INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 22 • 2011

ISSN 1507-3858

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

WYBRANE ZAGADNIENIA ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA W ASPEKCIE BEZPIECZEŃSTWA USŁUG I SYSTEMÓW INFORMATYCZNYCH

Streszczenie: Zarządzanie ciągłością działania (BCM) polega na opracowaniu rozwiązań i procedur umożliwiających takie działanie w sytuacji kryzysowej, które pozwoli na utrzymanie funkcjonowania najważniejszych procesów biznesowych na minimalnym akceptowalnym poziomie. Rozwiązania te są ściśle związane z zapewnieniem nieprzerwanych działań na płaszczyźnie IT. Artykuł przedstawia problematykę BCM w kontekście bezpieczeństwa systemów informatycznych, prezentuje standard BS 25999 oraz normę BS 25777, wspomagającą planowanie, organizację i wdrażanie strategii ciągłości funkcjonowania technologii informacyjno-komunikacyjnych. Przedstawia również informatyczną platformę BCMLogic, która stanowi rozwiązanie wspomagające procesy planowania i zarządzania incydentami oraz sytuacjami awaryjnymi w firmie.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, ryzyko informatyczne, zarządzanie ciągłością działania, standardy BS 25999 i BS 25777, Platforma BCMLogic.

1. Wstęp

Zarządzanie ciągłością działania (*Business Continuity Management* – BCM) to podejście do prowadzenia działalności organizacji w sposób pozwalający na utrzymanie ustalonego poziomu dostarczania produktów lub świadczenia usług, w sytuacji gdy mamy do czynienia z zakłóceniami procesów biznesowych. Skuteczna realizacja tego procesu zależy w dużej mierze od ciągłości funkcjonowania technologii komunikacyjno-informacyjnych w organizacji. Proces zarządzania ciągłością działania ma na celu zabezpieczenie organizacji m.in. przed utratą cennych danych, a dzięki temu – przed niebezpieczeństwem przerwania działalności biznesowej. Działania te minimalizują czas i energię niezbędne do odtworzenia utraconych danych, przywrócenia prawidłowych procesów biznesowych, umożliwiają one także minimalizację ryzyka utraty strategicznych aktywów oraz pomagają uniknąć konsekwencji prawnych i ekonomicznych wynikających np. z niedotrzymania zobo-

wiązań wobec partnerów biznesowych. Zapewnianie ciągłości działania jest silnie powiązane z problematyką zarządzania ryzykiem operacyjnym i zarządzania bezpieczeństwem informacji. Wszystkie te zagadnienia są zaś 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. Postępująca bardzo dynamicznie informatyzacja życia i procesów gospodarczych sprawia, że ciągłość działania organizacji kojarzona, wręcz utożsamiana jest z dostępem do zasobów informatycznych. W tym kontekście zagadnienia BCM ściśle związane są z zapewnieniem nieprzerwanych działań na płaszczyźnie technologii informacyjnych.

Celem niniejszego artykułu jest wprowadzenie do problematyki zarządzania ciągłością działania w kontekście bezpieczeństwa systemów informatycznych i zarządzania ryzykiem oraz prezentacja wybranych dobrych praktyk i standardów w tym obszarze. Ostatnią część niniejszego artykułu stanowi prezentacja platformy BCMLogic, informatycznego narzędzia wspierającego planowanie i zarządzanie incydentami oraz sytuacjami awaryjnymi w organizacji.

2. System pojęciowy ryzyka, bezpieczeństwa i ciągłości działania

Ryzyko

Na temat pojęcia ryzyka i jego różnorodnych kwalifikacji napisano już wiele. Ryzyko jest mieszaniną wielu wciąż zmieniających się czynników, dlatego ani praktycy, ani teoretycy nie podają jednej uniwersalnej definicji, stąd też istnieje ich wiele. W literaturze podkreśla się, że jest to termin wieloznaczny i trudny do syntetycznego zdefiniowania. Jak pisze W. Ostasiewicz [2004], intuicyjny sens tego pojęcia jest oczywisty i jest to coś, co może się zdarzyć, a czego nie chcemy lub czego się boimy. Autor jednocześnie podaje definicję tego terminu, określając ryzyko jako niechciane, niepewne zdarzenie, i traktuje je jako możliwość niepewnej straty, którą jest najczęściej strata finansowa [Ostasiewicz 2004, s. 11]. Ryzyko jest definiowane na bazie różnych nauk i teorii, m.in. w ekonomii, naukach behawioralnych, naukach prawnych, psychologii, statystyce, ubezpieczeniach, teorii prawdopodobieństwa i wielu innych. Nauka o ryzyku jest praktycznie rozwijana w większości nauk i stosowana we wszystkich technologiach. W zależności od autora i charakteru opracowania, czy też ze względu na różną perspektywę przedmiotową, branżową czy dyscyplinarną, uzyskujemy różne sposoby ujmowania zagadnień związanych z ryzykiem.

A. Winegard i S. Warhoe [2003] określają ryzyko jako iloczyn prawdopodobieństwa wystąpienia czynnika negatywnego oraz jego wpływ na przedsięwzięcie. Tak zdefiniowane ryzyko można opisać wzorem:

$$R = p \times c\,, \tag{1}$$

gdzie: p – prawdopodobieństwo wystąpienia czynnika ryzyka,
c – konsekwencja dla przedsięwzięcia (dokładnie dla jego czasu lub kosztu realizacji) wystąpienia tego czynnika.

Problematyka ryzyka podejmowana jest w technice, a zwłaszcza w diagnostyce technicznej. Według normy IEC 61508, będącej zasadniczym międzynarodowym standardem odnoszącym się do systemów związanych z bezpieczeństwem, składających się ze składników elektrycznych lub elektronicznych, pojęcie ryzyka związane jest z terminem hazardu: „ryzyko jest miarą stopnia zagrożenia, wyrażającą zarówno stopień szkodliwości hazardu, jak i prawdopodobieństwo jego wystąpienia". Natomiast ogólna definicja hazardu mówi, że jest to „ryzykowne przedsięwzięcie, którego wynik zależy wyłącznie od przypadku, także narażanie się na niebezpieczeństwo".

W inżynierii i naukach społecznych ryzyko mierzy się jako własność zdarzenia, np. uszkodzenia aparatury i miary wartości szkody spowodowanej przez to zdarzenie. W tym sensie ryzyko nie zależy od tego, kto podejmuje decyzje, a sposób jego oszacowania wynika z zaakceptowanych stałych norm, przyjętych także w biznesie.

W kontekście bezpieczeństwa systemów informatycznych ryzyko najczęściej jest traktowane jako zbiorcza miara prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu, a zatem pośrednią lub bezpośrednią szkodę dla organizacji.

Istnieje wiele innych standardów regulujących tę tematykę. I tak na przykład międzynarodowy ISO/IEC TR 13335 zawiera wskazówki, od czego zależy wielkość ryzyka związanego z bezpieczeństwem systemów informatycznych: „... ryzyko jest funkcją wartości zasobów objętych ryzykiem, możliwości wystąpienia zagrożeń, łatwości wykorzystania podatności przez zagrożenia oraz istniejących (lub planowanych, gdy szacuje się ryzyko dla projektowanych systemów bezpieczeństwa) zabezpieczeń mogących zredukować ryzyko" [PN-ISO-13335; Liderman 2008, s. 70]. Natomiast zgodnie ze wspomnianą normą ISO/IEC TR 13335 zarządzanie ryzykiem jest rozumiane jako całkowity proces identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego [PN-ISO-13335].

Bezpieczeństwo systemów informatycznych

Terminologia związana z bezpieczeństwem informacji jest ciągle modyfikowana ze względu na bardzo dynamiczne zmiany w tej problematyce. W pracy Stokłosy, Bilskiego i Pankowskiego stwierdza się, że **bezpieczeństwo informacji** „polega na ich ochronie, czyli zabezpieczeniu przed nieuprawnionym lub nieprawidłowym, przypadkowym bądź umyślnym ujawnieniem, modyfikacją lub zniszczeniem" [Stokłosa i in. 2001, s. 17]. Zgodnie z definicją zawartą w normie ISO/IEC 27001:2007 bezpieczeństwo informacji odnosi się do zachowania podstawowych jej atrybutów:

- **dostępność** (*availability*) – zapewnienie dostępu do informacji na żądanie upoważnionego podmiotu,
- **poufność** (*security*) – zapewnienie, że informacja nie jest udostępniana ani ujawniana nieupoważnionym osobom bądź podmiotom,
- **integralność** (*integrity*) – zapewnienie dokładności i kompletności informacji,
- **niezawodność** (*reliability*) to właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

Ciągłość działania

W powyższej części artykułu zostały omówione terminy i zagadnienia związane z ryzykiem i bezpieczeństwem systemów informatycznych. Pod koniec XX wieku pojawiła się koncepcja zintegrowanego zarządzania ryzykiem, natomiast aktualnie podejście do zarządzania ryzykiem ewoluuje w stronę zapewnienia ciągłości działania [Monkiewicz 2010, s. 64; Zapłata, Kaźmierczak 2011, s. 93]. U podstaw koncepcji ciągłości działania znajduje się inżynierskie podejście do niezawodności procesów produkcyjnych [Zawiła-Niedźwiecki 2007, s. 16; Zapłata, Kaźmierczak 2011, s. 94]. W pracy [Zapłata, Kaźmierczak 2011, s. 104] ciągłość działania definiowana jest jako „strategiczna i taktyczna zdolność organizacji do przewidywania zdarzeń i zakłóceń oraz do reagowania na nie w celu kontynuowania działalności na akceptowalnym, zdefiniowanym poziomie".

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 wpływa pozytywnie na wartość organizacji, wizerunek i możliwość osiągania zaplanowanych celów.

3. Zarządzanie ciągłością działania w organizacji

Zarządzanie ciągłością działania 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. Ogólnie mówiąc, zarządzanie ciągłością działania polega na identyfikacji zagrożeń dla funkcjonowania organizacji i na opracowaniu sposobów postępowania w wypadku wystąpienia zdarzeń, które mogą zakłócić to funkcjonowanie (opracowanie planów awaryjnych, wdrożenie środków technicznych, zastosowanie zabezpieczeń informatycznych oraz rozwiązań organizacyjnych) (http://security.dga.pl/page.php?13).

Zarządzanie ciągłością działania musi być oparte na potrzebach i możliwościach organizacji, w której ma być wdrożone. Dlatego też jego implementacja jest procesem złożonym, składającym się z wielu etapów, spośród których najważniejsze to faza analizy organizacji, budowy koncepcji, realizacji i testów. Pomimo 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 przewagi konkurencyjnej 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* – BCP), 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 okazać się fatalny w skutkach, np. poprzez generowanie znaczących 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 itp.) [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 zidentyfikowane potencjalne ryzyko, które w konsekwencji prowadzić może do utraty zdolności funkcjonowania organizacji, mogą wzorować się na tzw. dobrych praktykach lub dokonać wdrożenia standardów zarządzania ciągłością działania BS 25999 i normy BS 25777 zarządzania ciągłością działania technologii informacyjno-komunikacyjnych.

4. Wybrane źródła dobrych praktyk w zarządzaniu ryzykiem i ciągłością działania

Ciągłość działania jest przedmiotem wymagań stawianych przez przepisy Unii Europejskiej oraz poszczególnych jej krajów, zbiory rekomendacji branżowych oraz standardy międzynarodowe. Zapewnianie ciągłości działania początkowo trakto-

wane było łącznie z problematyką bezpieczeństwa informacji, dlatego też przewija się wraz z tamtym zagadnieniem w serii norm ISO 27000. Celem opracowania tych norm jest zebranie i ujednolicenie dotychczasowych opracowań i standardów poświęconych bezpieczeństwu informacji w organizacji i zarządzaniu ryzykiem w tym obszarze:

ISO/IEC 27000:2009 – „Technika informatyczna – Techniki bezpieczeństwa – Systemy Zarządzania Bezpieczeństwem Informacji – Omówienie i słownictwo" (*Overview and vocabulary*) – norma pomoże wszelkiego typu organizacjom zrozumieć podstawy, cele i pojęcia służące podniesieniu bezpieczeństwa ich zasobów informacyjnych.

ISO/IEC 27001:2007 – „Technika informatyczna – Techniki bezpieczeństwa – Systemy Zarządzania Bezpieczeństwem Informacji – Wymagania" (*Specification for an Information Security Management System*) – norma określa wymagania dla budowy i funkcjonowania systemów zarządzania bezpieczeństwem informacji. Standard jest specyfikacją systemów zarządzania bezpieczeństwem informacji, na zgodność z którą mogą być prowadzone audyty, będące podstawą do wydawania certyfikatów. Od stycznia 2007 r. dostępna jest również polska wersja normy PN–ISO/IEC 27001.

ISO/IEC 27002:2009 – „Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji" (*Code of Practice for Information Security Management*) – norma zawiera wytyczne do budowy systemów zarządzania bezpieczeństwem informacji. Określa ona wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem systemu zarządzania bezpieczeństwem informacji. Stanowi ona rozwinięcie normy ISO/IEC 27001.

ISO/IEC 27003:2010 – „Technika informatyczna – Techniki bezpieczeństwa – Porady i wskazówki dotyczące implementacji Systemu Zarządzania Bezpieczeństwem Informacji" (*Information Security Management System implementation guidance*) – norma będzie zawierać wytyczne do budowy systemów zarządzania bezpieczeństwem informacji pomocne przy ich implementacji.

ISO 27004:2009 – „Technika informatyczna – Techniki bezpieczeństwa – Wskaźniki i pomiar w bezpieczeństwie informacji" (*Information security management measurements*) – norma dotyczyć będzie pomiaru zarówno procesów zarządzania bezpieczeństwem, jak i poszczególnych zabezpieczeń funkcjonujących w ramach systemów zarządzania bezpieczeństwem informacji.

ISO 27005:2008 – „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem bezpieczeństwa informacji" (*Information security risk management*) – norma zawiera wytyczne dla procesu zarządzania ryzykiem. ISO/IEC 27005 nie zawiera żadnej określonej metodologii zarządzania ryzykiem, jednak standard ten ustanawia i uszczegóławia ramy procesu zarządzania ryzykiem w systemach bezpieczeństwa informacji zgodnych z ISO/IEC 27001. Można zatem sku-

tecznie zarządzać ryzykiem bezpieczeństwa informacji, wykorzystując jedną z wielu istniejących metodologii w tym zakresie, pod warunkiem że będzie ona spełniać opisane w standardzie wymagania. Wytyczne dla procesu zarządzania ryzykiem zostały opisane w siedmiu rozdziałach tego standardu, który zawiera także sześć dodatkowych załączników, przedstawiających w sposób praktyczny zawarte w normie wytyczne.

ISO/IEC 27006:2007 – „Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację Systemów Zarządzania Bezpieczeństwem Informacji" (*Requirements for bodies providing audit and certification of information security management systems*) – norma określa wymagania dla jednostek przeprowadzających audyty certyfikacyjne systemów zarządzania bezpieczeństwem informacji.

ISO/IEC 27011:2008 – „Technika informatyczna – Techniki bezpieczeństwa – Wytyczne w zakresie bezpieczeństwa informacji dla instytucji branży telekomunikacyjnej" (*Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*) – standard stanowi rozwinięcie norm ISO/IEC 27001 i ISO/IEC 27002 o wytyczne i zalecenia dla firm branży telekomunikacyjnej.

ISO/IEC TR 13335 – norma zwana GMITS (*Guidelines for the Management of IT Security*) – raport techniczny o istotnym znaczeniu dla funkcjonowania zarządzania bezpieczeństwem informacji, składający się z pięciu części. Standard zawiera wytyczne zarządzania bezpieczeństwem systemów informatycznych, opis różnych sposobów podejścia do prowadzenia analizy ryzyka, planów zabezpieczeń, roli szkoleń i działań uświadamiających, opis struktur organizacyjnych i stanowisk pracy związanych z bezpieczeństwem informacji i systemów. Zawiera również model trójpoziomowej polityki bezpieczeństwa oraz zasady reagowania na incydenty.

5. Standaryzacja zarządzania ciągłością działania – normy BS 25999 i BS 25777

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 dużej katastrofy, czy małego incydentu, jest w dzisiejszych czasach podstawowym wymogiem dla niemal każdej organizacji. BS 25999 to pierwsza na świecie brytyjska norma zarządzania ciągłością działania opracowana w celu zminimalizowania ryzyka takich incydentów (http://www.bsigroup.pl/pl/Auditowanie–i–certyfikacja/Systemy–zarzadzania/Normy–i–programy/BS–25999/).

Seria standardów o symbolu BS 25999 została opracowana w 2007 roku 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 (http://security.dga.pl/page.php?13). Zawierała ona 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 związaną właśnie z ideą utrzymania ciągłości działania [Kaczmarek 2009, s. 37]. Norma BS 25999 składa się z dwóch zasadniczych standardów. Pierwszy z nich, mający oznaczenie BS 25999-1, nosi pomocniczą nazwę *Code of Practice* (kodeks praktyk) i jest zbiorem wytycznych, które wprowadzają procesy, zasady, a przede wszystkim niezbędną terminologię [BS 25999-1: 2006; Kaczmarek 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 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 (także tych omówionych wcześniej w tym artykule), sformułowane w nim wymagania zostały opracowane w sposób pozwalający na zastosowanie go w organizacjach o różnym charakterze, profilu działalności oraz wielkości. Wobec tego może być on stosowany przez organizacje każdej wielkości w sektorach przemysłowym, handlowym, publicznym, a także w instytucjach non-profit (http://www.bsigroup.pl/pl/Auditowanie–i–certyfikacja/Systemy–zarzadzania/Normy–i–programy/BS–25999/). W szczególności dotyczy zaś 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 określo-

ne 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 (http://centrum.bezpieczenstwa.pl/content/view/1046/16/). 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 do 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 ryzyka,
- opracowanie i wdrożenie środków ochrony (m.in. BCP, DRP) 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 ciągłości działania,
- 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 (http://www.bsigroup.pl/pl/Audito wanie–i–certyfikacja/Systemy–zarzadzania/Normy–i–programy/BS–25999/):

- elastyczność – aktywna poprawa 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.

Kolejna norma – BS 25777 – wspomaga planowanie, organizację i wdrażanie strategii ciągłości funkcjonowania technologii informacyjno-komunikacyjnych (*Information and Communications Technologies* – ICT) w organizacji. Zarządzanie ciągłością działania ICT wspomaga ogólne zarządzanie procesami organizacji, zapewnia, że technologie informatyczne oraz usługi IT są elastyczne i mogą być odzyskane w terminach wymaganych i uzgodnionych z najwyższym kierownictwem. Skuteczne zarządzanie ciągłością działania zależy od ciągłości tych technologii, aby organizacja mogła osiągać swoje cele przez cały czas, szczególnie w okresach zakłóceń.

Najważniejsze korzyści płynące z odpowiedniego zarządzania ciągłością działania technologii informacyjno-komunikacyjnych w organizacji to przede wszystkim (http://www.bcpguide.com/index.php?option=com_content&view=article&id =225%3Abs–25777&catid=64%3Acertyfikacja–normy–boks–1&Itemid=96):

- zrozumienie zagrożeń i słabych punktów usług teleinformatycznych,
- identyfikacja potencjalnych wpływów zakłóceń na usługi teleinformatyczne,
- zachęcenie do lepszej współpracy między zarządcami przedsiębiorstw i dostawcami usług ICT (wewnętrznych i zewnętrznych),
- rozwijanie i wzmacnianie kompetencji pracowników branży teleinformatycznej,
- poprawa reputacji i wizerunku przedsiębiorstwa,
- możliwość wzrostu potencjalnej przewagi konkurencyjnej poprzez wykazanie zdolności do zapewnienia ciągłości działania, poprzez np. utrzymanie terminowości dostaw produktów i usług w czasie zakłóceń.

6. BCMLogic jako narzędzie zarządzania ciągłością działania IT w organizacji

Firma BCMLogic świadczy usługi w zakresie doradztwa i budowania specjalistycznych rozwiązań informatycznych dla małych, średnich i dużych przedsiębiorstw. Firma ta stworzyła platformę zarządzania działaniem procesów biznesowych, dostępnością ICT oraz ciągłością działania firmy w sytuacjach awarii. Platforma BCMLogic to informatyczne rozwiązanie funkcjonujące w modelu Cloud

Computing do planowania i zarządzania incydentami oraz sytuacjami awaryjnymi w firmie, które zapewnia przygotowanie planów zachowania ciągłości działania, integrację z istniejącymi systemami IT oraz zarządzanie ciągłością biznesu w czasie rzeczywistym z dowolnego miejsca. Jest to aplikacja w modelu SaaS (*Software as a Service*) całkowicie działająca na bazie platformy firmy Microsoft – Windows Azure. Rozpoczęcie z korzystania z aplikacji to jedynie prosta konfiguracja na stronie internetowej. Dzięki tym przyjętym rozwiązaniom technologicznym zapewniono dużą dostępność, optymalizację kosztów i wysoką skalowalność tego rozwiązania.

Usługa BCMLogic stanowi odpowiedź na podstawowe problemy związane z kompleksowością oraz efektywnością zarządzania dostępnością ICT oraz ciągłością działania biznesu. Usługi Microsoft dostępne w chmurze pozwoliły stworzyć platformę, która wszelkie zaburzenia w funkcjonowaniu ICT oraz dostępności zasobów analizuje na bieżąco. Poza tym prezentuje wizualizację w kontekście wpływu na biznes, potencjalnie generowane straty i rekomendowany plan działań (http://decyzje–it.pl/centrum–wiedzy/crm/inne–klasy/white–papers/bcmlogic–platforma–zarzadzania–ciagloscia–dzialania–4715.html).

System umożliwia monitorowanie procesów, usług i infrastruktury w czasie rzeczywistym, posiada zaawansowane narzędzia komunikacji i powiadamiania. Narzędzie nie tylko pozwala na wykrycie sytuacji awaryjnych, ale przede wszystkim ma na celu zapewnienie skutecznej reakcji i komunikacji, a w konsekwencji minimalizację skutków biznesowych związanych z wystąpieniem incydentu. Kontekstowa informacja jest dystrybuowana z użyciem dostępnych kanałów komunikacji, a odpowiedzi zwrotne pokazują aktualny status działań. Pracownicy dzięki urządzeniom mobilnym mają dostęp do informacji o niezbędnych do wykonania zadaniach, centralna konsola BCM zaś pozwala na bieżąco obserwować proces naprawczy i komunikacyjny. Wszelkie zaburzenia w funkcjonowaniu IT oraz dostępności zasobów są na bieżąco analizowane i wizualizowane w kontekście wpływu na biznes, potencjalnie generowanych strat i rekomendowanego planu działań. Interfejsy mobilne i WWW udostępniają informacje o aktualnym stanie działania organizacji z perspektywy IT, usług dla biznesu, procesów biznesowych. Wzajemne powiązania pomiędzy tymi elementami są prezentowane na bazie diagramów, co pozwala m.in. na określenie, jaki wpływ biznesowy ma awaria na działanie firmy, a menedżerom na zrozumienie, jakie narzędzia i zasoby są niezbędne do sprawnego funkcjonowania (http://bcmlogic.pl/resources/bcmlogic%20whitepaper1.pdf).

Podstawowe elementy modułowe omawianej platformy BCMLogic to (http://bcmlogic.pl/resources/bcmlogic%20whitepaper1.pdf):

- **BCMLogic Continuity Planner –** kompletne narzędzie pozwalające na przygotowanie, wdrożenie i utrzymanie aktualnych planów zachowania ciągłości działania w ich pełnym cyklu życia.

- **BCMLogic Business Availability** – moduł dostarczający zestaw dashboardów prezentujących w czasie rzeczywistym dostępność infrastruktury teleinformatycznej, krytycznych zasobów przedsiębiorstwa oraz stan działania procesów biznesowych. Na bieżąco monitorowany jest wpływ awarii i nieprzewidzianych zdarzeń na kondycję kluczowych zadań biznesowych.
- **BCMLogic Anywhere** – moduł umożliwiający zarządzanie ciągłością biznesową i dostępnością kluczowych zasobów z poziomu dedykowanych aplikacji dla urządzeń mobilnych, jak również poprzez WWW.
- **BCMLogic Notify** – moduł zapewniający powiadamianie i komunikację zwrotną wykorzystującą wszystkie dostępne kanały komunikacji.

Platforma BCMLogic integruje się z dostępną w przedsiębiorstwie architekturą aplikacji biznesowych, systemów monitoringu oraz aplikacjami service desk. Ważnym elementem platformy jest mechanizm dynamicznej dokumentacji, dzięki któremu pracownicy zawsze dysponują aktualnymi wersjami procedur, które przy każdej zmianie danych są automatycznie aktualizowane i wysyłane do ich urządzeń mobilnych. Główne korzyści omawianego rozwiązania to m.in. (http://biznes.onet.pl/windows-azure-studium-przypadku-bcmlogic,18528,4248340,news-detal):

– kompleksowe oraz efektywne zarządzanie dostępnością technologii informacyjno-komunikacyjnych,
– zapewnienie ciągłości działania biznesu,
– uzyskanie odpowiednio wysokiego poziomu bezpieczeństwa,
– spójny mechanizm zarządzania incydentami,
– możliwość błyskawicznej oceny wpływu incydentu na efektywność biznesu,
– elastyczny model opłat za wykorzystanie z omawianego rozwiązania informatycznego (oprogramowanie w formie usługi).

Docelowo firma BCMLogic chce połączyć działanie narzędzi monitorowania ICT i biznesu oraz platformy zarządzania ciągłością działania z komplementarnymi rozwiązaniami dostępnymi w Cloud Computing, a związanymi z bezpieczeństwem systemów informatycznych), takimi jak backup danych, wirtualizacja aplikacji i stacji roboczych w modelu Cloud.

7. Zakończenie

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, awarią infrastruktury informatycznej, musi podejść poważnie do zagadnienia związanego ze stworzeniem planu ciągłości działania. Wdrożenie odpowiednich norm, zaleceń, dobrych praktyk, a także implementacja właściwych funkcji, mechanizmów może zmniejszyć znacząco prawdopodobieństwo wystąpie-

nia incydentów, które mogłyby negatywnie wpłynąć na systemy informatyczne, a przez to również na ciągłość funkcjonowania organizacji. Pomocne w tym obszarze może być też skorzystanie z informatycznego narzędzia integrującego procesy zarządzania incydentami i utrzymania ciągłości działaniu biznesu. Jednym z takich narzędzi jest platforma BCMLogic, stanowiąca innowacyjne rozwiązanie do planowania i zarządzania incydentami oraz sytuacjami awaryjnymi w firmie.

Literatura

Białas A. [2006], *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa.

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 http://centrum.bezpieczenstwa.pl/content/view/348/16/.

Centrum bezpieczeństwa: BS25999–2 http://centrum.bezpieczenstwa.pl/content/view/1046/16/.

DGA – doradca bezpieczeństwa: Zarządzanie ciągłością działania (BS 25999); http://security.dga.pl/page.php?13.

Janas B., Perłowski W. [2007], *Od planów ciągłości działania do bezpieczeństwa informacji*, Akademia Wiedzy BCC, http://lepszybiznes.org/pad_files/aw_files/366_AW_SZBI_20070831.pdf.

Kaczmarek T.T., Ćwiek G. [2009], *Ryzyko kryzysu a ciągłość działania*, Difin, Warszawa.

Liderman K. [2008], *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa.

Liderman K. [2009], *Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego*, Biuletyn Instytutu Automatyki i Robotyki WAT nr 26/2009, Warszawa.

Monkiewicz J. [2010], *Przedsiębiorstwo jako podmiot ryzyka*: *Rozwój koncepcji zarządzania ryzykiem*, [w:] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa.

Norma BS 25777 http://www.bcpguide.com/index.php?option=com_content&view=article&id=225%3Abs–25777&catid=64%3Acertyfikacja–normy–boks–1&Itemid=96

Ostasiewicz W. (red.) [2004], *Składki i ryzyko ubezpieczeniowe. Modelowanie stochastyczne*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław.

Polska Norma PN-I-13335 – *Zarządzanie zabezpieczeniami systemów informatycznych*, Polski Komitet Normalizacyjny, 1999.

PN-ISO/IEC 27001:2007: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

Stokłosa J., Bilski T., Pankowski T. [2001], *Bezpieczeństwo danych w systemach informatycznych,* Wydawnictwo Naukowe PWN, Warszawa.

White Papers: BCMLogic – Platforma Zarządzania Ciągłością Działania, http://decyzje–it.pl/centrum–wiedzy/crm/inne–klasy/white–papers/bcmlogic–platforma–zarzadzania–ciagloscia–dzialania–4715.html.

Windows Azure – Studium Przypadku: BCMLogic, http://biznes.onet.pl/windows-azure-studium-przypadku-bcmlogic,18528,4248340,news-detal.

Winegard, A., Warhoe S.P. [2003], *Understanding Risk to Mitigate Changes and Avoid Disputes*, AACE International Transaction, The Association for the Advancement of Cost Engineering, Orlando, USA.

Zapłata S., Kaźmierczak M. [2011], *Ryzyko*, *ciągłość biznesu*, *odpowiedzialność społeczna*. *Nowoczesne koncepcje zarządzania*, Oficyna Wolters Kluwer business, Warszawa.

Zawiła-Niedźwiecki J. [2007], *Metoda TSM–BCP projektowania rozwiązań zapewnienia ciągłości działania organizacji*, [w:] *Zarządzanie przedsiębiorstwem*: *Teoria i praktyka*, *materiały konferencyjne*, Akademia Górniczo-Hutnicza w Krakowie, Kraków.

Zawiła-Niedźwiecki J., Rostek K., Gąsiorkiewicz A. (red.) [2010], *Informatyka gospodarcza*, t. IV, C.H. Beck, Warszawa.

SELECTED ISSUES ON INFORMATION SYSTEMS AND SERVICES SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

Summary: Business Continuity Management (BCM) is to develop solutions and procedures for such actions in a crisis situation to maintain the functioning of key business processes at a minimum acceptable level. These solutions are also associated with ensuring the continuity of functioning at the IT level. The article discusses BCM problems in the context of information systems security, presents BS 25999 norm and BS 25777 standard, supporting the planning, organization and implementation of business continuity strategy for ICT. BCMLogic system, which provides a solution to support the planning and incident management and emergency situations in the company, is also presented in the paper.

Keywords: information systems security, IS/IT risk, Business Continuity Management, BS 25999 and BS 25777 standards, BCMLogic system.