Propozycja metodyki zarządzania ciągłością działania

https://doi.org/10.33141/po.2003.06.01
Przegląd Organizacji, Nr 6 (761), 2003, ss. 5-9
www.przegladorganizacji.pl
Towarzystwo Naukowe Organizacji i Kierownictwa (TNOiK)

Janusz Zawiła-Niedźwiecki

Niezawodność układu a ciągłość działania systemu

Tak jak niezawodność, rozumiana jako stopień zdolności obiektu do spełniania stawianych mu wymagań, jest kluczowa dla oceny jakości układu czy wyrobu technicznego, tak w ocenach jakości systemów działania istotnym elementem tej oceny jest zdolność systemu do utrzymywania ciągłego działania. Tego typu dążenie w ocenie jakości wynika przede wszystkim z orientacji systemu działania na szeroko rozumianego klienta jako odbiorcę efektu działania systemu (produktu lub usługi), a składa się również na szeroko rozumianą kulturę organizacji.

Bezpieczeństwo systemu a jego ciągłość działania

Problematyka zarządzania ciągłością działania od strony organizacyjnej zbiega się z zarządzaniem jakością, zarządzaniem bezpieczeństwem i tego typu uzupełniającymi (wspierającymi) procesami, w znaczeniu analizy procesowej, działalności danej organizacji. Rozważanie integracji zarządzania tymi zagadnieniami, również w sensie wspólnych struktur organizacyjnych zarządzania, jest racjonalne, a pośrednio jest też rekomendowane przez normy ISO.

Niepewność – ryzyko – zagrożenie – zakłócenie – ciągłość działania

Ciągłość działania można rozpatrywać jako jeden z postulatów doskonałości teoretycznego systemu idealnego. Postulaty te to:

- optymalny organizacyjnie,
- optymalny kosztowo,
- dokładnie powtarzalny co do jakości efektu działania,
- w pełni skuteczny,
- bezpieczny,
- nieprzerwany.

Praktyczne próby realizacji poszczególnych postulatów doskonałości oczywiście mogą i przeważnie pozostają we wzajemnej sprzeczności, np. typowe, dla zapewnienia nieprzerwanego działania systemu, przedsięwzięcia zwiększania redundancji łączności lub wprowadzania środków bezpieczeństwa są sprzeczne z postulatami optymalnej organizacji i optymalnych kosztów działania. Postulat doskonałości nieprzerwanego działania systemu, czyli inaczej jego ciągłości działania, jest w praktyce nieosiągalny, choć może służyć wyznaczaniu celu optymalizacji działania systemu w podejściu prognostycznym do projektowania lub *reengineeringu*.

Fundamentem rozmyślań nad mechanizmem powodującym niemożność uzyskania stanu pełnej ciągłości działania systemu, jest niepewność, jako immanentna cecha rzeczywistości otaczającej człowieka i wytworzoną przezeń cywilizację, a wynikająca z wielkiej złożoności i zmienności obiektów i zjawisk w naturze oraz zależności zachodzących między nimi. Filozoficzna zasada niepewności stwierdza, że zjawiska w rzeczywistości otaczającej człowieka są zawsze niepewne, a skoro tak, to należy je traktować jako przypadkowe i jeśli można odnaleźć w przyrodzie pewne prawidłowości odnośnie do danego zjawiska, to tylko oparte na prawdopodobieństwie i statystycznym prawie wielkich liczb [1, s. 276 i następne]. Ta filozoficzna definicja została wywiedziona oraz zweryfikowana przez współczesne dokonania fizyki, zwłaszcza konfrontację klasycznej teorii mechaniki newtonowskiej z mechaniką kwantową i atomową.

Niepewność, która nieustannie dotyka człowieka, wcale nie oznacza, że podejmuje on ryzyko. Aby tak się stało, musi bowiem zaistnieć potrzeba działania, które może mieć charakter ryzykowny, co jest konsekwencją potrzeby podjęcia decyzji.

NIEPEWNOŚĆ
Potrzeba decyzji i działania Brak potrzeby decyzji i działania POWSTANIE RYZYKA BRAK RYZYKA

Ryzyko zachodzi, gdy podjęte działanie lub decyzja mogą być traktowane jako próba w eksperymencie podzielnym, tj. gdy wynik może być określony za pomocą jednego z trzech rodzajów prawdopodobieństwa: matematycznego, statystycznego lub szacunkowego, z których każdy opiera się na obiektywnej wiedzy. Wiedza ta musi usprawiedliwić przekonanie, że to, co zaszło w przeszłości, powtórzy się w przyszłości. Istotą ryzyka jest prawdopodobieństwo, które zakłada wiedzę, a ta wyklucza niepewność [2, s. 30]. W sensie praktycznym ryzyko jako kategoria pojęcio-

wa ogólna polega na tym, że podejmowana decyzja i będące jej konsekwencją działanie systemu mogą napotykać na konkretne utrudnienia i przeszkody właściwe dla ogólnej niepewności w obszarze i środowisku działania systemu, a antycypacyjnie postrzegane jako zagrożenia. A więc zagrożenie:

- jest formą realizowania się potencjalnego dotąd ryzyka,
- ma postać i cechy właściwe mierzalne obiektywnie,
- ma źródło i przyczyny,
- cechuje specyficzny mechanizm realizowania się,
- oddziałuje na system działania w sposób mierzalny subiektywnie z perspektywy systemu działania, a stopień wpływu jest zależny od podatności systemu działania i jego środowiska.

Zagrożenia, które rozważamy w praktyce biznesowej, dzielą się na następujące kategorie:

- katastrofy naturalne,
- terroryzm,
- destrukcja fizycznego środowiska pracy,
- destrukcja funkcjonalnego środowiska pracy,
- destrukcja technicznego środowiska pracy,
- destrukcja informatycznego środowiska pracy.

Gdy dane zagrożenie oddziałuje na system działania lub jego środowisko, a system staje się podatny na to oddziaływanie, mamy do czynienia z zakłóceniem, które:

- jest skutkiem interakcji zagrożenia z systemem działania lub środowiskiem tego systemu,
- skutkuje istotnymi zmianami w obszarze działania systemu,
- nie poddaje się ocenie obiektywnej, a subiektywna dokonywana jest z perspektywy systemu działania.

Zgodnie już choćby ze zdrowym biznesowym rozsądkiem, ale także np. z normą ISO17799, zarządzając działaniem systemu należy tworzyć rozwiązania skutecznie zapewniające zachowanie ciągłości tego działania. Przez analogię do organizmów żywych rozwiązania takie mają stanowić o zdolności do homeostazy, tj. o cesze systemu działania polegającej na uruchamianiu własnego wewnętrznego mechanizmu przeciwdziałania przez system zakłóceniu, celem przywrócenia stanu sprzed pojawienia się tego zakłócenia. Skuteczność rozwiązań antycypujących zakłócenia i ich adekwatność do faktycznych zdarzeń powinna się plasować powyżej progu minimalnej akceptacji przez decydentów, którzy oceny dokonują zwykle w świetle dwu kryteriów:

- prestiżu organizacji i stopnia jego podważenia w wyniku zawieszenia lub ograniczenia działania systemu,
- kosztów rozwiązań zabezpieczających oraz kosztów strat i przywracania działania naruszonego zakłóceniem.

Racjonalnie pojmowana homeostaza systemu działania świadomie prowadzi do okresowego ograniczenia jakości działania systemu do poziomu zawczasu ustalonego w świetle wyznaczników, takich jak:

- utrata nie usatysfakcjonowanego lub poszkodowanego klienta,
- *benchmarking* wobec konkurentów lub najlepszych praktyk rynkowych,
- solidne standardy współpracy z partnerami i klientami, tzw. *Service Level Agreement*.

Ograniczenie jakości nie powinno trwać dłużej, aniżeli czas potrzebny na usunięcie przyczyn i skutków zakłócenia, przy czym niekiedy te pierwsze mogą ustąpić samoistnie, jeśli taki jest charakter zakłócenia.

Czynniki oceny skali zakłócenia

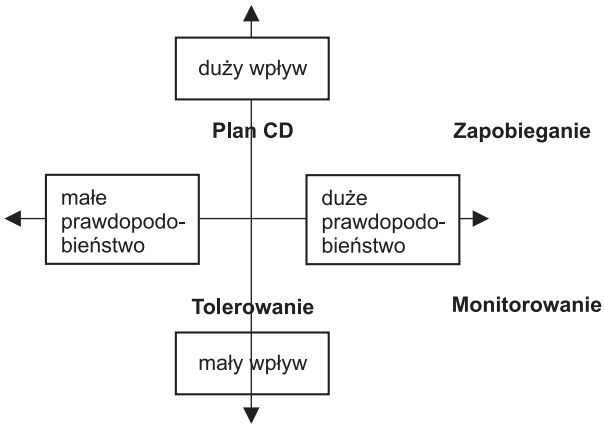
Percepcja zakłóceń jako zjawisk naruszania ciągłości działania uwzględnia dwa zasadnicze czynniki oceny ich istotności:

- prawdopodobieństwo lub częstość występowania zakłócenia,
- wpływ (destrukcyjny lub nie) zakłócenia na ciągłość działania.

Czynniki oceny nie oznaczają miar, te bowiem odpowiadają naturze zjawiska każdego konkretnego zakłócenia z osobna. Ocena powinna być indywidualna i dokonana z punktu widzenia danej organizacji.

Strategie postępowania z zagrożeniami

Modelowe podejście do reagowania na zagrożenia/zakłócenia może odbywać się na cztery sposoby określane mianem strategii reagowania (patrz rys. 1). Klasyfikacja poszczególnych przypadków zagrożeń do poszczególnych strategii jest nie tylko indywidualna oraz subiektywna, ale i tymczasowa. Wskazana jest okresowa, w miarę częsta weryfikacja takiej oceny, uwzględniająca rozwój organizacji i jej systemu działania oraz narastanie wiedzy o wpływie poszczególnych zagrożeń i prawdopodobieństwie ich wystąpienia w formie zakłóceń. Przydział do każdej z kategorii powinien uwzględniać kryteria ekonomiczne i prestiż.



Rys. 1. Strategie reagowania na zagrożenia

Tolerowanie oznacza pogodzenie się z przejściowymi niedogodnościami. **Monitorowanie** oznacza, że wiedza o zakłóceniu jest dostateczna do uruchomienia mechanizmu kompensacji. **Zapobieganie** oznacza działania (i wydatki) w celu zapobieżenia negatywnym skutkom zakłócenia. **Plan Ciągłości Działania** jest zestawem scenariuszy przewidywanego materializowania się zagrożeń oraz działań zaplanowanych na taką okoliczność.

Strategia Tolerowania (T) powinna być przypisywana do postępowania z zakłóceniami w swej na-

turze zewnętrznymi wobec danej organizacji, a tylko wtórnie jej dotyczącymi, w szczególności nie inwazyjnymi, a zwłaszcza nie destrukcyjnymi. Przykład: kolporter prasy – przeczekanie mgły porannej i późniejsze rozwiezienie gazet.

Strategia Monitorowania (M) powinna być przypisywana do postępowania z zakłóceniami w swej naturze drobnymi, choć częstymi (przez co należy zakładać ich incydentalnie większy wpływ przez kumulację zdarzeń w krótkim czasie), ale wyraźnie nie destrukcyjnymi. Z tej strategii ma wynikać obowiązek szczegółowego rozwiązania przez posunięcia organizacyjne oraz nawet drobiazgowe regulacje wewnętrzne reakcji na wszelkie typowe zakłócenia. Istotą jest nikły lub wręcz żaden wzrost kosztu z tytułu rozwiązań reagowania, bowiem mają one przede wszystkim organizacyjny charakter. Przykład: nieobecności chorobowe pracowników – obowiązek zawiadamiania zawczasu zakładu pracy oraz opracowane zasady organizowania zastępstw.

Strategia Zapobiegania (Z) powinna być przypisywana do postępowania z zakłóceniami istotnymi, destrukcyjnymi i potencjalnie często występującymi. Jest to strategia prewencji, jej naturalnymi konsekwencjami są inwestycje i rozwiązania ograniczające ryzyko zagrożenia. Typowe posunięcia to dublowanie rozwiązań technicznych. Przykład: częste wyłączenia zasilania – instalacja podtrzymywaczy napięcia lub generatorów energii.

Strategia Planu Ciągłości Działania (P) powinna być przypisywana do postępowania z zakłóceniami istotnymi, destrukcyjnymi, lecz potencjalnie rzadko występującymi, co uzasadnia decyzje o rezygnacji ze strategii Z i świadome podejmowanie ryzyka zagrożeń. Przykład: giełda – światowe statystyki mówią, że zawieszenie notowań z powodu niesprawności systemu komputerowego zdarza się nie częściej niż raz na 3 lata i trwa nie dłużej niż jeden dzień; uzasadnione jest więc poleganie na scenariuszu zastępczego funkcjonowania w trakcie usuwania tak rzadko zdarzającej się, poważnej awarii.

Lista zagrożeń – Mapa zakłóceń

Poszczególne strategie, jako modelowe wytyczne postępowania, przypisuje się zakłóceniom, których **Mapa Zakłóceń** jest opracowywana jako zestawienie par: zagrożenie – obiekt (patrz tab. 1 i 2). **Lista Zagrożeń** jest sporządzana zgodnie z podziałem na kategorie zagrożeń przedstawione wcześniej. **Lista Newralgicznych Obiektów** tworzona jest w wyniku nałożenia obrazu podstawowych procesów biznesowych [3] i związanych z nimi przepływów informacji na plan przestrzenny całej infrastruktury budowlanej i technicznej organizacji. Modelowe strategie są następnie rozwijane do postaci **Polityk Postępowania z Zakłóceniami.**

Polityki postępowania z zakłóceniami

Polityka Tolerowania (T) powinna określać podstawowe zasady przystępowania organizacji do stanu pogodzenia z zaistniałym zakłóceniem, badania przesłanek jego utrzymywania się, stwierdzania jego ustąpienia oraz powrotu do rutynowego funkcjonowania. Dokumentowi **Polityki T** powinny towarzyszyć procedury/instrukcje szczegółowo określające konieczne działania komórek organizacji w sytuacjach zakłóceń zakwalifikowanych do poddania ich tej polityce. Przykład: mimo że reakcja organizacji na zakłócenie może krańcowo polegać na zawieszeniu wypełniania statutowych funkcji, to być może należy poinformować o tym partnerów handlowych lub opinię publiczną, skierować pracowników do prac zastępczych nie poddających się działaniu zakłócenia, uruchomić rozwiązania śledzące stopień intensywno-

Tab. 1. Lista zagrożeń

Grupy / Zagrożenia	Ocena
A. Katastrofy naturalne ● trzęsienie ziemi ● skażenie środowiska ● powódź ● huragan ● wyładowania atmosferyczne	
B. Terroryzm ● szantaż ● zamach	
C. Zakłócenia fizycznego środowiska pracy ● brak dostępu do siedziby ● uszkodzenie budynku ● za niska / wysoka temperatura powietrza ● za duża wilgotność powietrza ● pożar ● zalanie	
D. Zakłócenie funkcjonalnego środowiska pracy ● strajk ● sabotaż ● niedostępność pracowników ● wypadek	
E. Zakłócenie technicznego środowiska pracy ● wyczerpanie zapasów mat. ● brak zasilania ● awaria klimatyzacji	
F. Zakłócenie informatycznego środowiska pracy Infrastruktura techniczna: ● serwerów ● stacji roboczych ● urządzeń pomocniczych ● urządzeń sieciowych ● okablowania ● brak połączenia z sieciami zewnętrznymi Oprogramowanie: ● wygaśnięcie licencji ● nie autoryzowane usunięcie ● wadliwe działanie Wirusy: ● itd. Dane: ● utrata lub zniszczenie danych ● nie autoryzowany dostęp do informacji ● nie autoryzowane powielanie informacji ● nie autoryzowana modyfikacja informacji	

Tab. 2. Lista newralgicznych obiektów

Kategorie	Obiekty	Np.
A. Budynki		własny biurowiec
B. Obiekty przemysłowe, techniczne		hala fabryczna, kotłownia, ośrodek komputerowy
C. Ośrodki biurowe		powierzchnia biurowa wynajęta w obcym budynku
D. Zewnętrzne urządzenia techniczne		wolno stojący generator napięcia zewnętrzny
E. Wewnętrzne urządzenia techniczne		klimatyzator, generator wewnętrzny
F. Infrastruktura informatyczna		
G. Zewnętrzne urządzenia telekomunikacyjne		antena satelitarna na dachu, router, który znajduje się u klienta
H. Usługi obce		telekomunikacja

ści zakłócenia. W momencie ustąpienia zakłócenia należy dokonać weryfikacji, czy jest możliwe podjęcie zawieszonych dotąd czynności/funkcji.

Polityka Monitorowania (M) powinna określać podstawowe zasady reagowania organizacji na zakłócenia, co do których świadomość ich zaistnienia w połączeniu z istniejącymi regułami zachowań (ewentualnie spisanymi w postaci procedur i instrukcji) powinna w dostatecznym stopniu uruchamiać organizacyjne mechanizmy kompensacji zakłócenia. Dokumentowi **Polityki M** powinny towarzyszyć procedury/instrukcje szczegółowo określające konieczne działania komórek organizacji w sytuacjach zakłóceń zakwalifikowanych do poddania ich tej polityce. Przykład: w banku, pracowników bezpośredniej obsługi klientów obowiązuje procedura uprzedzania o nieobecnościach spowodowanych np. chorobą, a określona liczba pracowników zaplecza jest przeszkolona do obsługi klientów na zasadzie zastępstw, przy czym każdego dnia określona ich liczba ma być gotowa do podjęcia takiej zastępczej pracy na wypadek absencji nadzwyczajnej, o której pracownik zawczasu nie uprzedził.

Polityka Zapobiegania (Z) powinna określać plany organizacji dotyczące działań prewencyjnych, które w odniesieniu do szczególnie istotnych elementów działalności organizacji, a zwłaszcza szczególnie wrażliwych elementów jej infrastruktury technicznej, mają zniwelować destrukcyjny wpływ zakłóceń. Typowymi działaniami podejmowanymi w tym celu są: tworzenie rozwiązań zapasowych, nadmiarowych, zwielokrotnionych w stosunku do przeciętnych zapotrzebowań. Dokumentowi **Polityki Z** powinny towarzyszyć analizy szczegółowo określające stopień i zakres wrażliwości rozwiązań istniejących, plany rozwiązań zmniejszających zagrożenia, procedury/instrukcje szczegółowo określające organizację i zasady działania bieżącego oraz specjalnych interwencji specjalistycznych zespołów do zwalczania specyficznych zagrożeń (pożar, atak hakerski, awaria informatyczna). Przykład: zapasowy ośrodek komputerowy, dublowane linie komunikacyjne prowadzone fizycznie różnymi drogami i/lub z wykorzystaniem odmiennych mediów transmisji. Także dyżury specjalnych ekip interwencyjnych o stosownych kwalifikacjach.

Równocześnie należy podkreślić, że każda z par obiekt – zagrożenie ujęta w **Polityce Z**, a więc w planie działań prewencyjnych, o ile polegają one na inwestycjach zmniejszających zagrożenie, to do czasu ich zakończenia powinny być ujęte także w jednej z pozostałych **Polityk** (zaleca się, aby w **Polityce P**) celem zapewnienia stosownej reakcji na zagrożenie.

Polityka Planu Ciągłości Działania (P) powinna określać plany organizacji dotyczące działań koniecznych w przypadku zmaterializowania zagrożenia w postaci konkretnego zakłócenia. Plany powinny obejmować rozwiązania organizacyjne dotyczące prowadzenia samej **Polityki** oraz scenariusze przypadków zakłóceń i zakładanych wobec nich działań, mających na celu zapewnienie kontynuacji przynajmniej podstawowej aktywności biznesowej organizacji. Ponadto **Polityka P** powinna określać zasady reagowania *ad hoc* na zdarzenia, których niestety nie udało się przewidzieć w scenariuszach (w ogóle lub co do skali). Dokumentowi **Polityki P** powinny towarzyszyć procedury/instrukcje szczegółowo określające organizację służb prowadzących plany ciągłości działania, podstawowe reguły komunikowania się w warunkach awarii, zasady reagowania na typowe zagrożenia, scenariusze przewidywanych rozległych zakłóceń i reagowania na nie, zasady uwzględniania w nowych wersjach planów awaryjnych doświadczeń ze zwalczania świeżo zaszłych zakłóceń.

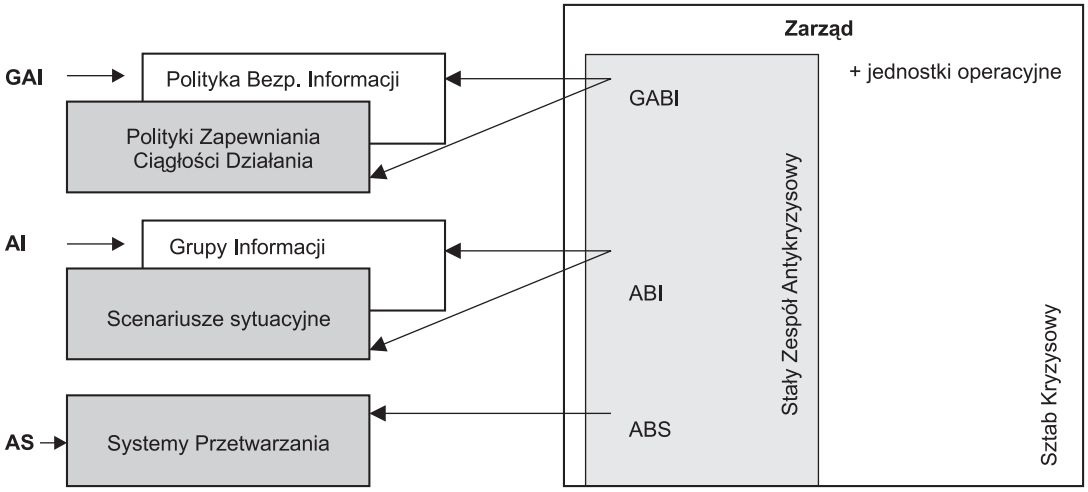
Organizacja zarządzania ciągłością działania

Zasadniczą ideę co do struktury organizacyjnej służb odpowiadających za bieżące zarządzanie problematyką przygotowywania **Polityk Postępowania z Zakłóceniami** oraz organizację sztabu kryzysowego powoływanego na wypadek awarii przedstawia rys. 2.

Podsumowanie

Jako streszczenie wytycznych normy ISO 17799 (rozdz. 11).

■ W działalności organizacji należy się liczyć z możliwością zaistnienia wydarzeń krytycznych, które



Rys. 2. Zintegrowane zarządzanie bezpieczeństwem informacji i ciągłością działania

uniemożliwią normalne kontynuowanie tej działalności.

■ Niezależnie od charakteru przyczyn tych wydarzeń, w ramach formalnego lub postrzeganego w kategoriach biznesowych obowiązku dołożenia należytej staranności w wypełnianiu swych zadań, organizacja powinna dążyć do choćby ograniczonego kontynuowania działalności.

■ Staranie takie powinno opierać się na uprzednio opracowanym, konsekwentnie doskonalonym i testowanym „Planie Ciągłości Działania" (PCD).

■ Zapewnianie ciągłości działania to przewidywanie potencjalnych scenariuszy zakłóceń oraz rozdzielne projektowanie:

- rozwiązań zapobiegających samym zagrożeniom,
- rozwiązań służących jak najszybszemu usuwaniu skutków zakłóceń ,
- rozwiązań kontynuowania ograniczonej działalności w warunkach krytycznych (PCD).

■ Podejście do problemu ciągłości działania powinno być racjonalne, a więc przede wszystkim obliczone na zapewnienie równowagi pomiędzy oczekiwanym stopniem pewności zachowania ciągłości działania a kosztami jego uzyskania. Konieczne więc jest przyjęcie założenia stopniowego rezygnowania z kolejnych elementów normalnej działalności stosownie do zidentyfikowanych rozmiarów sytuacji krytycznej na wzór wojskowego planu wycofywania się na z góry upatrzone pozycje.

■ PCD powinien być na tyle elastyczny, aby umożliwiał adaptatywne reagowanie na zakłócenia odbiegające od przewidywań będących podstawą planu.

■ Konieczne jest zdefiniowanie procesowej istoty działalności danej organizacji jako minimum czynności, które można jeszcze uznać za wypełnianie przez nią jej obowiązków. Niemożność kontynuowania takiego minimum czynności jest podstawą decyzji o rezygnacji z korzystania z PCD i skupieniu się tylko na usuwaniu skutków zakłóceń.

■ W ramach przygotowywania PCD rozważa się w pierwszym rzędzie aspekty biznesowe, prawne i organizacyjne, bo one decydują o koniecznym zakresie rozwiązań technicznych.

■ Analiza biznesowa dotyczyć może kwestii prestiżu firmy, a na pewno swoistego bilansu ryzyka oraz środków finansowych przeznaczonych na jego ograniczenie. Rozsądne jest potraktowanie PCD jako długofalowego projektu, w którym założone cele biznesowe będą osiągane stopniowo, kolejnymi przybliżeniami (wersjami PCD).

■ Analiza prawna jest szczególnie ważna przy tworzeniu założeń PCD, bowiem pozwala zdefiniować zakres odpowiedzialności firmy za poszczególne obszary jej działalności, wskazać obszary newralgiczne oraz dobrać pozatechniczne formy zabezpieczeń.

■ Analiza organizacyjna pozwala wyodrębnić kadrę osób właściwą do posługiwania się PCD w warunkach krytycznych, stworzyć im odpowiedni zakres autonomii decyzyjnej w takiej sytuacji, a w warunkach codziennych umożliwić przygotowywanie się do takiej trudnej roli.

■ Żaden z elementów analizy, a podobnie i projektowanie rozwiązań technicznych, nie jest etapem zamkniętym. Doskonalenie PCD polega na stałym ponawianiu takich analiz i projektowania w odniesieniu do zmian w działalności organizacji, rozwoju rozwiązań PCD oraz wniosków z wystąpienia faktycznych zagrożeń.

Janusz Zawiła-Niedźwiecki

BIBLIOGRAFIA

[1] *Metodyka zapewniania ciągłości działania TISM-BCP*, European Network Security Institute, Warszawa 2003.
[2] RUMMLER G, BRACHE A., *Podnoszenie efektywności organizacji*, PWE, Warszawa 2000.
[3] SAMECKI W., *Ryzyko i niepewność w działalności przedsiębiorstwa przemysłowego*, PWE, Warszawa 1967.
[4] TATARKIEWICZ W., *Historia filozofii,* tom 3, PWN, Warszawa 1995.

Autor: dr inż., adiunkt w Instytucie Organizacji Systemów Produkcyjnych Politechniki Warszawskiej.