IDENTYFIKACJA ZAGROŻEŃ DLA CIĄGŁOŚCI DZIAŁANIA ORGANIZACJI

Krzysztof Szwarc, Piotr Zaskórski

Wojskowa Akademia Techniczna

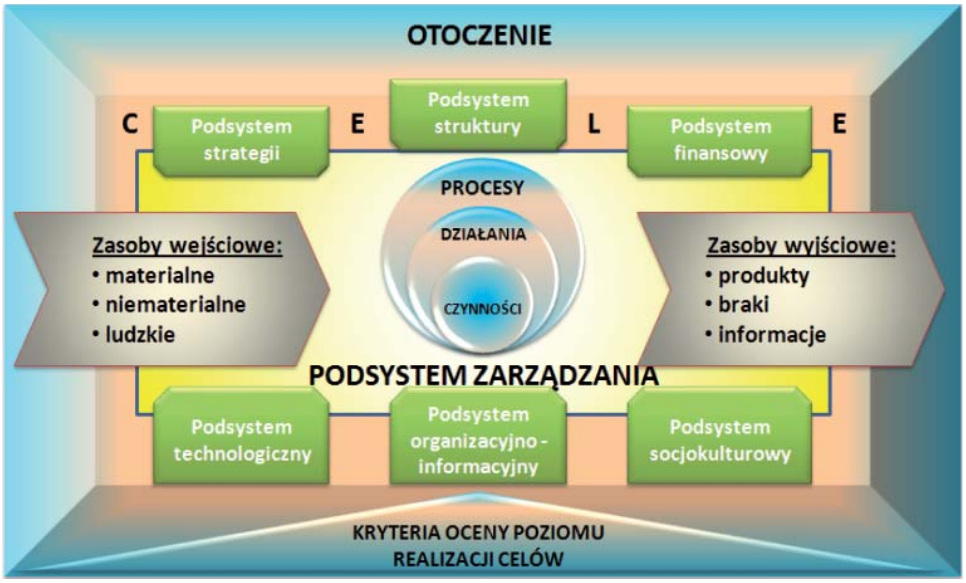
Streszczenie. W artykule podjęto próbę identyfikacji czynników warunkujących ocenę poziomu bezpieczeństwa organizacji. Bezpieczeństwo organizacji jest kategorią ogólnosystemową i funkcją złożoną, której wartość warunkowana jest poziomem ryzyka. Współczesne modele organizacji budowanych na procesach wskazują na potrzebę zwrócenia szczególnej uwagi na zasoby informacyjne, które w warunkach działania na globalnych rynkach nabierają strategicznego znaczenia. Dlatego jednym z podstawowych problemów zarządzania współczesną organizacją wydaje się problem bezpieczeństwa informacyjnego, w tym zapewnienia ciągłości działania w wymiarze informacyjnym, logistyki czy finansów. Powiązanie ww. obszarów wymaga znalezienia uniwersalnej platformy integracji umożliwiającej sprawne realizowanie zakładanych celów. Funkcjonowanie organizacji rozproszonej determinowane jest szeregiem zagrożeń, wynikających zarówno z uwarunkowań samej organizacji jak i z jej otoczenia. Dlatego problem bezpieczeństwa organizacji wymaga zwrócenia szczególnej uwagi na problem identyfikacji zagrożeń dla ciągłości jej funkcjonowania.

1. Wstęp

Bezpieczeństwo organizacji jest kategorią ogólnosystemową i funkcją złożoną, której wartość warunkowana jest poziomem ryzyka. Jednym z podstawowych warunków realizacji celów organizacji jest zapewnienie bezpieczeństwa jej funkcjonowania. Współczesne modele organizacji budowanych na procesach wskazują na potrzebę zwrócenia szczególnej uwagi na zasoby informacyjne, które w warunkach działania na globalnych rynkach nabierają strategicznego znaczenia. Dlatego jednym z podstawowych problemów zarządzania współczesną organizacją wydaje się kwestia zapewnienia ciągłości działania w wymiarze informacyjnym, logistyki czy finansów. Powiązanie ww. obszarów wymaga znalezienia uniwersalnej platformy integracji umożliwiającej sprawne realizowanie zakładanych celów. W tym kontekście na szczególną uwagę zasługują zintegrowane systemy informatyczne zarządzania, bazujące na danych transakcyjnych i historycznych oraz sieci Internet, umożliwiające dostęp do rozproszonych geograficznie zasobów w trybie on-line. Funkcjonowanie w takich warunkach obok oczywistych zalet determinuje szereg zagrożeń, wynikających zarówno z uwarunkowań samej organizacji jak i jej otoczenia. Dlatego kwestia zapewnienia ciągłości działania wymaga zwrócenia szczególnej uwagi na problem identyfikacji zagrożeń.

2. Istota organizacji

Analiza literatury przedmiotu wskazuje na wieloznaczność pojęcia „organizacja". W kontekście rzeczowym organizację można definiować jako grupę ludzi, którzy współpracują w uporządkowany i skoordynowany sposób. Ich działanie motywowane jest chęcią realizacji swoich celów [5]. Tak więc przedsiębiorstwo można traktować jako sposób sprawnego i skutecznego osiągania celów pewnej zbiorowości, dzięki odpowiedniemu wykorzystaniu potencjału jej członków. Wpływ osiągnięć cybernetyki na naukę o organizacji i zarządzaniu wskazuje na możliwość analizy organizacji w kategoriach systemu otwartego, którego funkcjonowanie warunkowane jest wpływem otoczenia (schemat 1)



Schemat 1. Organizacja w ujęciu systemowym. Opracowanie własne na podstawie: [10], [18]

Organizacja jest więc (schemat 1) zbiorem elementów i relacji z otoczeniem. Jak widać, kluczowym elementem każdej organizacji są procesy umożliwiające przekształcenie elementów wejściowych w wartość na wyjściu systemu. Kompleksowe spojrzenie na organizację proponowane w ramach podejścia systemowego zwraca uwagę na konieczność dokonywania oceny osiągania zakładanych celów w odniesieniu do kryteriów niezawodności, ryzyka, bezpieczeństwa czy efektywności oraz konsekwencji, jakie wiążą się z próbą zmiany ww. parametrów bez uwzględnienia wzajemnych powiązań i relacji. Dążąc do maksymalizacji bezpieczeństwa, efektyw-

ności czy wydajności działania, nie wolno zapominać o zależnościach między tymi cechami, determinującymi jakość tego systemu.

3. Pojęcie bezpieczeństwa i jego zagrożeń

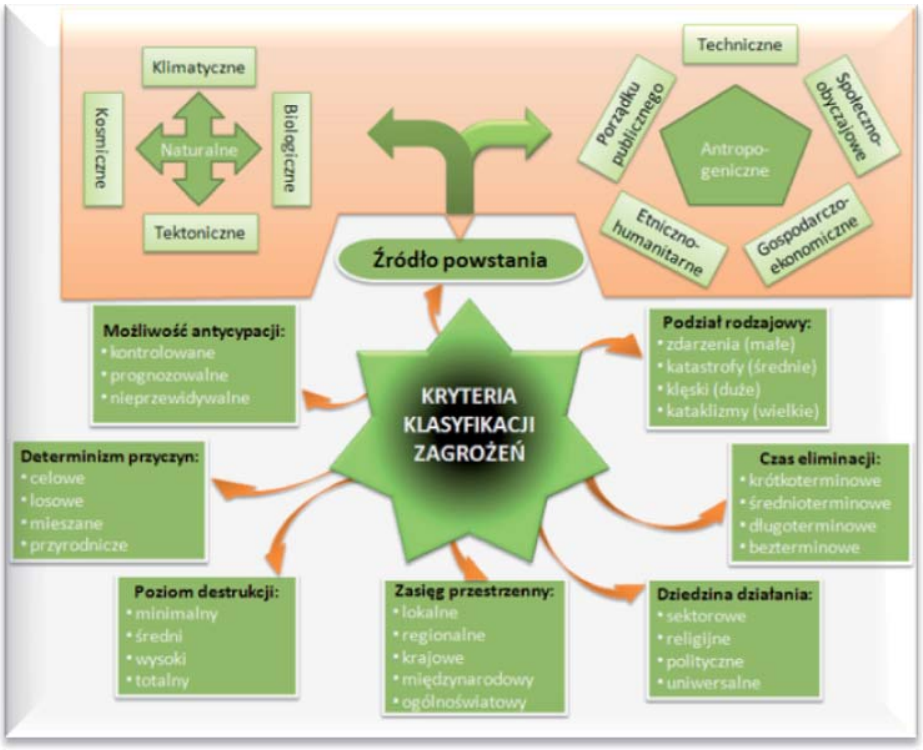
Jednym z przyjętych do tej pory założeń było stwierdzenie, że motywem skłaniającym ludzi do podejmowania działania jest chęć zaspokojenia swoich potrzeb. Teoria motywacji Maslowa wskazuje na szczególną rolę bezpieczeństwa jako jednego z najważniejszych motywów skłaniających człowieka do działania. Istota teorii zaprezentowanej przez Maslowa pokazuje, że niespełnienie tej potrzeby będzie prowadziło do zahamowania rozwoju człowieka (potrzeby wyższego rzędu, która nie może być spełniona bez realizacji potrzeb niższego rzędu). Tak więc poznanie specyfiki bezpieczeństwa wydaje się niezwykle istotne z punktu widzenia zarządzania organizacją XXI wieku.

Wskazanie jednoznacznej definicji bezpieczeństwa jest równie trudne jak w przypadku terminu „organizacja". Definicje leksykalne interpretują bezpieczeństwo jako stan niezagrożenia, spokoju i pewności – nawiązując do źródłosłowu (bez pieczy – czyli bez konieczności sprawowania ochrony). Inna definicja bezpieczeństwa wskazuje, że jest to „stan, który daje poczucie pewności i gwarancje jego zachowania oraz szansę na doskonalenie (…). To sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych" [13, s. 13]. Zgodnie z przytoczonymi stwierdzeniami, bezpieczeństwo na ogół definiowane jest przez wskazanie warunków, w których dany podmiot odczuwa stan pewności przetrwania i swobodnego rozwoju.

We wszystkich ze wskazanych definicji bezpieczeństwo postrzegane jest w kategoriach statycznych (stanu). Należy jednak zauważyć, że zagrożenia determinujące poczucie bezpieczeństwa nie pozwalają utożsamiać tego pojęcia w kategoriach czegoś trwałego, niezmiennego. Stąd trafne wydaje się stwierdzenie, że „bezpieczeństwo jest nie tyle określonym stanem rzeczy, ile ciągłym procesem społecznym, w ramach którego podmioty działające starają się doskonalić mechanizmy zapewniające im poczucie bezpieczeństwa" [14, s. 18]. Tak więc bezpieczeństwo powinno być traktowane również jako dynamiczny proces, umożliwiający spełnianie związanych z nim potrzeb.

Przytoczone definicje bezpieczeństwa wskazują na ścisłe powiązanie tego pojęcia z terminem zagrożenie, określanym jako „sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia" [13 s. 159]. Wskazana definicja jeszcze raz podkreśla zależności między zagrożeniem (stanem niebezpieczeństwa) a bezpieczeństwem (rozumianym jako stan braku zagrożenia). Przenosząc rozważania na temat zagrożeń na grunt organizacji, warto przytoczyć inną definicję prezentowaną w literaturze przedmiotu, wedle której zagrożenie należy rozumieć jako „zdarzenie spowodowane przyczynami losowymi (naturalnymi) lub nielosowymi (celowymi), negatywnie wpływającymi na funkcjonowanie systemu

lub jego otoczenia" [2, s. 76]. Tak więc organizacja rozumiana jako pewien system działania, wchodzący w interakcje z otoczeniem, jest narażona na zagrożenia negatywnie wpływające na jej funkcjonowanie.



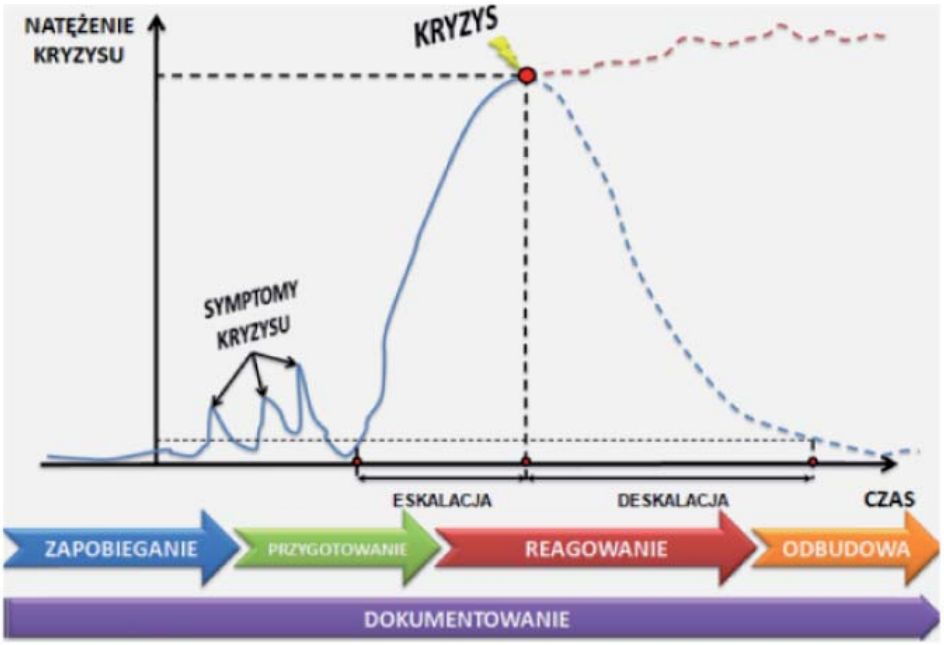
Rys. 1. Kryteria klasyfikacji zagrożeń. Opracowanie własne na podstawie: [2, s. 76-115]

Zaprezentowana taksonomia zagrożeń (rys. 1) umożliwia opis danego zjawiska np. ze względu na jego skalę, źródło powstania czy poziom wpływu na otocznie. Każdy z przytoczonych typów zagrożeń wiąże się z określoną specyfiką, której poznanie umożliwia podjęcie działań zmniejszających prawdopodobieństwo wystąpienia sytuacji kryzysowej dla ciągłości działania organizacji oraz ograniczenie potencjalnych skutków, w przypadku gdy jest to niemożliwe.

4. Infrastruktura krytyczna

Zagrożenia wpływające negatywnie na sposób funkcjonowania organizacji są przyczyną powstawania kryzysów. Należy przy tym zauważyć, że powszechne rozumienie tego pojęcia odbiega od jego faktycznego znaczenia. W tym momencie należy rozróżnić dwa terminy: kryzys oraz sytuacja kryzysowa.

Zgodnie z ustawą o zarządzaniu kryzysowym sytuacją kryzysową jest sytuacja „będąca następstwem zagrożenia i prowadząca w konsekwencji do zerwania lub znacznego naruszenia więzów społecznych przy równoczesnym poważnym zakłóceniu w funkcjonowaniu instytucji publicznych (…)”[1]. Tak więc sytuacje kryzysowe będące następstwem zagrożeń wpływają negatywnie na sposób funkcjonowania organizacji.



Wykres 1. Dynamika sytuacji kryzysowej na tle działań reagowania kryzysowego. Opracowanie własne na podstawie: [15, s. 49]

Przedstawiona na wykresie 1 dynamika sytuacji kryzysowej odzwierciedla przyjęte wcześniej założenie dotyczące zależności pomiędzy poziomem bezpieczeństwa i zagrożenia. Szczególnym momentem w przedstawionej dynamice jest kryzys, czyli moment przełomowy, wywołujący zmianę dotychczasowego stanu rzeczy, a w konsekwencji prowadzonych działań powrót do akceptowalnego poziomu bezpieczeństwa. Zgodnie z kryterium czasu eliminacji warto zauważyć, że przedstawiona na wykresie faza pokryzysowa może odnosić się do różnego horyzontu czasowego. Ponadto

[1] Art. 3, pkt 1 Ustawy z dn. 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (DzU z 2007 r. Nr 89, poz. 590 z pózn. zm.).

w zależności od fazy sytuacji kryzysowej, konieczne jest podjęcie różnych działań umożliwiających przywrócenie oczekiwanego stanu.

Szczególnie istotnym aspektem zapewnienia ciągłości działania jest wyszczególnienie newralgicznych elementów systemu. Takimi z punktu widzenia przytaczanej wcześniej ustawy jest tzw. infrastruktura krytyczna, czyli „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzania, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców”[2]. Zatem infrastruktura krytyczna jest zbiorem materialnych i niematerialnych elementów systemu, decydującym o ciągłości jego funkcjonowania. Patrząc na wymienione w ustawie systemy składające się na infrastrukturę krytyczną, należy zauważyć, że w kontekście współczesnych organizacji, opartych na pracy w środowisku sieciowym, szczególnej staranności wymaga zapewnienie bezpieczeństwa:

- energetycznego (energia elektryczna, surowce energetyczne, paliwa),
- informacyjno-komunikacyjnego (sieci teleinformatyczne, sprzęt komputerowy i jego oprogramowanie, łączność telefoniczna, satelitarna, radiowa),
- finansowego (płynności, dostępu do instrumentów finansowych),
- pracy (ochrona zdrowia, BHP, wsparcie psychologiczne).

Ponadto kluczowym czynnikiem warunkującym sprawność działania organizacji są ludzie, dlatego ich szczególnej uwagi wymaga ograniczanie podatności organizacji na zagrożenia związane z ich świadomą działalnością (np. szpiegostwo gospodarcze, korupcja) oraz przypadkową (błędy).

5. Ciągłość działania jako przedmiot zarządzania

Zarządzanie rozumiane jako zestaw działań ukierunkowanych na zasoby organizacji i wykonywanych z zamiarem osiągania zakładanych celów w sposób sprawny i skuteczny umożliwia spełnianie potrzeb ludzi. Na szczególną uwagę w przytoczonej definicji zasługuje zwłaszcza aspekt sprawności działania, odnoszący się do mądrego wykorzystania zasobów, pozbawionego marnotrawstwa. W tym kontekście można powiedzieć, że jednym z zasadniczych problemów nauki o organizacji i zarządzaniu jest zwiększanie efektywności działania [5, s. 6]. Dostrzeżenie możliwości konkurowania czasem oraz jego wpływu na bezpieczeństwo organizacji w wielu wymiarach zwróciło uwagę na konieczność zarządzania ciągłością działania.

Zarządzanie ciągłością działania to ciągły proces realizowany i finansowany na poziomie wyższego kierownictwa, w celu zapewnienia niezbędnych działań

[2] Art. 3, pkt 2 ustawy z dn. 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (DzU z 2007 r. Nr 89, poz. 590 z pózn. zm.).

w zakresie identyfikacji wpływu potencjalnych strat, tworzenia i doskonalenia strategii i planów przywracania działania oraz zapewnienia ciągłości pracy [11]. Dlatego zarządzanie ciągłością działania należy traktować jako kompleksowe narzędzie zwiększania efektywności, umożliwiające minimalizowanie strat wywołanych wystąpieniem niepożądanych zdarzeń, wpływających negatywnie na funkcjonowanie organizacji. Istotą tego obszaru zarządzania jest zmniejszanie podatności organizacji na zakłócenia, uniemożliwiające realizację zakładanych celów.

BCI[3] definiuje zarządzanie ciągłością działania jako holistyczny proces, umożliwiający identyfikację wpływu potencjalnych zagrożeń na funkcjonowanie organizacji oraz stworzenie warunków dla budowania odporności i zdolności skutecznego reagowania i zabezpieczenia kluczowych interesów właścicieli, reputacji, marki oraz wartości osiągniętych w jej dotychczasowej działalności [4]. Wymagane jest zatem zintegrowanie tego obszaru zarządzania ze strategią organizacji, a także wiedzą i doświadczeniem w zakresie zarządzania ryzykiem, wsparcia logistycznego czy IT.

Rys. 2. Zarządzanie ciągłością działania jako proces holistyczny. Źródło: [3]

Zgodnie z zaprezentowaną wcześniej definicją, zarządzanie ciągłością działania organizacji jest procesem holistycznym (rys. 2). Co więcej, dążenie do utrzymania ciągłości działania powinno wynikać z celów firmy oraz strategii ich realizacji. Istotnym wyzwaniem dla zarządzania w warunkach gospodarki cyfrowej staje się więc zapewnienie informacyjnej ciągłości działania, zwłaszcza w kontekście idei organizacji zorientowanej na procesy, często rozproszonej geograficznie.

[3] ***BCI – Business Continuity Institute.***

Rys. 3. Cykl życia programu zarządzania ciągłością działania zgodny z normą BS 25999-1.
Źródło: [8, s. 20]

Można zatem powiedzieć, że zapewnienie ciągłości działania jest jednym ze strategicznych procesów warunkujących przetrwanie organizacji w turbulentnym otoczeniu. Dlatego istnieje potrzeba systemowego podejścia do zarządzania tym obszarem, zwanego programem zarządzania ciągłością działania (rys. 3). Przedstawiony cykl życia programu zarządzania ciągłością działania wskazuje na sekwencję czynności niezbędnych do zapewnienia bezpieczeństwa organizacji w omawianym zakresie. Niezwykle istotnym aspektem tego procesu jest zakorzenienie problemu zapewnienia ciągłości organizacji na wszystkich poziomach realizacji działań, począwszy od stanowiska pracy po najwyższe kierownictwo. Stąd program BCM wymaga zmiany kultury organizacji.

6. Identyfikacja zagrożeń ciągłości działania organizacji

Wśród zaprezentowanych na rysunku 2 aspektów zarządzania ciągłością działania szczególne miejsce zajmuje obszar zarządzania ryzykiem. Ryzyko, będące jednym z kryteriów oceny systemu (schemat 1), w literaturze przedmiotu poruszane jest w kontekście [21, s. 13-14]:

- teorii podejmowania decyzji – nawiązującej do miar matematycznych i statystycznych, określającej prawdopodobieństwo wyniku będącego konsekwencją decyzji,
- teorii zarządzania ryzykiem – rozpatrywanym pod kątem skutków działania (pozytywnych i negatywnych).

Stąd też ryzyko często charakteryzowane jest za pomocą określonych miar ilościowych [20, s. 220]:

$$Ry=P\times S\times B\times E,$$

gdzie:
Ry – ryzyko,
P – poziom częstości występowania zagrożenia,
S – poziom/wartość strat,
B – podatność na zagrożenie,
E – współczynnik ekspozycji.

Analizując problematykę ryzyka, należy zauważyć, że jego poziom bardzo często określany jest za pomocą subiektywnych odczuć podmiotów dokonujących jego oceny. Ponadto specyfika badanego podmiotu wymaga uzupełnienia przedstawionych powyżej teorii o wskaźnik podatności oraz współczynnik ekspozycji, umożliwiający podkreślenie specyficznych z punktu widzenia bezpieczeństwa obszarów działania organizacji.

Schemat 2. Model zarządzania ryzykiem. Opracowanie własne na podstawie: [12]

Proces zarządzania ryzykiem według normy PN-IEC 62198 został przedstawiony na schemacie 2. Jednym z zasadniczych działań jest właściwe zidentyfikowanie jego źródeł. Na podstawie przyjętego modelu postępowania etap identyfikacji ryzyka można przestawić w postaci cyklu (schemat 3).

Jak widać (schemat 3), przyjęty model identyfikacji zagrożeń dla ciągłości działania składa się z ośmiu etapów. Początkowe działania umożliwiające poznanie specyfiki analizowanego systemu, a zwłaszcza procesów ich zasileń i efektów, wskazują na potrzebę odwołania się do dokumentacji. W zależności od typu organizacji, działania te mogą jednak napotkać na szereg problemów, w tym brak niezbędnych zapisów. Należy zauważyć, że stan posiadanej dokumentacji determinuje zakres identyfikacji

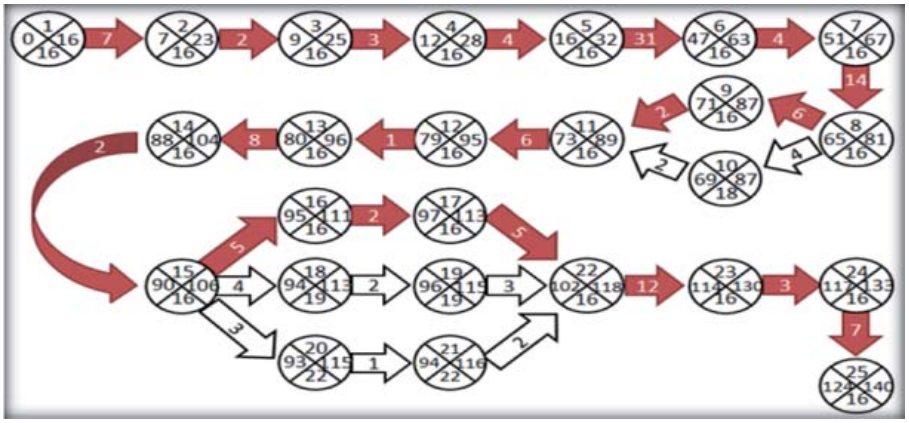
i analizy ryzyka, przez to również i koszty całego przedsięwzięcia. Dokumentami wykorzystywanymi dla ww. działań są m.in. [19, s. 91], [1, s. 298-300]:

- spisy inwentaryzacyjne (zestawienia zasobów i ich właścicieli),
- mapy procesów i przepływów informacyjnych,
- definicje i opisy procesów,
- plany zarządzania: ryzykiem, zakresem, kosztami, harmonogramem, jakością,
- rejestry interesariuszy,
- diagramy sieciowe,
- raporty z wykonywanych prac,
- wyniki audytów i ocen bezpieczeństwa.

Schemat 3. Metodyka identyfikacji zagrożeń dla ciągłości działania organizacji. Opracowanie własne na podstawie: [19, s. 80-92]

Niezależnie od przyjętej strategii, przedsiębiorstwo już na wstępie powinno zdefiniować procesy realizowane w przedsiębiorstwie oraz dokonać ich klasyfikacji ze względu na kryterium tworzenia wartości dla klienta. Na tej podstawie można wyodrębnić megaprocesy: podstawowy – kluczowy dla tworzenia produktu – oraz pomocniczy, którego realizacja umożliwia sprawny przebieg procesów podstawowych. Katalog procesów kluczowych będą stanowiły procesy podstawowe (np. obsługa klienta, projektowanie i przygotowanie produkcji, zakupy, wytwarzanie, dystrybucja), jak również wybrane procesy pomocnicze (np. transport wewnętrzny i magazynowanie).

Problematyka zapewnienia ciągłości działania organizacji wymaga zwrócenia szczególnej uwagi na procesy opisywane przez strukturę: statyczną (drzewo), dynamiczną (sieć), niezawodnościową (szeregowa, równoległa, mieszana).



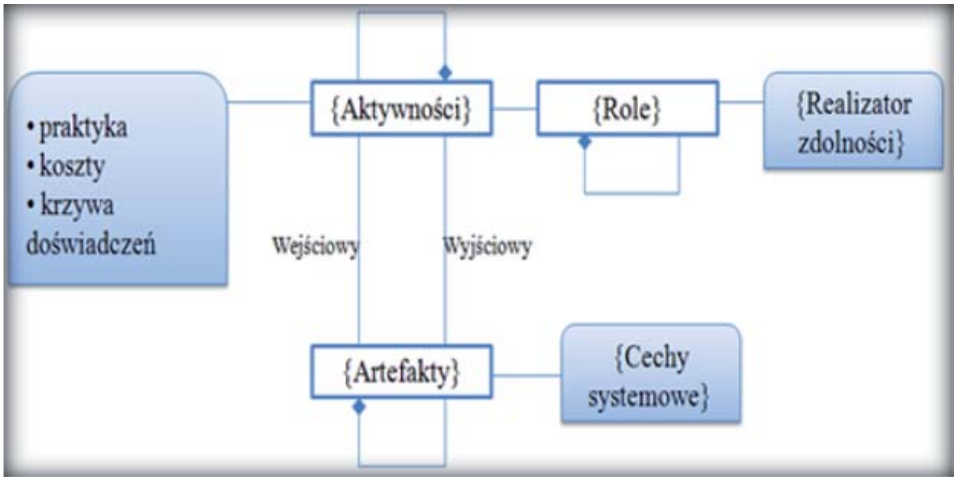
Schemat 4. Odwzorowanie przykładowego procesu za pomocą struktury sieci. Opracowanie własne

Analiza struktury sieciowej procesu (schemat 4) umożliwia wyznaczenie najwcześniejszego czasu realizacji procesu przy wykonaniu wszystkich niezbędnych prac. Na tej podstawie można również wyznaczyć ścieżkę krytyczną odzwierciedlającą przebieg zdarzeń od początkowego do końcowego, których opóźnienie wpływa na przekroczenie zakładanego czasu realizacji całego przedsięwzięcia (opóźnienia dostawy produktu procesu). Dlatego zasadniczą kwestią związaną z zapewnieniem ciągłości działania jest wyznaczenie odpowiedniej rezerwy czasowej, będącej w realiach biznesu swego rodzaju kompromisem między kosztami związanymi z zaangażowaniem danego kapitału[4] oraz bezpieczeństwem spełnienia ograniczeń kosztowych[5]. Należy zauważyć, że szacowanie czasu realizacji zdarzenia powinno być oparte na doświadczeniach oraz wynikach pomiarów procesów. Proces jest zatem przedmiotem oceny w ujęciu *ex post,* pozwalającym określić np., w jakiej części udało się osiągnąć założenia wejściowe, oraz *ex ante* będącym próbą wykorzystania informacji o zdarzeniach przeszłych dla prognozowania stanu przyszłego. Jakość takiej prognozy w dużej mierze determinowana jest jakością systemu zarządzania, a zwłaszcza funkcji monitoringu, ewidencjonowania i raportowania.

Kolejnym etapem w przyjętym modelu jest identyfikacja zagrożeń na poziomie procesów. W tym celu konieczne jest odwołanie się do wyodrębnionego zbioru dokumentów, a zwłaszcza definicji i opisów procesów czy map procesów. Wyodrębnione w dokumentacji modele procesów (schemat 5) są podstawą do identyfikacji zagrożeń na przyjętym poziomie istotności. Ich analiza jest podstawą do identyfikacji źródeł ryzyka. Jak widać, dla każdego działania można określić zbiór elementów, które należy interpretować w kontekście potencjalnych zagrożeń (tabela 3).

[4] Np. poprzez jego zamrożenie w postaci finalnego produktu, którego koszty zostaną pokryte w ustalonym czasie.

[5] Których przekroczenie może wiązać się np. z karami umownymi.



Schemat 5. Metamodel procesu w notacji UML. Źródło: [6]

Tabela 3

Wybrane wzorce identyfikacji ryzyka na podstawie metamodelu procesu

Klasa zdarzeń ze względu na:	Klasy zdarzeń	Wzorce ryzyka
Artefakt	– nie został wykonany, – traci cechę,	– jeżeli artefakt traci cechę, to aktywność przekracza zakładane koszty, – jeżeli artefakt nie został wykonany, to aktywność nie została wykonana,
Aktywność	– nie została wykonana, – zabiera więcej czasu niż przewidziano, – kosztuje więcej niż przewidziano, – traci rolę, – traci artefakt, – traci praktykę	– jeżeli aktywność X nie jest wykonana, to aktywność Y trwa dłużej, niż zakładano, – jeżeli aktywność trwa dłużej, niż zakładano, to rola traci zdolność, – jeżeli aktywność Z traci praktykę, to aktywność Z trwa dłużej, – jeżeli aktywność kosztuje więcej, to aktywność traci praktykę, – jeżeli aktywność nie została wykonana, to artefakt traci cechę
Rola	– nie jest przydzielona, – traci zdolność	– jeżeli rola nie została przydzielona, to aktywność nie została wykonana, – jeżeli rola traci zdolność, to artefakt traci cechę

Opracowanie własne na podstawie: [6]

Przyjęty poziom analizy (tabela 3) umożliwia wskazanie potencjalnych zagrożeń w oparciu o uniwersalne klasy zdarzeń oraz zidentyfikowane na ich podstawie wzorce ryzyka. Jak widać występowanie określonych typów zagrożeń może prowadzić do

ciągu zdarzeń obniżających ogólny poziom bezpieczeństwa organizacji, w aspekcie ciągłości procesów informacyjnych, produkcyjnych czy finansowych.

Obok przyjętej w prezentowanym modelu analizy metamodelu na potrzeby identyfikacji ryzyka można wykorzystać [19, s. 91], [1, s. 300-302]:

- technikę burzy mózgów,
- metodę delficką (opinie ekspertów),
- analizę przyczyn źródłowych,
- techniki oparte na diagramach (schematy blokowe, diagramy przyczynowo--skutkowe, diagramy wpływów),
- analizę SWOT (określenie silnych i słabych cech procesu oraz szans i zagrożeń wynikających z jego realizacji w otoczeniu),
- wywiady środowiskowe,
- kwestionariusze i listy pytań kontrolnych,
- dane historyczne (doświadczenie),

W kolejnym etapie zidentyfikowane wcześniej kluczowe procesy są przedmiotem analizy pod kątem zidentyfikowanych typów zagrożeń dla ciągłości ich realizacji, na podstawie których szacowane są wskazane wcześniej elementy miary ryzyka. Przedstawione w tabeli 3 wzorce ryzyka umożliwiają analizę każdego procesu w kontekście określonego katalogu zagrożeń oraz szacowanych strat związanych z ich wystąpieniem. Należy zauważyć, że realizacja tego etapu polega na określeniu:

- częstości występowania zagrożeń,
- potencjalnych strat wywołanych ich wystąpieniem,
- ekspozycji czynników szczególnie wpływających na poziom ogólnego ryzyka,
- podatności badanego obiektu na zagrożenia.

Działanie to wymaga analizy danych historycznych dotyczących przebiegu procesów. Przedstawione wcześniej komponenty ilościowej miary ryzyka wskazują na zasadność określenia podatności analizowanego obiektu na wystąpienie zagrożenia. Należy tu brać zatem pod uwagę ogół czynników (fizycznych, organizacyjnych, personalnych, administracyjnych) wpływających na zwiększenie prawdopodobieństwa wystąpienia zagrożenia utraty ciągłości działania.

W tabeli 4 przedstawiono przykładowe wielkości poziomu ryzyka dla zidentyfikowanych zagrożeń dla wyodrębnionych procesów kluczowych. W rozważnym przykładzie procesami, z którymi wiąże się najwyższy poziom ryzyka, są odpowiednio:

- **proces 2 (P2)** – szacowany poziom ryzyka 170 – zidentyfikowano trzy zagrożenia,
- **proces 4 (P4)** – szacowany poziom ryzyka 94,5 – zidentyfikowano jedno zagrożenie,
- **proces 1 (P1)** – szacowany poziom ryzyka 71 – zidentyfikowano trzy zagrożenia.

Tabela 4

Przykładowe zestawienie miar ryzyka dla procesów kluczowych

Proces	Symbol	Opis	Poziom częstości wystąpienia		Poziom strat		Współczynnik ekspozycji	Współczynnik podatności	VaR
			Wartość	Ranga	Wartość	Ranga			
P1	**R1**	Artefakt X_1 nie spełnia wymagań jakościowych	0,07	1	9	8	1	1	**8**
P2	**R2**	Rola R_1 traci umiejętność obsługi maszyny	0,33	5	7	6	1	1	**30**
P2	**R3**	Aktywność A_2 nie została wykonana → artefakt X_2 nie spełnia norm bezpieczeństwa	0,84	10	5	3	**1**	**2**	**60**
P4	**R4**	Aktywność A_1 nie została zrealizowana → Artefakt X_{21} nie został zrealizowany	0,64	9	8	7	**1,5**	**1**	**94,5**
P2	**R5**	Artefakt X_3 nie został dostarczony → Aktywność A_3 przekracza czas	0,21	4	10	10	**2**	**1**	**80**
P5	**R6**	Aktywność A_7 kosztuje więcej niż zakładano → Artefakt X_5 – nieefektywny	0,35	6	4	2	**1**	**1**	**12**
P3	**R7**	Aktywność A_6 traci praktykę → Aktywność A_6 trwa dłużej	0,14	2	9	9	**1**	**1**	**18**

Proces	Symbol	Opis	Poziom częstości wystąpienia		Poziom strat		Współczynnik ekspozycji	Współczynnik podatności	VaR
			Wartość	Ranga	Wartość	Ranga			
P1	**R8**	Artefakt X_7 nie został dostarczony → Aktywność A_{13} nie została wykonana	0,46	8	5	4	**1**	**1,5**	**48**
P6	**R9**	Aktywność A_{12} traci rolę R_5 → aktywność A_{21} trwa dłużej	0,38	7	1	1	1	1	**7**
P1	**R10**	Rola R_2 nie została przydzielona → Artefakt X_6 nie spełnia norm jakości	0,16	3	7	5	1	1	15

Opracowanie własne

W ten sposób możliwa jest selekcja procesów szczególnie podatnych na zagrożenia. Odnosząc się jeszcze raz do tabeli 4, można zauważyć, że wyszczególnione wcześniej procesy zostały scharakteryzowane jako szczególnie podatne na zagrożenia. W przypadku procesów 2 i 4 czynnikiem determinującym poziom ryzyka był również ich wpływ na ogólną kondycję organizacji (np. skuteczność realizacji celów) wskazującą na potrzebę wyeksponowania tych procesów jako szczególnie istotnych ze względu na przyjęte kryteria (cechy systemowe).

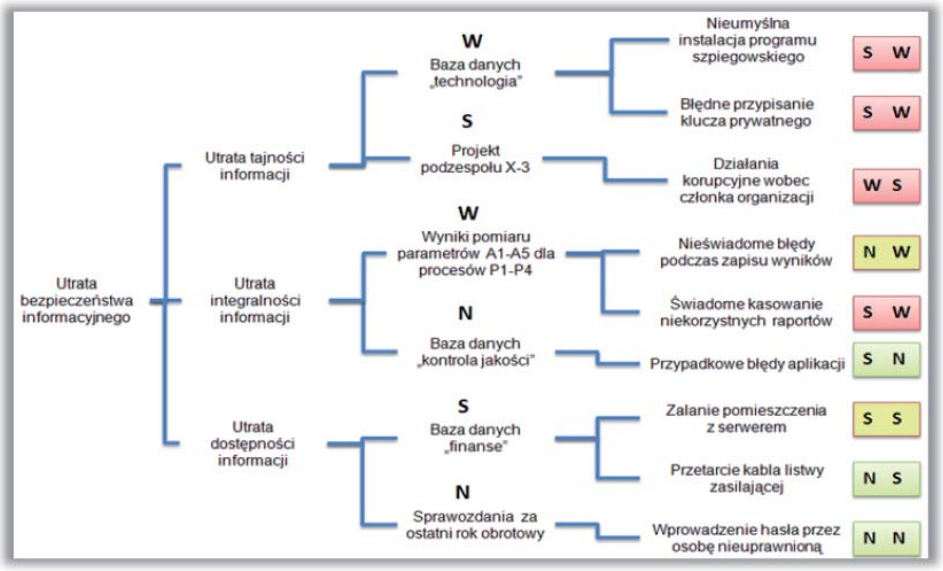
Na podstawie dotychczasowej analizy można zauważyć, że zagrożenia będące źródłem ryzyka dla ciągłości działania organizacji mogą mieć charakter złożony. Narzędziami dobrze oddającymi problem zagrożeń dla ciągłości działania są drzewa oraz wygenerowane na ich podstawie scenariusze. Tak więc kolejnym krokiem w przyjętym modelu jest generowanie drzew zagrożeń, będących modyfikacją powszechnie wykorzystywanych w zarządzaniu drzew użyteczności. Omawiane narzędzie można wykorzystać do identyfikacji i ewaluacji poziomu zagrożeń w wielu obszarach działania organizacji. Jednym z zasadniczych problemów zapewnienia ciągłości działania, zwłaszcza w kontekście organizacji procesowych, jest obszar bezpieczeństwa informacyjnego.

Projektowanie drzew zagrożeń wymaga [19, s. 82-85]:

- określenia natury rozważanego problemu (wskazania obszaru identyfikacji zagrożeń),
- określenia atrybutów analizowanego obiektu,
- przypisania zasobów do wyselekcjonowanych obiektów,
- określenia poziomu strat (w postaci wartości lub skali liczbowej/literowej),
- przypisania zagrożeń do wyszczególnionych obiektów,
- określenia poziomu istotności danego zagrożenia,
- przypisania priorytetów dla zagrożeń na podstawie związku poziomu strat oraz poziomu istotności.

Na schemacie 6 przedstawiono przykładowe drzewo identyfikacji zagrożeń dla bezpieczeństwa informacyjnego organizacji. Zgodnie z przedstawionym wcześniej modelem po wyznaczeniu obszaru analizy dokonano jego określania kluczowych atrybutów dla zapewnienia bezpieczeństwa, tj. tajności, integralności i dostępności. Na podstawie wyodrębnionych do tej pory procesów szczególnie podatnych na zagrożenia dokonano zaklasyfikowania kluczowych zasobów oraz przyporządkowano wielkość strat wynikających z utraty danego atrybutu bezpieczeństwa dla danego zasobu w skali:

- niski (**N** – 1),
- średni (**S** – 2),
- wysoki (**W** – 3).



Schemat 6. Przykładowe drzewo zagrożeń dla problemu utraty bezpieczeństwa informacyjnego
Opracowanie własne na podstawie: [19]

Następnie przy wykorzystaniu omówionych wcześniej technik i narzędzi dokonano identyfikacji oraz przyporządkowania zagrożeń do zasobów. Dla ustalenia priorytetów poszczególnych zagrożeń dokonano oceny ich istotności, tworząc uporządkowane pary: [IS, PS][6]. Zgodnie z odpowiadającymi danym poziomom wartościom liczbowym wyodrębniono trzy obszary oddziaływania:

- czerwony – najwyższy priorytet – wartość[7] z przedziału 5-6,
- żółty – średni priorytet – wartość z przedziału 3-4,
- zielony – niski priorytet – wartość z przedziału 1-2.

Jak już wcześniej wspomniano, zakres identyfikacji jest wprost proporcjonalny do jej kosztów. Dlatego dokonana taksonomia jest podstawą do nadawania priorytetów w tworzeniu scenariuszów realizacji/wystąpienia zagrożeń oraz zawężenia przedmiotu działania. Dokonując takiego podziału, należy zakładać, że firma jest w stanie zaakceptować ryzyko związane z wystąpieniem określonego zagrożenia. Można np. przyjąć, że firma akceptuje zagrożenia na najniższym poziomie – oznaczonym kolorem zielonym. Pozostałe zagrożenia wymagają tworzenia scenariuszy, czyli serii zdarzeń, które począwszy od zdarzenia inicjującego, przez zdarzenia pośrednie prowadzą do realizacji/wystąpienia zagrożeń.

[6] IS – poziom istotności, PS – poziom strat.
[7] Określana na podstawie iloczynu IS × PS.

Podobnie jak w przypadku samej identyfikacji zagrożeń, generowanie scenariuszy wymaga wykorzystania szeregu narzędzi i technik, a zwłaszcza metod heurystycznych, tj. burzy mózgów czy metody delfickiej, umożliwiających usuwanie skrajności (np. wygenerowanych na etapie burzy mózgów). Przy realizacji scenariuszy niezwykle ważna jest dbałość o spełnianie szeregu zasad [19, s. 88]:

- zapewnienie możliwości swobodnego, pozbawionego krytyki wypowiadania się,
- rozłożenie akcentów rozmowy w miarę możliwości równoważnie między członków organizacji,
- ograniczanie przerw, a zwłaszcza opuszczania miejsca pracy przez analityków,
- wyraźne rozgraniczanie kwestii podatność – zagrożenie – skutek,
- ograniczanie dyskusji poza głównym forum.

Wynikiem sesji burzy mózgów są scenariusze przedstawione w tabeli 5.

Tabela 5

Scenariusze wystąpienia zagrożeń

Atrybut bezpieczeństwa	**Zdarzenie inicjujące**	**Zdarzenia pośrednie**		**Zidentyfikowanie zagrożenie**
Tajność	Wyniesienie optycznego nośnika danych poza obszar firmy	Wykorzystywanie nośnika na własny użytek (np. w domu)	Nieświadomy zapis programu szpiegowskiego na nośniku	Nieumyślna instalacja programu szpiegowskiego
Tajność	Błędne przypisanie pracownika do zespołu realizacji procesu	Brak weryfikacji otrzymanej listy ze strukturą zespołów zapisaną w bazie danych „Kadry”		Błędne przypisanie klucza prywatnego
Tajność	Przypisanie zapisom atrybutu „tajne”	Udostępnienie komputera koledze z innego zespołu	Sprzeczka z właścicielem procesu – groźba zwolnienia	Działania korupcyjne wobec członka organizacji
Integralność	Analiza sprawozdań za ostatni cykl	Publiczna krytyka pracownika	Groźba zwolnienia sformułowana przez właściciela procesu	Świadome kasowanie niekorzystnych raportów
Integralność	Nieobecność pracownika podczas szkolenia	Opóźnienia w realizacji bieżących zleceń – pośpiech i praca po godzinach		Nieświadome błędy podczas zapisu wyników
Dostępność	Remont instalacji sanitarnych	Brak kontroli realizacji zlecenia		Zalanie pomieszczenia z serwerem

Opracowanie własne

Analiza zapisów w tabeli 5 potwierdza zasadność tworzenia scenariuszy zagrożeń i w pełni odpowiada koncepcji systemowego spojrzenia na problem ryzyka utraty ciągłości działania. Na ich podstawie możliwe jest bowiem identyfikowanie przyczyn występowania zagrożeń oraz podejmowanie działań zmniejszających podatność organizacji na zidentyfikowane zdarzenia inicjujące i pośrednie. Tak więc konsekwencją tworzenia scenariuszy jest ograniczenie podatności na zagrożenia wynikające z błędów natury organizacyjnej. Wskazane stwierdzenie potwierdza zasadność analizowania procedury zarządzania ciągłością działania w aspekcie jej cyklicznego charakteru. Można bowiem zauważyć, że celem zarządzających w omawianym obszarze nie jest eliminacja zagrożeń, lecz zmniejszenie podatności systemu na ryzyko ich wystąpienia (schemat 7).

Schemat 7. Elementy systemu reagowania na zagrożenia ciągłości działania. Opracowanie własne na postawie: [21, s. 6-7]

Jak widać (schemat 7), zdolność organizacji na reagowania na zakłócenia w jej prawidłowym funkcjonowaniu wymaga stałego doskonalenia wykształconego i sformalizowanego mechanizmu. Można zatem powiedzieć, że jednym z zasadniczych problemów w kontekście zarządzania ciągłością działania jest doskonalenie opracowywanych i wdrażanych procedur umożliwiających standaryzację działań w tym zakresie.

7. Wnioski i podsumowanie

Zarządzanie ciągłością działania należy traktować jako jeden z integralnych obszarów zapewnienia bezpieczeństwa organizacji. Koncepcja podejścia procesowego w zarządzaniu, traktowana jako środek zwiększania efektywności działania, sprawia, że identyfikowane kiedyś zagrożenia związane z fizycznym środowiskiem realizacji produktów nabierają nowego znaczenia. Rozproszone miejsca tworzenia wspólnej

wartości wymagają bowiem przeniesienia ciężaru pracy na środowisko sieciowe, zwłaszcza za pomocą sieci Internet. Dlatego jednym z zasadniczych problemów współczesnej organizacji jest zapewnienie informacyjnej ciągłości działania.

Należy zauważyć, że podejmowana tematyka ma charakter interdyscyplinarny i jest ściśle powiązana z aspektem zarządzania ryzykiem i bezpieczeństwem organizacji. Dlatego szereg metod, narzędzi i technik dla ww. obszarów jest wspólny i wymaga integracji.

Prezentowany w pracy model identyfikacji zagrożeń wskazuje na konieczność rozpatrywania tego problemu w aspekcie systemowym. Tak więc działania zmierzające do zapewnienia ciągłości realizowanych procesów zwracają szczególną uwagę na problem specyfiki procesu, zakresu i sposobu jego definiowania oraz miejsca systemów informatycznych w działaniu współczesnej organizacji. Rozpatrywanie zagrożeń w aspekcie określonych miar ryzyka umożliwia bezpośrednie połączenie problematyki ciągłości działania w obszarach informacyjnym, logistycznym, jakościowym czy finansowym.

Podsumowując, należy stwierdzić, że we współczesnych warunkach gospodarowania zasoby informacyjne należy traktować jako strategiczne, decydujące o realizacji celów przedsiębiorstwa. Zasadne wydaje się zatem traktowanie tej grupy zasobów w kategorii czynnika krytycznego dla zachowania ciągłości działania, zwłaszcza w przypadku organizacji procesowych o zdywersyfikowanych źródłach zasobów.

LITERATURA:

1. *A Guide to the Project Management Body of Knowledge*, Fourth Edition, wydanie polskie, MT & DC, Warszawa 2009.
2. K. Ficoń, *Inżynieria zarządzania kryzysowego: podejście systemowe*, wyd. BEL Studio, Warszawa 2007.
3. *Good Practice Guidelines 2002*, Business Continuity Institute 2002
4. *Good Practice Guidelines 2008*, Business Continuity Institute 2008.
5. R.W. Griffin, *Podstawy zarządzania organizacjami*, PWE, Warszawa 2004.
6. Z. Huzar, Z. Mazur (red. nauk.), *Problemy i metody inżynierii oprogramowania*, Wyd. Naukowo-Techniczne, Warszawa 2003.
7. R. Jakubczak, J. Flis (red. nauk.), *Bezpieczeństwo narodowe Polski w XXI wieku: wyzwania i strategie*, wyd. Bellona, Warszawa 2006.
8. T.T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania = Busines continuity management*, wyd. Difin, Warszawa 2009.
9. B. Klimczak, *Mikroekonomia*, wyd. Akademii Ekonomicznej im. Oskara Langego, Wrocław 1998.
10. S. Marek, M. Białasiewicz (red. nauk.), *Podstawy nauki o organizacji*, PWE, Warszawa 2008.
11. NFPA 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs*, 2007 Edition.

12. PN-IEC 62198:2005: *Zarządzanie ryzykiem przedsięwzięcia. Wytyczne stosowania*, PKN, Warszawa 2005.
13. *Słownik terminów z zakresu bezpieczeństwa narodowego*, AON, Warszawa 2002.
14. J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, PAN, Warszawa 1996, s. 18.
15. T. Szczurek, *Resort obrony narodowej w zarządzaniu kryzysowym w latach 1989-2009*, wyd. WAT, Warszawa, 2009.
16. Ustawa z dn. 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (DzU z 2007 r. Nr 89, poz. 590 z pózn. zm.).
17. J. Walas-Trębacz, J. Ziarko, *Podstawy zarządzania kryzysowego: Cz. 2. Zarządzanie kryzysowe w przedsiębiorstwie*, wyd. Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2011.
18. A. Warchał (red. wyd.), „Nowoczesne systemy zarządzania. Zeszyt 3", WAT, Warszawa 2008.
19. P. Zaskórski (red. nauk.), *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa 2011.
20. P. Zaskórski, *Informacyjno-biznesowa ciągłość działania firmy*, (w:) „Zeszyty naukowe" nr 5, red. nauk. P. Zaskórski, wyd. Warszawska Wyższa Szkoła Informatyki, Warszawa 2011.
21. J. Zawiła-Niedźwiecki, *Ciągłość działania organizacji*, wyd. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.

Identification of the threats to continuity of the organization

Abstract. In this article an attempt is made to identify the determinants of the organisation's safety within security levels. Safety is a system-wide category and a complex function, which is conditioned by the risk level. Modern organisations models based on processes indicate that one should draw special attention to information resources. Those in today's global markets are becoming strategically more significant. Therefore, one of the basic problems of modern organisation management seems to be an information security problem, especially maintaining business continuity of the terms of information, logistics and finance. The connection between highlighted areas needs finding the universal platform of the integration, which enables the efficient realisation of goals. The existence of a dispersed organisation is determined by a number of threats, which result from organisational specifications, as well as from its environment. Therefore, the matter of organisational security needs to be focused first, on how to determine the threats identification for its business continuity.