PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 119
Informatyka Ekonomiczna 18 2010

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

RYZYKO SYSTEMÓW INFORMATYCZNYCH A ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA W ORGANIZACJI (*BUSINESS CONTINUITY MANAGEMENT*)

Streszczenie: Zarządzanie ciągłością działania to podejście do prowadzenia działalności organizacji w sposób pozwalający na utrzymanie ustalonego poziomu dostarczania produktów lub świadczenia usług, gdy mamy do czynienia z zakłóceniami procesów biznesowych w organizacji. Zapewnianie ciągłości działania jest silnie powiązane z problematyką zarządzania ryzykiem operacyjnym i zarządzania bezpieczeństwem informacji. Wszystkie te zagadnienia zaś są elementem kompleksowego zarządzania jakością w działalności organizacji, a powiązanie systemów bezpieczeństwa informacji oraz ciągłości działania jest jednym z najbardziej efektywnych sposobów wyszukiwania elementów ryzyka w działalności całej organizacji. Artykuł przedstawia tematykę zarządzania ciągłością działania w kontekście ryzyka systemów informatycznych oraz prezentuje mało znany standard zarządzania ciągłością działania BS 25999.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, ryzyko informatyczne, zarządzanie ryzykiem, zarządzanie ciągłością działania, standard BS 25999.

1. Wstęp

Metody, techniki zabezpieczeń systemów informacyjnych są przedmiotem standaryzacji zarówno przez międzynarodowe, jak i przez krajowe instytucje standaryzacyjne. Instytucje te poświęcają coraz więcej uwagi problematyce dotyczącej zarządzania ryzykiem, a szczególnie ryzykiem związanym z funkcjonowaniem systemów informatycznych w organizacjach. Widoczna jest również pewna tendencja, objawiająca się tym, że kwestie związane z bezpieczeństwem systemów informatycznych, które jeszcze niedawno były traktowane niezależnie, rozpatrywane są coraz częściej w kontekście kompleksowego procesu zarządzania ryzykiem. Jedną z podstawowych norm związanych z zarządzaniem bezpieczeństwem systemu informacyjnego jest standard ISO/IEC 17799 (por. [PN-ISO/IEC-17799:2007…]). W roku 2000 zalecenia brytyjskie BS 7799, opublikowane w „Code of Practice for

Information Security Management", zostały poddane normalizacji przez ISO oraz IEC. Wynikiem tych prac jest norma o nazwie „Praktyczne zasady zarządzania bezpieczeństwem informacji". Innym wiodącym standardem w dziedzinie zarządzania ryzykiem jest raport techniczny – ISO/IEC TR 13335, określany mianem *Guidelines for the Management of IT Security*, który składa się z pięciu zasadniczych części. W odniesieniu do systemów informatycznych proces zarządzania ryzykiem najpełniej opisany jest w części trzeciej – „Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych". Obecnie w dziedzinie szeroko rozumianego bezpieczeństwa teleinformatycznego największą popularność ma norma ISO/IEC 27001 oraz standard *Common Criteria* (w zakresie oceny i wytycznych do budowy bezpiecznych systemów informatycznych). Coraz częściej, obok powyższych standardów dotyczących problematyki zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych, pojawiają się standardy i zalecenia odnoszące się do zbliżonej problematyki zarządzania ciągłością działania. Ciągłość działania to zdolność organizacji do takiego reagowania na zakłócenia warunków zwyczajnego funkcjonowania, aby tam, gdzie to możliwe, szybko przywrócić te normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań [Staniec, Zawiła-Niedźwiecki 2008, s. 261]. Niniejszy artykuł ma na celu przedstawienie problematyki zarządzania ciągłością działania w kontekście ryzyka systemów informatycznych oraz zaprezentowanie nieco mniej znanego standardu BS 25999.

2. Zarządzanie ciągłością działania w organizacji

Zarządzanie ciągłością działania (*Business Continuity Management* – BCM) to podejście do prowadzenia działalności gospodarczej w sposób pozwalający na utrzymanie określonego poziomu dostarczania produktów lub świadczenia usług w przypadku wystąpienia istotnych zakłóceń w funkcjonowaniu procesów organizacji. Istotną przesłanką stanowiącą o potrzebie odpowiedniego podejścia do problematyki zarządzania ciągłością działania (ZCD) są nie tylko wymogi wynikające z regulacji prawnych, ale przede wszystkim fakt, że kontrolowanie ryzyka i umiejętne planowanie ciągłości funkcjonowania organizacji wpływają pozytywnie na wartość organizacji, wizerunek i możliwość osiągania zakładanych celów. Ogólnie mówiąc, zarządzanie ciągłością działania polega na identyfikacji zagrożeń dla funkcjonowania organizacji i na opracowaniu sposobów postępowania w przypadku wystąpienia zdarzeń, które mogą zakłócić to funkcjonowanie (opracowanie planów awaryjnych, wdrożenie środków technicznych, zastosowanie zabezpieczeń informatycznych oraz rozwiązań organizacyjnych) [DGA – doradca bezpieczeństwa…].

Zarządzanie ciągłością działania musi być oparte na potrzebach i możliwościach organizacji, w której ma być wdrożone. Dlatego też jego implementacja jest procesem złożonym z wielu etapów, spośród których najważniejsze to faza analizy

organizacji, budowy koncepcji, realizacji i testów. Mimo że jest to proces skomplikowany, to efektywne wdrożenie koncepcji zarządzania ciągłością działania pozwala na [Janas, Perłowski 2007]:

- zidentyfikowanie ryzyka i zarządzanie nim,
- zidentyfikowanie oraz uświadomienie sobie słabych i mocnych stron w przedsiębiorstwie,
- możliwie szybkie i skuteczne reagowanie na przerwy w dostarczaniu usług dla klientów,
- uzyskanie konkurencyjnej przewagi w postaci zdolności utrzymywania obsługi klientów,
- wdrożenie procesu zarządzania incydentami.

Efektem wdrożenia systemu zarządzania ciągłością działania powinien być m.in. odpowiedni plan ciągłości działania (*Business Continuity Plan*), określający zestaw procedur, przepisów, dokumentów, które będą wskazywać zasady postępowania w razie nieoczekiwanego wystąpienia zakłócenia normalnej działalności organizacji [Janas, Perłowski 2007].

Plany ciągłości działania są zatem bardzo ważnym elementem zarządzania ciągłością działania. Proces ten, wraz z planami ciągłości działania, powinien być obecny w każdej organizacji, w której jakikolwiek przestój może się okazać fatalny w skutkach, poprzez np. generowanie znacznych strat. Plany ciągłości działania dla systemów informatycznych identyfikują ścieżki dla poszczególnych systemów, które warunkują prawidłowe działanie, wskazują osoby odpowiedzialne za ich uruchomienie i realizację, zawierają opisy procedur, które muszą być wykonane, by przywrócić dostępność danych i możliwość funkcjonowania procesów (np. częstotliwość, sposoby i narzędzia archiwizacji) [Janas, Perłowski 2007]. Ważną częścią planu ciągłości działania jest plan odtwarzania utraconych zasobów (*Disaster Recovery Plan* – DRP), który składa się, ogólnie rzecz biorąc, z procedur postępowania w wypadku zdarzenia losowego lub krytycznej awarii, w wyniku której procesy w organizacji zostają przerwane, a zasoby i dane utracone.

Przedsiębiorstwa nastawione na zbudowanie organizacji odpornej na większość zidentyfikowanych potencjalnych rodzajów ryzyka, które w konsekwencji mogą prowadzić do utraty zdolności funkcjonowania organizacji, mogą wdrożyć standard zarządzania ciągłością działania BS 25999.

3. Standard zarządzania ciągłością działania – BS 25999

Jak już wspomniano, zarządzanie ciągłością działania to podejście do prowadzenia działalności organizacji w sposób pozwalający na utrzymanie ustalonego poziomu dostarczania produktów lub świadczenia usług w przypadku wystąpienia pewnych zaburzeń w normalnym funkcjonowaniu procesów w organizacji. Takie nieprzerwane działanie w przypadku zakłóceń, czy to wielkiej katastrofy, czy małego in-

cydentu, jest w dzisiejszych czasach podstawowym wymogiem niemal dla każdej organizacji. BS 25999 to pierwsza na świecie brytyjska norma zarządzania ciągłością działania opracowana w celu zminimalizowania ryzyka takich zakłóceń [BSI Management Systems…].

Seria standardów o symbolu BS 25999 została opracowana w 2007 r. przez BSI (British Standards Institution) – najstarszą na świecie instytucję zajmująca się tworzeniem norm i standardów, uznawaną za jedną z ważniejszych organizacji w zakresie normalizacji i certyfikacji. Wspomniana seria standardów dotyczy obszaru zarządzania ciągłością działania w organizacji i wprowadza systemowe podejście do tego zagadnienia w oparciu o dobre praktyki. BS 25999 został opracowany przez specjalistów, zarówno teoretyków, jak i praktyków z różnych krajów, na bazie badań akademickich, a także doświadczeń praktycznych w zarządzaniu ciągłością działania. Standard zastąpił funkcjonującą wcześniej specyfikację PAS-56, która została jednocześnie wycofana [DGA – doradca bezpieczeństwa…]. Specyfikacja PAS-56 zawierała również zbiór wytycznych do zarządzania ciągłością działania, opisując działania i rezultaty związane z ustanowieniem procesu zarządzania ciągłością działania, przedstawiała dobre praktyki oraz określała kryteria oceny. Był to pierwszy dokument w Wielkiej Brytanii, definiujący pojęcie *Business Continuity Management* oraz wyszczególniający podstawowe obszary, procesy i terminologię związane właśnie z ideą utrzymania ciągłości działania [Kaczmarek, Ćwiek 2009, s. 37]. Norma BS 25999 składa się z dwóch zasadniczych standardów. Pierwszy z nich, mający oznaczenie BS 25999-1, nosi nazwę pomocniczą „Code of Practice" (kodeks praktyk) i jest zbiorem wytycznych, które wprowadzają procesy, zasady, a przede wszystkim niezbędną terminologię [BS 25999-1: 2006…; Kaczmarek, Ćwiek 2009, s. 37-38]. Druga norma, o symbolu BS 25999-2, nosi nazwę „Specification for Business Continuity Management" (specyfikacja dla zarządzania ciągłością działania) jest standardem, określającym wymagania do wdrożenia środków kontroli ciągłości działania, na podstawie których może być przyznany certyfikat zgodności [BS 25999-2: 2007…; Kaczmarek, Ćwiek 2009, s. 38].

Celem tego standardu jest zbudowanie pojedynczego źródła informacji pozwalającego zidentyfikować środki kontroli, które, zgodnie z praktyką, są niezbędne do zarządzania ciągłością działania. Jego układ jest zbliżony do innych norm dotyczących systemów zarządzania i podobnie jak w przypadku wielu innych standardów, sformułowane w nim wymagania zostały opracowane w sposób pozwalający na zastosowanie go w organizacjach o różnym charakterze, profilu działalności oraz wielkości. Wobec tego może on być stosowany przez organizacje każdej wielkości w sektorach przemysłowym, handlowym, publicznym, a także w instytucjach *non-profit* [BSI Management Systems…; *Centrum bezpieczeństwa:* BS 25999…; Liderman 2009]. Szczególnie zaś dotyczy organizacji, które działają w środowiskach obciążonych wysokim ryzykiem, takich jak branża finansowa, telekomunikacja,

logistyka czy też sektor publiczny, w których ciągłość realizacji operacji ma kluczowe znaczenie dla samej organizacji, dla jej partnerów biznesowych i klientów.

Omawiany standard definiuje wymagania związane z funkcjonowaniem systemu zarządzania ciągłością działania w organizacji. Wymagania te zostały określone w stosunku do ustanowienia, wdrożenia, eksploatacji, przeglądu, testowania, utrzymania i doskonalenia systemu zarządzania ciągłością działania (*Business Continuity Management System* – BCMS), który może funkcjonować w ramach kompleksowego zarządzania ryzykiem działalności organizacji [*Centrum bezpieczeństwa:* BS 25999-2…]. Ryzyko związane z szerokim zastosowaniem technologii informatycznych w biznesie rośnie wraz ze zwiększaniem się współzależności organizacji od jej klientów, partnerów biznesowych i operacji zlecanych na zewnątrz. Standard ten natomiast może stanowić podstawę dla zrozumienia, rozwoju i wdrożenia ciągłości działania w organizacji i może dawać pewność w relacjach z innymi firmami i z klientami. Obejmuje on też wszechstronny zestaw narzędzi kontroli opartych na najlepszych praktykach, które można stosować w całym cyklu procesu zarządzania ciągłością działania w organizacji.

Pierwsza część normy o symbolu BS 25999-1:2006 koncentruje się na następujących kwestiach i problemach [BS 25999-1: 2006…]:

- polityka zarządzania ciągłością działania definiująca cele kierownictwa,
- proces zarządzania ciągłością funkcjonowania organizacji zapewniający systemowe podejście,
- analiza działalności przez pryzmat ryzyka,
- strategia zarządzania ciągłością działania jako odpowiedź na istniejące rodzaje ryzyka,
- opracowanie i wdrożenie środków ochrony (m.in. BCP – *Business Continuity Planning*, DRP – *Disaster Recovery Plan*) wynikających z realizacji strategii,
- testowanie, zarządzanie i przegląd środków ochrony – zarówno technicznych, jak i organizacyjnych (przede wszystkim planów awaryjnych),
- budowa świadomości pracowników i podmiotów współpracujących z organizacją.

Natomiast druga część standardu, opisana symbolem BS 25999-2:2007, porusza następujące obszary i zagadnienia [BS 25999-2:2007…]:

- terminy i definicje,
- planowanie systemu zarządzania ciągłością biznesu (BCMS),
- wdrażanie i eksploatowanie systemu BCMS – standard charakteryzuje te procesy jako składające się z następujących działań:
- poznanie organizacji,
- analiza wpływu na działalność biznesową,
- szacowanie ryzyka,
- określanie opcji postępowania z ryzykiem,
- określanie strategii ciągłości biznesu,
- opracowywanie i wdrażanie odpowiedzi na zdarzenia BCM,

– testowanie, utrzymywanie i przeglądanie planów BCM,
– monitorowanie i przegląd systemu BCMS,
– utrzymywanie i doskonalenie systemu BCMS.

Korzyści wynikające ze stosowania normy BS 25999 mają bardzo szeroki zasięg i obejmują m.in. trzy zasadnicze obszary [BSI Management Systems…]:
– elastyczność – zapewnia aktywną poprawę elastyczności organizacji w zakresie realizowania podstawowych celów w obliczu zakłóceń,
– dostarczanie – zapewnia sprawdzoną metodę przywracania dostarczania najważniejszych produktów i realizacji istotnych usług do ustalonego poziomu oraz w określonym czasie po zaistnieniu zakłócenia,
– zarządzanie – zapewnia sprawdzoną zdolność zarządzania zakłóceniami oraz ochrony reputacji i marki firmy.

Aktualnie BS 25999 jest formalnie standardem brytyjskim, może być jednak stosowany na skalę międzynarodową. Prawdopodobnie w niedługim czasie organizacja ISO rozpocznie prace nad wprowadzeniem międzynarodowego odpowiednika tej normy. Podobną ścieżkę zastosowano w przypadku systemu bezpieczeństwa (oryginalna norma BS 7799 została przyjęta jako międzynarodowy standard ISO/IEC 17799, a kolejno rozszerzona, zaktualizowana oraz opublikowana jako ISO/IEC 27001) [PN-ISO/IEC 27001:2007…; PN-ISO/IEC-17799:2007…]. Omawiany standard jest jedną z nowszych norm z rodziny systemów zarządzania, nic więc dziwnego, że idealnie uzupełnia wymagania systemów jakości usług IT (ISO/IEC 20000) oraz bezpieczeństwa informacji (ISO/IEC 27001) (por. [PN-ISO/IEC 27001:2007…]).

4. Zarządzanie ciągłością działania jako element zarządzania ryzykiem na potrzeby bezpieczeństwa informacji

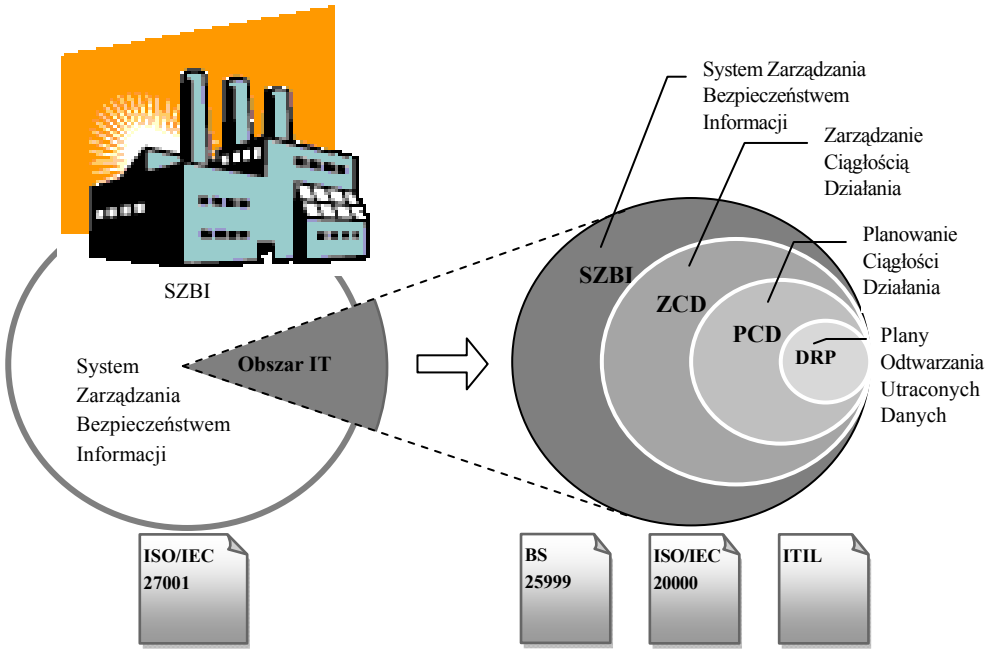
Często się zdarza, że nieprzewidziane wstrzymanie działalności firmy spowodowane jest poprzez nieuprawnione modyfikacje informacji, a szczególnie awarie infrastruktury informatycznej. Ale zagrożenia informacji w działalności gospodarczej wynikają nie tylko z możliwości kradzieży, nieuprawnionych modyfikacji danych przez pracowników firmy czy awarii systemów informatycznych. Ryzyko tego typu incydentów zawsze będzie istniało, nawet mimo skutecznego systemu zarządzania bezpieczeństwem informacji, ponieważ nie istnieje możliwość zagwarantowania stuprocentowego bezpieczeństwa informacji i systemów w organizacji. Czasami, mimo odpowiedniego podejścia do problematyki zarządzania bezpieczeństwem w przedsiębiorstwie, może dojść do wypadku, który doprowadzi do przerwania ciągłości działania firmy. Następstwem tego mogą być poważne straty, a w skrajnych przypadkach nawet bankructwo. W ciągu ostatnich lat na całym świecie wiele przedsiębiorstw straciło miliardy dolarów z powodu wystąpienia różnych nieprzewidzianych sytuacji mających znaczny wpływ na dalszą działalność bizne-

sową [Polaczek]. Z badań DTI Information Security Breaches Survey (2006) wynika, że najgorszym skutkiem naruszeń bezpieczeństwa jest właśnie przerwanie ciągłości działania. Z badania tego wynika również, że 22% organizacji doświadczyło przerwania ciągłości działania na ponad jeden dzień, a 3% na ponad tydzień [Witryna firmy ISecMan…].

Ciągłość działania jest postulatem doskonałości systemu działania, jakim jest każda firma. W tym znaczeniu zapewnianie ciągłości działania jest przedmiotem zarządzania strategicznego, określającym cel nadrzędny sprawności organizacji i zajmującym istotne miejsce w obszarze zarządzania ryzykiem w organizacji, także ryzykiem informatycznym. Ciągłość działania jest rozumiana jako działanie tworzące zdolność organizacji do skutecznego reagowania w sytuacji zaistnienia zakłócenia jako wyniku swoistej interakcji przejawów zagrożenia z podatnością organizacji wewnętrznej, infrastruktury lub zasobów. W tym sensie zapewnianie ciągłości działania jest elementem zarządzania IT i stanowi ważny element systemu bezpieczeństwa, jako ogniwo zarządzania ryzykiem informatycznym [Staniec, Zawiła-Niedźwiecki 2008, s. 261].

Organizacje, które uzyskały certyfikat systemu zarządzania jakością lub bezpieczeństwa informacji, lub wdrożyły podobne rozwiązania standaryzacyjne w obszarze ryzyka i bezpieczeństwa systemów informatycznych, niewątpliwie będą miały łatwiejszą drogę przy implementacji standardu BS 25999. Jak już bowiem podkreślono, standard ten uzupełnia system zarządzania bezpieczeństwem informacji oraz system zarządzania usługami IT w przedsiębiorstwie, a samo zarządzanie ciągłością działania traktowane jest jako integralna część systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacji.

Wdrożenie systemu zarządzania bezpieczeństwem informacji i systemu zarządzania ciągłością działania można traktować jako istotny element procesu doskonalenia organizacji pod względem zarządzania informacją. W obszarze IT, jak i w innych sferach funkcjonowania przedsiębiorstw, warto korzystać ze światowych standardów, norm, zaleceń i dobrych praktyk w tym zakresie. W obszarze IT warto przypomnieć o takich normach, jak wspomniany już standard zarządzania systemem bezpieczeństwa informacji ISO/IEC 27001 czy obecnie jedyna oficjalna norma w obszarze zarządzania usługami informatycznymi – ISO/IEC 20000 [Janas, Perłowski 2007]. Najlepsze praktyki i zalecenia są również zebrane i opisane w takich standardach, jak ITIL, COBIT, czy w metodyce Six Sigma. Interesujące z punktu rozważań podjętych w niniejszym artykule jest zagadnienie integracji metodyki Six Sigma i standardu ITIL, gdyż np. narzędzia Six Sigma, takie jak FMEA (Failure Mode and Effect Analysis), mogą być wykorzystywane przy wykonywaniu analizy ryzyka w wielu procesach zdefiniowanych w normie ITIL [Janas, Perłowski 2007]. Relacje pomiędzy systemem zarządzania bezpieczeństwem informacji a zarządzaniem ciągłością działania, planami ciągłości działania zostały przedstawione na rys. 1.



Rys. 1. Zarządzanie bezpieczeństwem informacji w organizacji ze szczególnym uwzględnieniem systemu zarządzania ciągłością działania

Źródło: opracowanie własne na podstawie [Janas, Perłowski 2007].

Najpopularniejsza i najczęściej wdrażana obecnie norma w zakresie bezpieczeństwa systemów informatycznych – ISO/IEC 27001 – obejmuje całość zagadnień związanych z ochroną tworzonych, przechowywanych oraz przetwarzanych informacji w organizacji, a jej istotna część dotyczy ciągłości działania. Jej zalecenia nie odnoszą się do określonej platformy technologicznej, co umożliwia ich uniwersalne zastosowanie. Ponadto bezpieczeństwo informacji już od dawna nie jest utożsamiane wyłącznie z obszarem IT. W normie ISO/IEC 27001 wyróżniono jedenaście obszarów mających wpływ na bezpieczeństwo informacji w organizacji. Są to [PN-ISO/IEC 27001:2007…]:

- polityka bezpieczeństwa,
- organizacja bezpieczeństwa informacji,
- zarządzanie aktywami,
- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrola dostępu,
- zarządzanie ciągłością działania,

– pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
– zarządzanie incydentami związanymi z bezpieczeństwem informacji,
– zgodność z wymaganiami prawnymi i własnymi standardami.

Załącznik A omawianej normy ISO/IEC 27001 (cele stosowania zabezpieczeń i zabezpieczenia) wymienia właśnie zarządzanie ciągłością działania jako jedno z obligatoryjnych działań. Załącznik ten jest normatywny, czyli jego wymagania muszą być spełnione. Jak wspomniano i podkreślano wcześniej, zarządzanie ciągłością działania może być też traktowane jako jeden z elementów systemu zarządzania bezpieczeństwem. W załączniku tym punkt A14 porusza następujące zagadnienia z tego obszaru [PN-ISO/IEC 27001:2007…]:

A.14 Zarządzanie ciągłością działania

A.14.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania

A.14.1.1 Włączenie bezpieczeństwa informacji do procesu zarządzania ciągłością działania

A.14.1.2 Ciągłość działania i analiza skutków dla działalności biznesowej

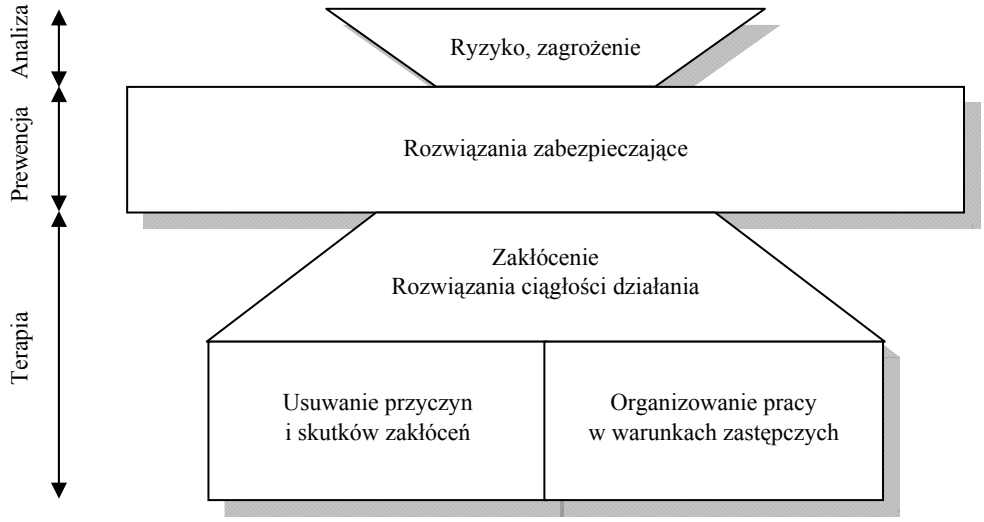
A.14.1.3 Opracowanie i wdrażanie planów ciągłości uwzględniających bezpieczeństwo informacji

A.14.1.4 Struktura planowania ciągłości działania

A.14.1.5 Testowanie, utrzymywanie i ponowna ocena planów ciągłości działania

Norma definiuje podstawowy cel stosowania powyższych zabezpieczeń jako: „przeciwdziałanie przerwom w działalności biznesowej oraz ochrona krytycznych procesów biznesowych przed rozległymi awariami systemów informacyjnych lub katastrofami, a także zapewnienie wznowienia działalności w wymaganym czasie" (ISO/IEC 27001). Zatem z powyższych rozważań wynika, że oba standardy ISO/IEC 27001 i BS 25999 uzupełniają się wzajemnie, a obszary zarządzania bezpieczeństwem systemów informatycznych i związanego z nim ryzyka oraz zarządzania ciągłością działania są ściśle ze sobą powiązane i dotyczą podobnych działań. Relacje pomiędzy zadaniami zapewniającymi bezpieczeństwo i ciągłość działania w organizacji przedstawiono na rys. 2.

Należy także podkreślić, że reagowanie na zakłócenia, jako zapewnianie ciągłości działania, należy rozumieć nie tylko jako bezpośrednie postępowanie wobec zakłóceń, ale także jako aktywność o charakterze prewencyjnym, związaną z analizą zagrożeń i podatności na nie oraz z poszukiwaniem metod i rozwiązań dotyczących zapobiegania zaistnieniu zakłóceń. W tym sensie starania o ciągłość działania i bezpieczeństwo splatają się. Z punktu widzenia ciągłości działania rozwiązania bezpieczeństwa zapewniają prewencję wobec zagrożeń, z punktu widzenia bezpieczeństwa zaś rozwiązania ciągłości działania stanowią dodatkowe zabezpieczenie, gdy zawodzą wdrożone i zastosowane rozwiązania bezpieczeństwa (zob. rys. 2). Uzasadnia to koncepcję zintegrowanego podejścia do obu zagadnień oraz wspólnego zarządzania obydwoma zagadnieniami, a podobnie i zarządzaniem jakością, co jest pośrednio rekomendowane m.in. przez normy ISO serii 9000, 14000 oraz standardy omówionej w artykule serii ISO/IEC 27000 [Staniec, Zawiła-Niedźwiecki 2008, s. 262].



Rys. 2. Relacje zadań zapewnienia bezpieczeństwa i ciągłości działania w organizacji

Źródło: [Staniec, Zawiła-Niedźwiecki 2008, s. 262].

Powiązań i podobieństw między oboma obszarami jest jeszcze więcej. Mianowicie, jak już wskazywano w artykule, standard BS 25999 określa wymagania dla systemów zarządzania ciągłością działania – ustanowienia, wdrożenia, eksploatacji, przeglądu, testowania, utrzymania i doskonalenia dokumentowanego systemu zarządzania ciągłością w kontekście kompleksowego zarządzania ryzykiem. Pokazuje przede wszystkim związki z lansowanym przez instytucję BSI tzw. cyklem Deminga (PDCA – *plan*, *do*, *check*, *act*) stanowiącym model dla systemu zarządzania bezpieczeństwem informacji, opisanym właśnie w normach ISO/IEC 19977 oraz ISO/IEC 27001 [Liderman 2009].

5. Podsumowanie

Wdrożenie procesu zarządzania ciągłością działania ma na celu zabezpieczenie organizacji m.in. przed utratą cennych danych, a dzięki temu – przed ryzykiem wstrzymania działalności biznesowej. Podsumowując, jeśli organizacja chce ominąć nieprzewidziane przypadki zaprzestania działalności spowodowane np. kradzieżą informacji czy awarią infrastruktury informatycznej, musi podejść poważnie do zagadnienia związanego ze stworzeniem planu ciągłości działania. Oczywiście plan taki jest, jak wskazano w artykule, integralną częścią wdrożenia systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 27001.

Literatura

BS 25999-1: 2006: Business continuity management. Code of practice.
BS 25999-2: 2007: Specification for business continuity management.
BSI Management Systems Polska Sp. z o.o.: BS 25999 – Ciągłość biznesowa http://www.bsigroup.pl/pl/Auditowanie-i-certyfikacja/Systemy-zarzadzania/Normy-i-programy/BS-25999/.
Centrum bezpieczeństwa: BS 25999-2 http://centrum.bezpieczenstwa.pl/content/view/1046/16/.
Centrum bezpieczeństwa: BS 25999 http://centrum.bezpieczenstwa.pl/content/view/348/16/.
DGA – doradca bezpieczeństwa: *Zarządzanie ciągłością działania* (*BS 25999*) http://security.dga.pl/page.php?13.
Janas B., Perłowski W., *Od planów ciągłości działania do bezpieczeństwa informacji*, Akademia Wiedzy BCC, http://lepszybiznes.org/pad_files/aw_files/366_AW_SZBI_20070831.pdf, 2007.
Kaczmarek T.T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania*, Wydawnictwo Difin, Warszawa 2009.
Liderman K., *Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego*, [w:] Biuletyn Instytutu Automatyki i Robotyki WAT nr 26/2009, Warszawa 2009.
PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.
PN-ISO/IEC-17799:2007: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*.
Polaczek T., *Business Continuity & Disaster Recorvery* http://www.outsourcing.com.pl/888,zarzadzanie_ciagloscia_dzialania_organizacji_w_sytuacji_krytycznej.html.
Staniec I., Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym*, C.H. Beck, Warszawa 2008.
Witryna firmy ISecMan – *Zarządzanie ciągłością działania*, http://isecman.org/wydarzenia/258-BCM___Zarzadzanie.

INFORMATION SYSTEMS SECURITY RISK AND BUSINESS CONTINUITY MANAGEMENT IN AN ORGANIZATION

Summary: Business Continuity Management is an approach to business, which allows to maintain the agreed level of products or services supply, when the organization has to deal with the disruption of business processes. Ensuring business continuity is closely linked to the issues of operational risk management and information security management. All these issues are a part of a complex quality management system in the organization. Information security and business continuity systems are one of the most effective ways to find the elements of risk in the entire organization. This article discusses the problem of business continuity management in the context of information systems security risks and presents a less well known business continuity management standard – BS 25999.