz chętniej wdrażają ten system, gdyż do 31 grudnia 2013 r. co najmniej 1 129 446 certyfikatów wydano w 187 krajach. W 2013 r. nastąpił wzrost o 3%, tj. o 32 459 certyfikatów w stosunku do roku 2012. W Polsce na dzień 31 grudnia 2013 r. jest nowo certyfikowanych 10 527 podmiotów w stosunku do roku 2012[24]. Choć standard ISO 9001 nie jest wymagany, to często się go stosuje. Wynikać to może z potrzeby dostosowania się do kooperantów, dostawców a przede wszystkim klientów. W praktyce spotyka się sytuacje, kiedy podmioty gospodarcze działają w ramach systemu zarządzania według ISO 9000, a nie są certyfikowane (nie mają potwierdzenia zgodności wydanego przez niezależne jednostki do tego celu powołane) w ramach systemu. Wynika to z indywidualnych przesłanek organizacji, choć najczęściej stwierdza się, że głównymi

---

[22] *PN-EN ISO 9000:2015-10. Systemy zarządzania jakością. Podstawy i terminologia*, Polski Komitet Normalizacyjny, Warszawa 2016.

[23] *Leksykon zarządzania*, red. M. Adamska, Warszawa 2004, s. 568.

[24] *Standards*, www.iso.org/iso/home/standards.htm (dostęp: 13.10.2014).

determinantami są warunki finansowe, a także ścisłe procedury postępowania, na które organizacje nie zawsze mogą sobie pozwolić.

Standard określony przez normy z rodziny ISO 9000, jego wszechstronność, stał się również podwaliną pod inne systemy zarządzania ukierunkowane na jakość, dając możliwość integracji systemów tworzących jedną całość.

4.2.6. AQAP – Zapewnienie jakości

AQAP jako międzynarodowy system[25] związany z zapewnieniem odpowiedniego poziomu jakości wymagany jest przez jednostki wojskowe NATO, wynika z dokumentów standaryzacyjnych NATO – STANAG 4107.

Powiązania standaryzacyjne mają znaczący wpływ na wymagania stawiane przedsiębiorcom ujęte są między innymi w[26]:

- AQAP 160 NATO Integrated Quality Requirements for Software throughout the Life Cycle (AQAP 160 NATO Zintegrowane wymagania jakościowe dla oprogramowania w całym cyklu życia),
- AQAP 169 NATO Guidance on the Use of AQAP 160, Ed.1 (AQAP 169 Wytyczne NATO w sprawie stosowania AQAP 160, wyd. 1),
- AQAP 2000 NATO Policy on an Integrated Systems Approach to Quality through the Life Cycle (AQAP 2000 Polityka NATO dotycząca zintegrowanego systemowego podejścia do jakości w cyklu życia),
- AQAP 2009 NATO Guidance on the Use of the AQAP 2000 Series (AQAP 2009 Wytyczne NATO do stosowania AQAP serii 2000),
- AQAP 2050 NATO Project Assessment Model (AQAP 2050 NATO Projekt Szacunkowego Modelu),
- AQAP 2070 NATO Mutual Government Quality Assurance (GQA) Process (AQAP 2070 Proces NATO dotyczący wzajemnej realizacji Rządowego Zapewnienia Jakości (GQA)),
- AQAP 2105 NATO Requirements for Deliverable Quality Plans (AQAP 2105 Wymagania NATO dotyczące planów jakości dla wyrobu będącego przedmiotem zamówienia),
- AQAP 2110 NATO Quality Assurance Requirements for Design, Development and Production (AQAP 2110 Wymagania NATO dotyczące zapewnienia jakości w projektowaniu, pracach rozwojowych i produkcji),
- AQAP 2120 NATO Quality Assurance Requirements for Production (AQAP 2120 Wymagania NATO dotyczące zapewnienia jakości w produkcji),
- AQAP 2130 NATO Quality Assurance Requirements for Inspection and Test (AQAP 2130 Wymagania NATO dotyczące zapewnienia jakości w kontroli i badaniach),

[25] Skrót AQAP (ang. Allied Quality Assurance Publication) tłumaczony jako Publikacja Standaryzacyjna dotycząca Zapewnienia Jakości lub Sojusz Publikacji Zarządzania Jakością. Potocznie stosuje się nazwę: system zapewniający jakość.

[26] Por. *Akty prawne dotyczące oceny zgodności wyrobów i akredytacji OiB*, www.wcnjk.wp.mil.pl/pl/18.html (dostęp: 20.10.2014).

- AQAP 2131 NATO Quality Assurance Requirements for Final Inspection (AQAP 2131 Wymagania NATO dotyczące zapewnienia jakości przy kontroli końcowej),
- AQAP 2210 NATO Supplementary Software Quality Assurance Requirements to AQAP 2110 (AQAP 2210 NATO Dodatkowe wymagania dotyczące zapewnienia jakości oprogramowania dla AQAP 2110),
- Decyzji Nr 67/MON Ministra Obrony Narodowej z dnia 5 marca 2014 r. w sprawie nadzoru nad funkcjonowaniem w resorcie obrony narodowej systemu zapewnienia jakości wyrobów obronnych (Dz.Urz. MON 2014, poz. 77),
- Decyzji Nr 36/PUM Podsekretarza Stanu ds. Uzbrojenia i Modernizacji z dnia 16 maja 2011 r. w sprawie określenia zasad funkcjonowania systemu zapewnienia jakości, obowiązków zamawiającego, Rejonowych Przedstawicielstw Wojskowych (RPW), gestora i centralnego organu logistycznego uzbrojenia i sprzętu wojskowego oraz Wojskowego Centrum Normalizacji, Jakości i Kodyfikacji (WCNJiK) w zakresie zapewnienia jakości wyrobów obronnych (nieopublikowana),
- Decyzji Nr 39/PUM Podsekretarza Stanu w MON ds. Uzbrojenia i Modernizacji z dnia 7 maja 2012 r. w sprawie wprowadzenia do stosowania w resorcie obrony narodowej procedur wykonawczych dotyczących zapewnienia jakości wyrobów obronnych (nieopublikowana).

System zapewnienia jakości (AQAP) odnosi się do podmiotów gospodarczych świadczących usługi wojsku, a w szczególności dostawców. Usługodawcy wojskowi nieposiadający systemu AQAP, a chcący świadczyć usługi dla „służb mundurowych", muszą mieć inny system zarządzania jakością odpowiadający stawianym wymaganiom systemowym, np. według normy ISO 9001 gwarantujący, między innymi, powtarzalność jakości oferowanego produktu lub odpowiednią jakość usługi.

Wojska NATO reprezentowane przez kraje Unii Europejskiej swój system zapewnienia jakości oparły na międzynarodowych normach jakości serii ISO w celu ujednolicenia wymagań i wytycznych stawianych wobec przedsiębiorców z różnych stron świata. Uniwersalnym narzędziem do budowy aktualnego sytemu zapewnienia jakości AQAP 2000 stał się system zarządzania jakością według normy ISO 9001, który pozwolił określić:

- wymagania NATO:
  - dotyczące zapewnienia jakości w projektowaniu, pracach rozwojowych i produkcji (AQAP 2110:2009),
  - dotyczące zapewnienia jakości w produkcji (AQAP 2120:2009),
  - dotyczące zapewnienia jakości w kontroli i badaniach (AQAP 2130:2009),
  - dotyczące systemu zarządzania jakością dostawców dla przemysłu lotniczego i obronnego (AQAP 2310:2013);
- wytyczne NATO:
  - zintegrowane systemowe podejście do jakości podczas cyklu życia wyrobu (AQAP 2000:2009),
  - stosowanie AQAP serii 2000 (AQAP 2009:2010),
  - wzajemny proces rządowego zapewnienia jakości (GQA) w NATO (AQAP 2070:2009).

Jednostki wojskowe w ramach procesowego zarządzania doskonalą się i podnoszą poziom jakości m.in. w obszarach:

- wykonywanych czynności organizacyjnych, planistycznych i wykonawczych,

- świadczenia „usług obronnych”,
- zaplecza niezbędnego do świadczenia podstawowych zadań (wyposażenie wojskowe, infrastruktura, systemy informatyczne itd.),
- posiadanych zasobów ludzkich,
- procesu decyzyjnego.

Reasumując, stosowanie działań projakościowych w jednostkach wojskowych (w resorcie obrony) przynosi korzystne zmiany związane między innymi z podnoszeniem jakości szkoleń, wyposażenia, gotowości bojowej, możliwości wspólnego reagowania z wojskami sojuszu. Wprowadzane zmiany i ich tempo spowodowały ewolucję w myśleniu i postrzeganiu jakości, w tym także jakości informacji. Takie działania szybko wymusiły przeobrażenia w przedsiębiorczości okołowojskowej. Przedsiębiorcy pragnący świadczyć usługi dla wojsk NATO muszą zastosować się do określonych wymagań jakościowych wg międzynarodowych standardów. Jednocześnie w celu zwiększenia konkurencyjności i atrakcyjności mogą integrować system AQAP z systemem ISO 9000, a także w celu podniesienia bezpieczeństwa przekazywanych informacji z systemem ISO 27001, tworząc jeden zintegrowany system zarządzania[27] projakościowego.

5. System zarządzania bezpieczeństwem informacji

Zabezpieczenie wszystkich obszarów informatycznych w przedsiębiorstwie wymusza na organizacjach przyjęcie odpowiedniego sposobu postępowania, najlepiej opartego na procesowym działaniu, pozwalającym m.in.:

- w odpowiedni sposób określić bezpieczeństwo przetwarzanych informacji w systemach,
- monitorować formy zabezpieczeń i w razie konieczności w nie ingerować,
- doskonalić elementy systemów informatycznych gwarantujących bezpieczeństwo,
- nadzorować bezpieczeństwo informacji w obszarze niszczenia lub usuwać dane, informacje z różnych nośników lub systemów informatycznych.

Stosowanie odpowiednich form bezpieczeństwa przyczynia się do zwiększenia jakości oferowanych usług, co pozwala na zwiększenie konkurencyjności, gwarantując minimalizację wystąpienia ryzyka ujawnienia lub przekazania informacji osobom niepowołanym. Oznacza to, że bezpieczeństwo teleinformatyczne ściśle powiązane jest z zarządzaniem ryzykiem, co umożliwia zastosowanie rozwiązań procesowych (systemowych) w ramach określonych zasobów oraz poziomów zabezpieczeń. W szczególności dotyczyć to może informacji niejawnych, uzależnionych od stref kontrolowania, trybu i sposobu przetwarzania informacji w ramach poszczególnych klauzul: zastrzeżone, poufne, tajne czy ściśle tajne.

W ramach odpowiedzialnego zarządzania bezpieczeństwem informacji przedsiębiorstwa wykorzystują systemy rodziny norm ISO 27000. Stosowanie systemu zarządzania ISO nie jest obowiązkowe, ale stanowi dobrą praktykę. Określone sposoby postępowania dotyczą różnych obszarów działania organizacji wyłącznie w aspekcie informacji, np. finansowo-księgowych, techniczno-technologicznych, organizacji pracy, personalnych (pracowniczych), a także w zakresie informacji poufnych. W znaczą-

[27] M. Olkiewicz, *Funkcjonowanie zintegrowanego systemu zarządzania w organizacji*, [w:] *Jakościowe aspekty integracji zarządzania*, red. E. Skrzypek, Lublin 2012, s. 75–88.

cy sposób wskazane rozwiązania ingerują w bezpieczeństwo IT w przedsiębiorstwie, zarówno w ramach systemów czy procesów, ale także sprzętu komputerowego i monitorującego pracowników w celu zwiększenia bezpieczeństwa aktywów informacyjnych. Do rodziny norm ISO 27000 zalicza się standardy:

- ISO/IEC 27001:2013 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania,
- ISO/IEC 27002:2013 – Technika informatyczna – Techniki bezpieczeństwa – Praktyczne informacje dla kontroli bezpieczeństwa,
- ISO/IEC 27003:2010 – Technika informatyczna – Techniki bezpieczeństwa – Wytyczne do zarządzania bezpieczeństwem informacji Wdrożenie systemu,
- ISO/IEC 27004:2009 – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie bezpieczeństwem informacji – Pomiar.

Wzrost znaczenia bezpieczeństwa informacji, uniwersalność zastosowania systemu a także zmieniające się otoczenie „jakości organizacji" wymusiły działania doskonalące w ramach systemu. Znowelizowana norma ISO/IEC 27001:2013 weszła w życie 23 października 2013 r. i zastępuje poprzednie wydanie z roku 2005 (ISO/IEC 27001:2005) w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) (odpowiednika ISMS – *Information Security Management System*). Zgodnie z wytycznymi normy SZBI traktowany jest jako „część ogólnego systemu zarządzania, bazującego na biznesowym podejściu do ryzyka, w celu ustanowienia, wdrożenia, działania, monitorowania, przeglądania, utrzymywania i doskonalenia bezpieczeństwa informacji"[28].

SZBI oparty na procesowym zarządzaniu ukierunkowany na systematyczne działania związane z zarządzaniem ryzykiem ma m.in. na celu zwiększenie świadomości bezpieczeństwa informacyjnego pracowników (związanych np. z korzyściami, zagrożeniami, konsekwencjami, sposobami zabezpieczeń, procedurami działania) oraz bezpieczeństwa systemów teleinformatycznych w organizacji.

Ciągłe doskonalenie procesowego zarządzania opierać się ma na następujących obszarach:

- polityce bezpieczeństwa,
- organizacji bezpieczeństwa informacji,
- zarządzaniu aktywami,
- bezpieczeństwie zasobów ludzkich,
- bezpieczeństwie fizycznym i środowiskowym,
- zarządzaniu systemami i sieciami,
- kontroli dostępu,
- pozyskiwaniu, rozwoju i utrzymaniu systemów informatycznych,
- zarządzaniu incydentami związanymi z bezpieczeństwem informacji,
- zarządzaniu ciągłością działania,
- zgodności.

Należy wspomnieć, że ustawa o ochronie informacji niejawnych podkreśla znaczenie audytu kontrolnego bezpieczeństwa systemu w ramach oceny przyjętych sposobów postępowania dotyczących skuteczności realizacji zabezpieczeń teleinformatycznych[29].

---

[28] PN-ISO/IEC 27001:2014–12 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, Polski Komitet Normalizacyjny, Warszawa 2014.

[29] Ustawa z dnia 5 sierpnia 2010 r.…, art. 2 pkt. 11 i 12.

Wprowadzone zmiany określone w normie ISO/IEC 27001:2013 poprzez systemowe zarządzanie będą znacząco determinowały funkcjonowanie organizacji i skuteczne osiąganie celów, zwiększają nacisk m.in. na:

- klientów (zainteresowane strony, akcjonariuszy rynku itd.),
- świadomość i zaangażowanie pracowników (w szczególności kadrę zarządzającą),
- ryzyko (począwszy od identyfikacji, skończywszy na sposobach postępowania często opartych na innych systemach, np. ISO 31000),
- doskonalenie systemu,
- monitorowanie i nadzór (w tym także audytowanie).

Organizacje stają więc przed wyzwaniem w zakresie odpowiedniego zarządzania ryzykiem, ponieważ źle przeprowadzona identyfikacja oraz analiza mogą skutkować błędnymi danymi wyjściowymi. Odpowiednie wdrożenie systemu gwarantującego bezpieczeństwo informacyjne skutkuje osiąganiem korzyści, np.:

- zwiększeniem wiarygodności,
- zwiększeniem udziału w rynku,
- zwiększeniem konkurencyjności i zyskowności,
- minimalizacją kosztów poprzez odpowiednie zarządzanie ryzykiem,
- skuteczniejszym zarządzaniem majątkiem organizacji,
- skuteczniejszym monitoringiem przekazu informacji jawnych i niejawnych,
- skuteczniejszymi zabezpieczeniami informacji niejawnych.

Poprzez osiągane korzyści, rekompensujące koszty poniesione na wdrożenie i utrzymanie systemu, przedsiębiorstwa rozwijają się w dynamiczny sposób i coraz częściej wdrażają SZBI. Wskaźnik ten widoczny jest w ujęciu globalnym (światowym), gdyż w roku 2007 scertyfikowanych w ramach ISO 27001 było 6112 podmiotów, a w 2013 r. aż 21 922, co stanowi wzrost o ponad 358%. W Europie wskaźnik przyrostu z roku na rok, w okresie 2010–2013, kształtuje się powyżej 30% (rok 2010 to 30,7%, 2011 r. to już 31,1%, a rok 2012 to 32,5%, natomiast w roku 2013 poziom wzrostu wyniósł aż 35,7%).

Doświadczenia światowe i europejskie miały przełożenie na przedsiębiorstwa polskie, wskazując, że czynnikiem gwarantującym ciągłość rozwoju jest minimalizacja poziomu ryzyka i niepewności, co zawarto w tabeli nr 1.

Tabela 1

Liczba certyfikowanych podmiotów rocznie

Table 1

Number of certified entities annually

Lata	2007	2008	2009	2010	2011	2012	2013
Przedsiębiorstwa	5	38	93	102	155	282	102

Źródło: opracowanie własne na podstawie *ISO 9000 – Quality* management, www.iso.org/iso-9001-quality-management (dostęp: 27.10.2015).

Dane zamieszczone w tabeli nr 1 wskazują, że przyrost podmiotów wdrażających i certyfikujących system bezpieczeństwa informacji stale rośnie do roku 2012 natomiast w roku 2012 ich liczba zmalała. W tabeli nr 2 zostały przedstawione dane potwierdzające uniwersalność systemu zarządzania bezpieczeństwem informacji z punktu widzenia zastosowania w podmiotach różnych branż.

Tabela 2

Liczba certyfikowanych podmiotów rocznie w poszczególnych branżach

Table 2

Number of certified entities annually in various industries

Rodzaje branż	Lata							
	2006	2007	2008	2009	2010	2011	2012	2013
Rolnictwo, rybołówstwo	1	45	1	13	8	14	13	13
Górnictwo i kopalnictwo	0	1	3	6	2	12	31	34
Produkty spożywcze, napoje i tytoń	3	14	1	10	6	8	10	24
Tekstylia i wyroby włókiennicze	0	1	1	3	3	2	12	10
Skóra i produkty skórzane	0	0	0	1	2	5	1	2
Drewno i wyroby z drewna	0	0	0	1	3	5	4	4
Produkcja papieru i wyrobów z papieru	2	6	6	7	4	7	13	17
Wydawnictwa	1	5	6	10	11	20	18	22
Firmy poligraficzne	34	84	30	62	78	101	121	148
Produkcja koksu i produktów rafinacji ropy naftowej	3	6	9	8	3	5	4	14
Paliwo jądrowe	0	0	0	0	0	1	1	2
Chemikalia, produkty chemiczne i włókna	7	3	3	9	9	9	11	24
Farmacja	0	1	3	4	6	3	0	3
Wyroby z gumy i tworzyw sztucznych	7	5	0	10	15	16	16	36
Niemetalicznych produktów mineralnych	1	3	0	16	16	8	0	5
Beton, cement, wapno, gips itp.	1	1	1	6	6	14	27	25
Podstawowe metalu i wyroby metalowe	10	5	2	16	25	28	36	50
Maszyny i urządzenia	18	10	9	29	31	36	43	52
Urządzenia elektryczne i optyczne	38	58	50	135	221	280	342	289
Przemysł stoczniowy	0	0	2	5	3	3	4	8
Lotnictwo	0	7	12	22	24	17	22	18
Pozostały sprzęt transportowy	1	3	2	4	4	7	4	25
Działalność produkcyjna, gdzie indziej niesklasyfikowana	4	14	2	5	5	23	8	5
Recykling	2	10	4	11	32	44	61	72
Energetyka wraz z usługami dystrybucji	8	10	11	20	9	12	15	45
Gazownictwo wraz z usługami dystrybucji	0	2	2	4	3	2	6	6
Wodociąg	1	1	2	11	13	13	10	23
Budownictwo	55	17	12	127	266	350	409	396
Handel detaliczny i hurtowy; naprawa pojazdów samochodowych, motocykli i artykułów użytku osobistego i domowego	12	38	26	93	164	214	215	224
Hotele i restauracje	2	4	0	6	10	32	4	5
Transport, gospodarka magazynowa i łączność	60	70	63	170	184	241	288	322
Pośrednictwo finansowe, obsługa nieruchomości, wynajem	47	54	68	148	185	113	138	169
Technologia informacyjna	890	1236	1152	2086	3217	3588	4558	5059
Usługi inżynierskie	25	33	48	173	122	126	189	211
Inne usługi	189	204	228	380	579	564	755	849
Administracja publiczna	23	33	79	181	79	106	155	192
Edukacja	8	9	25	47	75	65	102	101
Ochrona zdrowia i opieka społeczna	14	10	61	102	102	145	201	201
Inne usługi socjalne	8	13	16	46	54	75	98	106

Źródło: opracowanie własne na podstawie: *ISO Survey*, www.iso.org/the-iso-survey.html (dostęp: 13.10.2014).

Z analizy danych wynika, że najwięcej podmiotów wdrażających SZBI funkcjonuje w sektorach usługowych, do których zaliczają się m.in.: technologia informacyjna, usługi inżynierskie, poligrafia, administracja publiczna z opieką zdrowotną, a także budownictwo, transport i łączność. W branżach produkcyjnych prym wiedzie optyka oraz budowa maszyn i urządzeń. W tabeli nie ujęto służb mundurowych, gdyż nie są to podmioty gospodarcze, lecz sektory działalności państwowej. Obszary działalności Państwa, NATO, UE objęte są dodatkowymi systemowymi zabezpieczeniami informacji. Ochrona informacji w obszarze NATO regulowana jest następującymi dyrektywami:

- AC/35-D/2000 – Dyrektywa bezpieczeństwa osobowego,
- AC/35-D/2001 – Dyrektywa bezpieczeństwa fizycznego,
- AC/35-D/2002 – Dyrektywa bezpieczeństwa obiegu informacji,
- AC/35-D/2003 – Dyrektywa bezpieczeństwa przemysłowego,
- AC/35-D/2004 – Dyrektywa podstawowa INFOSEC,
- AC/35-D/2005 – Dyrektywa zarządzania INFOSEC w systemach teleinformatycznych (CIS)

oraz dokumentem C-M(2002)49[30].

Natomiast przepisy bezpieczeństwa Unii Europejskiej uregulowane są decyzjami Rady Unii Europejskiej[31] oraz Komisji Europejskiej[32].

Podsumowując, należy zatem przyjąć, że wyżej wymienione branże to „sektory wrażliwe", gdzie zarządzanie informacją, zwłaszcza niejawną, stanowi jeden z priorytetów, który mógłby mieć znaczący wpływ na funkcjonowanie państwa lub gospodarki (szczególnie konkurencyjności rynku w danej branży). Istnieje zatem konieczność stosowania systemów ukierunkowanych na zarządzanie bezpieczeństwem informacji w różnych podmiotach niezależnie od wielkości, branży, obszaru działania, a także od tego, czy są publiczne czy prywatne.

Podsumowanie

Analiza literatury oraz badania z zakresu systemowego zarządzania organizacją ukierunkowanego na zwiększanie wartości organizacji, w ramach działań projakościowych, wskazują m.in. na:

- zwiększanie świadomości i bezpośrednich działań gwarantujących bezpieczeństwo informacji;
- zmianę mentalności w stosunku do informacji jako zasobu, który stał się „produktem" sprzedaży;

---

[30] C-M(2002)49 z dnia 17 czerwca 2002 r. – Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego (z późn. zm.).

[31] Decyzja Rady Unii Europejskiej 2011/292/UE z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.Urz. UE 2011, L141, poz. 17 z późn. zm.).

[32] Decyzja Komisji Europejskiej 2001/844/EC z dnia 29 listopada 2001 r. zmieniająca jej regulamin wewnętrzny (notyfikowana jako dokument nr C (2001) 3031) (Dz.Urz. UE 2001, L317, poz. 1).

- coraz częstsze wdrażanie w organizacjach projakościowych systemów zarządzania, ze szczególnym uwzględnieniem znormalizowanych międzynarodowych systemów zarządzania bezpieczeństwem informacji;
- rosnące koszty standardowych oraz alternatywnych rozwiązań stosowanych w celu zapewnienia stabilności ochrony informacji oraz zrównoważonego rozwoju kapitału intelektualnego;
- konieczność doskonalenia mechanizmów regulujących zapewnienie bezpieczeństwa między innymi obiegu informacji, przemysłowego.

Zapewnienie bezpieczeństwa informacji w działalności gospodarczej minimalizuje ryzyko utraty danych, które bezpośrednio oddziaływają na konkurencyjność przedsiębiorstw oraz stabilny rozwój organizacji.

Bibliografia

Adamczyk A., Renk R., Radziulis J., Hołubowicz W., *Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania*, „ORACLE'owe PLOUG'tki" 2005, nr 36.

Bober B., *Zastosowanie sieci neuronowych w modelowaniu ryzyka szpitalnego*, [w:] *Uwarunkowania jakości życia w społeczeństwie informacyjnym*, red. E. Skrzypek, Lublin 2007.

Bober B., *Rola standardów w procesie podejmowania decyzji o wyborze procedur szpitalnych*, red. E. Skrzypek, Lublin 2008.

Boruszewski J., *Jakość i wiarygodność informacji w infobrokerstwie*, „Lingua ac Communitas" 2012, Vol. 22.

Chyliński M., *Informacja i zarządzanie informacją w działalności samorządowej*, „Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie" 2014, nr 69.

Dahlgaard J.J., Kristensen K., Kanji G.K., *Podstawy zarządzania jakością*, tłum. L. Wasilewski, Warszawa 2000.

Flakiewicz W., *Pojęcie informacji w technologii multimedialnej*, Warszawa 2005.

Gleick J., *Informacja*, Kraków 2012.

Griffin R.W., *Podstawy zarządzania organizacjami*, Warszawa 2004.

Grudzewski W.M., Hejduk I.K., *Metody projektowania systemów zarządzania*, Warszawa 2004.

Harmon G., *The measurement of information*, "Information Processing and Management" 1984, no. 1-2.

Iwaszko B., *Ochrona informacji niejawnych w praktyce*, Wrocław 2012.

Kałuszyńska E., *Wiedza i informacja*, [w:] *Informacja a rozumienie*, red. M. Heller, J. Mączka, Warszawa 2005.

Kister A., *Użyteczność informacyjna rachunku kosztów innowacji*, [w:] *Kreatywność i przedsiębiorczość w projakościowym myśleniu i działaniu*, t. I, red. E. Skrzypek, Lublin 2009.

Kowalewski M., Ołtarzewska A., *Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności – Państwowego Instytutu Badawczego*, „Telekomunikacja i Techniki Informacyjne" 2007, nr 3–4.

Leksykon zarządzania, red. M. Adamska, Warszawa 2004.

Łunarski J., *Zarządzanie jakością. Standardy i zasady*, Warszawa 2012.
Majchrzak-Lepczyk J., *Safety in the context of logistics and marketing support*, [w:] *Bezpieczeństwo w procesach globalizacji – dziś i jutro*, t. 1, red. Z. Grzywna, Katowice 2013.
Malara Z., *Przedsiębiorstwo w globalnej gospodarce: wyzwania współczesności*, Warszawa 2006.
Nogalski B., Surawski B.M., *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, [w:] *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona. Wybrane problemy, teorii i praktyki*, red. R. Borowiecki, M. Kwieciński, Kraków 2003.
Olkiewicz M., *Podstawy zarządzania jakością. Wybrane aspekty*, Koszalin 2008.
Olkiewicz M., *Funkcjonowanie zintegrowanego systemu zarządzania w organizacji*, [w:] *Jakościowe aspekty integracji zarządzania*, red. E. Skrzypek, Lublin 2012.
PN-ISO/IEC 27001:2014–12, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, Polski Komitet Normalizacyjny, Warszawa 2014.
PN-EN ISO 9000:2015-10, Systemy zarządzania jakością. Podstawy i terminologia, Polski Komitet Normalizacyjny, Warszawa 2016.
Szczepańska K., *Metody i techniki TQM*, Warszawa 2009.
Zarządzanie ryzykiem działalności organizacji, red. J. Monkiewicz, L. Gąsiorkiewicz, Warszawa 2010.

Akty prawne dotyczące oceny zgodności wyrobów i akredytacji OiB, www.wcnjk.wp.mil.pl/pl/18.html (dostęp: 20.10.2014).
ISO 9000 – Quality management, www.iso.org/iso-9001-quality-management (dostęp: 27.10.2015).
ISO Survey, www.iso.org/the-iso-survey.html (dostęp: 13.10.2014).
Norma ISO 24762, www.centrum.bezpieczenstwa.pl/index.php/standardy-othermenu-16/1064-iso-24762 (dostęp: 24.10.2014).
Standards, www.iso.org/iso/home/standards.htm (dostęp: 13.10.2014).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228).
Decyzja Rady Unii Europejskiej 2011/292/UE z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.Urz. UE 2011, L141, poz. 17 z późn. zm.).
Decyzja Komisji Europejskiej 2001/844/EC z dnia 29 listopada 2001 r. zmieniająca jej regulamin wewnętrzny (notyfikowana jako dokument nr C (2001) 3031) (Dz.Urz. UE 2001, L317, poz. 1, Polskie Wydanie Specjalne 2004, rozdz. 1, t. 3, s. 353–407).
C-M(2002)49 z dnia 17 czerwca 2002 r. – Bezpieczeństwo w ramach organizacji Traktatu Północnoatlantyckiego (z późn. zm.).

Summary

Information security is an increasing challenge for companies because market demand for information about quality is very high and still increasing. Because of the growing awareness of the possibility of loss of classified information organizations often

take radical action to ensure the safety or minimize the risk of loss of such information. As a result, more and more is being done to protect information in the following areas: personal, physical and industrial security (creating processes, groups, storing and distributing information), data (including information systems, security tools, recording items) and logistics.

The proper management of security of classified information is part of the increasing competitive advantage because it is focused on international standards. This standard includes, inter alia, the Management System according to ISO 27001.