Dariusz Andrzej Magierek
Wydział Humanistyczny
Politechniki Koszalińskiej
ORCID: 0000-0002-7835-3282
e-mail: dariusz.magierek@tu.koszalin.pl

Ciągłość działania w przedsiębiorstwie z punktu widzenia bezpieczeństwa

Streszczenie

Ze względu na szybko zmieniające się otoczenie przedsiębiorstwa przykładają coraz większą uwagę do zarządzania ciągłością działania. Wiele mówi się o zagrożeniu współczesnego świata, jakim jest uzależnienie od technologii, które powoduje, że ciągłość działania staje się podstawowym czynnikiem sukcesu wielu organizacji. Świadome przedsiębiorstwa zabezpieczają się na różne sposoby, żeby nie stracić zaufania klientów, nie stracić przychodów, a także zapobiec utracie ewentualnych korzyści.

Autor podjął problematykę właściwego działania przedsiębiorstwa z punktu widzenia jego bezpieczeństwa. W związku z tym ważne jest zarządzanie ciągłością jego działania, co przekłada się bezpośrednio na bezpieczeństwo przedsiębiorstwa.

Słowa kluczowe

przedsiębiorstwo, bezpieczeństwo, zarządzanie

Wstęp

Ze względu na zapewnienie przedsiębiorstwu bezpieczeństwa jest tworzona analiza ryzyka, również operacyjnego, a na jej podstawie opracowuje się procedury i plany awaryjne, które mają uchronić przedsiębiorstwo na wypadek incydentów, kryzysów czy katastrof. Czy w tych planach jest miejsce dla marketingu? Głównym celem badawczym niniejszego artykułu jest zbadanie czy ciągłość działania organizacji wpływa na bezpieczeństwo przedsiębiorstwa? W związku z powyższym

zostaną przedstawione pojęcia „bezpieczeństwo przedsiębiorstwa" i „ciągłość działania", a także jak zarządza się nią w organizacji oraz jakich narzędzi można do tego użyć. Ponadto zostanie omówiona istota analizy ryzyka w przedsiębiorstwie, procedury oraz plany awaryjne tworzone w celu zapewnienia ciągłość działania w przedsiębiorstwie, a także standardy, które muszą spełniać plany ciągłości działania, oraz korzyści z przygotowania i odpowiedniego zabezpieczenia się w celu utrzymania ciągłości działania w zmieniającym się środowisku.

Pojęcie bezpieczeństwa przedsiębiorstwa

Współcześnie biznes jest coraz bardziej wymagający, a warunki do jego prowadzenia coraz bardziej zmienne. Zaczynając od małych przedsiębiorstw, a kończąc na dużych korporacjach, bez względu na branże czy klienta, coraz większe wyzwania stoją przed firmami i ich prowadzącymi. Ostatnie lata pokazują jak bardzo elastyczne powinno być przedsiębiorstwo, żeby dostosować się do zmiennego środowiska i warunków.

Organizacje określają swoje misje i cele strategiczne w każdym z obszarów działalności[1]. Na drodze do osiągnięcia celu istnieje ryzyko napotkania pewnych barier mających wszelakie podłoże. Mogą to być bariery zarówno ekonomiczne, jak i komunikacyjne czy informacyjne[2].

Poziom osiągania tych celów jest uzależniony od odpowiedniego planu i zabezpieczenia się przed ryzykiem, które organizacja może napotkać. Skuteczność tego planu jest zdeterminowana odpowiednim podejściem i jego dobrym przygotowaniem, a także zachowaniem odpowiednich procedur bezpieczeństwa[3].

Współcześnie obserwuję się, że bardzo wzrosła świadomość ryzyka, możliwości jego pojawienia się i zakłócenia poprawnego funkcjonowania firmy[4]. Organizacje zabezpieczają się na wiele sposobów, żeby utrzymać ciągłość działania przedsiębiorstwa, utrzymać jego zasoby i procesy na wypadek pojawienia się zewnętrznych bądź wewnętrznych zakłóceń.

1 H Bieniok i in., *Metody sprawnego zarządzania*, Warszawa 2004 s. 50.
2 *Marketing przedsiębiorstw przemysłowych*, red. W. Mantura, Poznań 2000, s. 12.
3 P. Zaskórski, *Informacyjno-biznesowa ciągłość działania firmy*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2011, nr 5, s. 218.
4 J. Zawiła-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*, Kraków–Warszawa 2013, s. 14.

Ostatnie dziesięciolecia cechuje rosnąca zmienność i złożoność warunków działania podmiotów gospodarczych, co powoduje, że nieustannie poszukuje się sposobów minimalizacji ryzyka towarzyszącego podejmowanym decyzjom, zwłaszcza strategicznym. Dlatego tak ważne jest, żeby wszelkie procesy w przedsiębiorstwie były poprawnie zabezpieczone i w kryzysowym dla firmy momencie pomogły jej przetrwać bez zakłóceń, a co za tym idzie, pomogły jej utrzymać ciągłość biznesową. Bezpieczeństwo w przedsiębiorstwie jest ściśle powiązane z ryzykiem i ciągłością działania. W organizacji biznesowej możemy wyróżnić następujące rodzaje bezpieczeństwa:

- środowiskowe,
- procesowe,
- pracy,
- osobowe,
- informacji,
- informatyczne,
- fizyczne,
- techniczne[5].

Ponadto ze względu na aspekty związane z bezpieczeństwem wyróżniamy:

- zarządzanie w kryzysie,
- ochronę wartości materialnych i niematerialnych,
- ciągłość działania,
- ryzyko zawodowe[6].

Zabezpieczenie wyżej wymienionych obszarów pozwala zapewnić funkcjonowanie przedsiębiorstwa. Szczególną ochroną można objąć całą organizację bądź poszczególną jednostkę (np. jeden z działów). Bezpieczeństwo jest ważne także w kontekście współpracy z jednostkami zewnętrznymi takimi jak firmy outsourcingowe. Tutaj firma również powinna mieć obraną strategię na wypadek wystąpienia zakłóceń lub zagrożeń, które mogą wpłynąć na kontynuację biznesu. W kontekście zarządzania ryzykiem termin „bezpieczeństwo" to określony stan rzeczywistości społecznej oraz podmiotowej. Jest także dobrem społecznym w aspekcie wartości humanistycznych, praw człowieka czy potrzeb ludzkich[7].

5 *Ryzyko operacyjne w naukach o zarządzaniu*, red. nauk. I. Staniec, J. Zawiła-Niedźwiecki, Warszawa 2015, s. 119.

6 Ph. Kotler, G. Armstrong, J. Saunders, V. Wong, *Marketing. Podręcznik europejski*, Warszawa 2002, s. 45.

7 E. Michalski, *Marketing*, Warszawa 2004, s. 187–189.

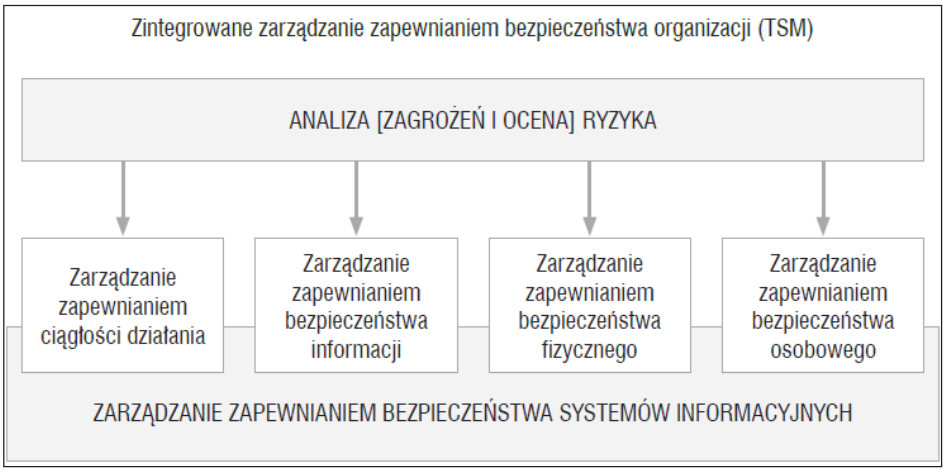
Zgodnie z klasycznymi badaniami Maslowa poczucie bezpieczeństwa jest drugą z podstawowych potrzeb człowieka. Samo zapewnienie przedsiębiorstwu bezpieczeństwa jest także działaniem prewencyjnym, ponieważ polega na rozwiązaniach, których głównym celem jest zapobieganie pojawieniu się sytuacji krytycznej poprzez dostrzeganie czynników zagrożenia, a także wczesne monitorowanie charakterystycznych symptomów wskazujących na możliwość pojawienia się zagrożenia dla działalności. Jeżeli te kroki zawodzą i dojdzie do zakłóceń działalności organizacji, to wtedy przychodzi pora na zaplanowaną i zorganizowaną aktywność naprawczą, której zadaniem jest zapewniać akceptowalną zdolność do utrzymywania ciągłości działania[8].

Istotnym zagadnieniem jest także kwestia zapewnienia bezpieczeństwa zasobów organizacji. Jeżeli tych zasobów brak bądź można zaobserwować ich niedostatek, to tworzy również zagrożenie. Zachowanie zasobów organizacji na odpowiednim poziomie to przejaw zapewnienia efektywnego bezpieczeństwa[9], które jest kojarzone z rodzajem zasobu, co znajduje swoje odzwierciedlenie w organizacji i możemy podzielić je na dwie kategorie, tj. ochronę fizyczną, techniczną i bezpieczeństwo osobowe, a także bezpieczeństwo informacji i systemów informatycznych oraz zapewnienie ciągłości działania.

Zamiast sformułowania „zarządzanie ryzykiem operacyjnym" możemy też spotkać określenie „zarządzanie zapewnianiem bezpieczeństwa operacyjnego", w pełnym ujęciu jako zintegrowane zarządzanie zapewnianiem bezpieczeństwa" (TSM – total security management)[10].

Każdy z obszarów TSM ma swoje zasady, dobre praktyki i odpowiednie metody mające na celu zapewnienie bezpieczeństwa organizacji (schemat 1). Wyróżnienie kwestii bezpieczeństwa systemów informacyjnych zostało pokazane po to, żeby podkreślić obecność informacji w zarządzaniu oraz informatyki w działalności organizacji. Pominięcie w TSM ryzyka związanego z niedoborem zasobów finansowych jest powiązane z zarządzaniem ryzykiem biznesowym i ryzykiem finansowym oraz z tym, że jest ono rozwiązywane w ramach zarządzania tymi rodzajami ryzyka[11].

8 Ibidem, s. 85.
9 Ibidem, s. 84.
10 J. Zawiła-Niedźwiecki, op. cit., s. 84.
11 Ibidem



Źródło: M. Blim, M. Byczkowski, J. Zawiła-Niedźwiecki, *Zintegrowane zarządzanie bezpieczeństwem organizacji*, [w:] *Systemy informatyczne. Bankowość i finanse,* red. F. Marecki, J.K. Grabara, J. Nowak, Warszawa 2005, s. 12.

Schemat 1. Koncepcja zintegrowanego zarządzania bezpieczeństwem

Zapewnianie bezpieczeństwa organizacji, zwłaszcza w ujęciu TSM, jest odnoszone do poszczególnych rodzajów zasobów[12]. Jak już zostało wspomniane, wyróżniamy bezpieczeństwa: osobowe, fizyczne i techniczne, finansowe oraz informacji i informatyczne. Zapewnianie bezpieczeństwa fizycznego i technicznego wywodzi się z następujących podstawowych przesłanek:

– potrzeby precyzyjnego zakreślenia granic lokalizacji organizacji oraz stref wykonywania poszczególnych funkcji i usług na rzecz klientów, a także przez pracowników organizacji oraz na ich rzecz,

– potrzeby wyobrażenia sobie i zdefiniowania potencjalnych zagrożeń oraz możliwych scenariuszy ich realizowania się jako zakłóceń normalnej pracy organizacji,

– potrzeby zorganizowania procesów wykonywania funkcji organizacji, zapewniania ochrony fizycznej oraz dobierania i stosowania rozwiązań ochrony, w tym także technicznych[13].

Z kolei zapewnianie bezpieczeństwa osobowego wynika z następujących głównych przesłanek:

12 M. Blim, M. Byczkowski, J. Zawiła-Niedźwiecki, op. cit., s. 12.
13 *Ryzyko operacyjne w naukach*…, s. 22.

– potrzeby doboru i zatrudniania pracowników odznaczających się wysokim poziomem morale i odpowiedzialności (tzw. reguła prawości),

– wymogu adekwatności umiejętności zawodowych pracowników do wykonywanych zadań oraz potencjalnej zdolności do adaptowania się do zmieniających się wymagań, co może być pochodną rozwoju organizacyjnego i biznesowego podmiotu lub konkurencyjnego rozwoju rynku (tzw. reguła fachowości),

– potrzeby doboru pracowników oraz organizacji pracy, które z dwu stron współprzyczyniają się do stworzenia atmosfery i warunków do identyfikacji powodzenia zawodowego[14].

Jeżeli chodzi o bezpieczeństwo informacji, to wywodzi się z następujących podstawowych przesłanek:

– zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. reguła poufności),

– zapewnienia zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania (tzw. reguła integralności),

– zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. reguła dostępności)[15].

Określa się trzy poziomy merytorycznego zarządzania bezpieczeństwem informacji:

– polityka bezpieczeństwa informacji – określenie wymagań bezpieczeństwa na poziomie całej organizacji i w odniesieniu do wszystkich grup informacji oraz wszystkich systemów i rozwiązań służących przetwarzaniu tych informacji (w tym przechowywaniu i transportowaniu),

– grupa informacji – uszczegółowienie wymagań bezpieczeństwa dla grup informacji, wyodrębnianych przede wszystkim jako autonomiczna klasa informacji służących określonym zagadnieniom, przetwarzanych w określonym pionie funkcjonalnym (np. informacje finansowe, informacje kadrowe, informacje o klientach itd.), ale także niekiedy objętych odrębnymi przepisami prawa ogólnego, np. informacje niejawne, informacje o danych osobowych,

– system przetwarzania – spełnienie wymagań bezpieczeństwa przez systemy także tradycyjne, ale przeważnie informatyczne, które przetwarzają określone grupy informacji na rzecz pewnej kategorii użytkowników[16].

14 Ibidem.

15 K. Lidermann, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017, s. 12.

16 M. Rydel, *Komunikacja jako element marketingu*, [w:] *Komunikacja marketingowa*, red. idem, Gdańsk 2001, s. 21.

Jeżeli mowa o bezpieczeństwie informacji, to warto wspomnieć o zaproponowanym przez Stowarzyszenie Audytorów Informatycznych (Information Security Audit and Control Association – ISACA[17]) modelu, który pokazuje poziomy dojrzałości zarządzania bezpieczeństwem informacji (schemat 2). Zarządzanie zapewnianiem bezpieczeństwa przedsiębiorstwa jest prowadzone w zależności od obszaru, którego dotyczy[18].

Stopień 0 Brak świadomości	– brak zdefiniowania wymagań bezpieczeństwa – bezpieczeństwo traktowane jako problem poszczególnych użytkowników
Stopień I Początkowy	– świadomość potrzeby – kierownictwo uważa to za problem służb IT (typu: prawa dostępu, ochrona antywirusowa)
Stopień II Intuicyjny	– próby tworzenia zabezpieczeń – brak jednolitego podejścia – efekty zależne od zaangażowania osób zainteresowanych
Stopień III Zdefiniowany	– zdefiniowane zasady (w tym polityka bezpieczeństwa) w całej organizacji – procedury bezpieczeństwa są utrzymywane i komunikowane – brak kontroli stosowania
Stopień IV Zarządzany	– jednolite podejście dla wszystkich komórek i wszystkich rozwiązań – obowiązuje perspektywa biznesu – funkcjonuje mechanizm kontroli stosowania
Stopień V Optymalizowany	– świadome zarządzanie ryzykiem – zgodność strategii bezpieczeństwa ze strategią biznesową – zapewnianie bezpieczeństwa jako proces (wiedza, doskonalenie)

Źródło: M. Forystek, *Audyt informacyjny*, Zgierz 2005, s. 23.

Schemat 2. Poziomy dojrzałości zarządzania bezpieczeństwem informacji

17 Zob. https://engage.isaca.org/warsawchapter/home [dostęp: 3.02.2025].
18 J. Zawiła-Niedźwiecki, op. cit., s. 92.

W zależności od stopnia dojrzałości organizacji zmienia się podejście do bezpieczeństwa, a także sposób zarządzania ryzykiem. Odpowiada za nie każda jednostka w firmie, ponieważ każda z nich może stworzyć potencjalne zagrożenie. Dlatego tak ważna jest ochrona danych w różnych działach zarówno IT, jak i zasobów ludzkich, który dysponuje informacjami o pracownikach czy działu obsługi klienta mającego dane klientów. Wszystkie te obszary w firmie powinny być zabezpieczone[19]. Ważna jest również świadomość użytkowników, którzy je przetwarzają.

Zarządzenie ciągłością działania jako podstawowe narzędzie w procesie zapewnienia bezpieczeństwa przedsiębiorstwa

Negatywne zjawiska, kryzysy czy nieprzewidziane zdarzenia wpływają na ludzkie postawy[20]. Pod koniec XX wieku powstała dyscyplina zwana „zarządzanie ryzykiem". Jednocześnie menadżerowie zaczęli zastanawiać się jak utrzymywać ciągłość działania przedsiębiorstwa, którym zarządzają? Chyba zarządzają[21]. Współcześnie coraz bardziej rozwija się pojęcie kontroli jakości w firmie, co ma bardzo istotny wpływ na ciągłość działania zarówno dużych spółek, jak i małych podmiotów gospodarczych[22].

Ciągłość działania oznacza zdolność funkcjonowania w sytuacji wystąpienia np.: klęsk żywiołowych, nieszczęśliwych wypadków, aktów sabotażu, ataków terrorystycznych lub poważnych awarii najważniejszych maszyn i urządzeń produkcyjnych[23]. Trzeba podkreślić, że problematyka zapewniania ciągłości jest dość trudna do wyodrębnienia z elementów, które składają się na zarządzanie ryzykiem oraz zapewnianie bezpieczeństwa w firmie[24]. Wzorcem w systematycznym podejściu do zapewniania ciągłości działania jest koncepcja Business Continuity Management (BCM), którą Business Continuity Institute[25] zdefiniował jako holistyczny proces zarządzania, który ma na

19 A. Sznajder, *Marketing. Encyklopedia biznesu*, t. 1, Warszawa 1995, s. 475.
20 T.T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania*, Warszawa 2009, s. 146.
21 Ibidem, s. 23.
22 Ibidem, s. 43.
23 Ibidem, s. 44.
24 J. Zawiła-Niedźwiecki, op. cit., s. 140.
25 Zob. www.thebci.org [dostęp: 15.02.2025].

celu określenie potencjalnego wpływu zakłóceń na organizację i stworzenie warunków budowania odporności na nie oraz zdolności skutecznej reakcji w zakresie ochrony kluczowych interesów właścicieli, reputacji i marki organizacji, a także wartości osiągniętych w jej dotychczasowej działalności[26].

Do powyższej definicji odwołują się również normy ISO 22301, BS 25777 i BS 25999, które rekomendują spiralny cykl procesu zarządzania zapewnianiem ciągłością działania (schemat 3). W tym miejscu warto wspomnieć również o holistycznym procesie zapewniania ciągłości działania zaproponowanym również przez Business Continuity Institute (schemat 4), która identyfikuje potencjalne zagrożenia organizacji wraz ze skutkami, tych zagrożeń dla biznesu. Żeby dobrze zrozumieć cały ten proces, należy zacząć od cyklu życia zarządzania ciągłością działania, która przedstawia się następująco:

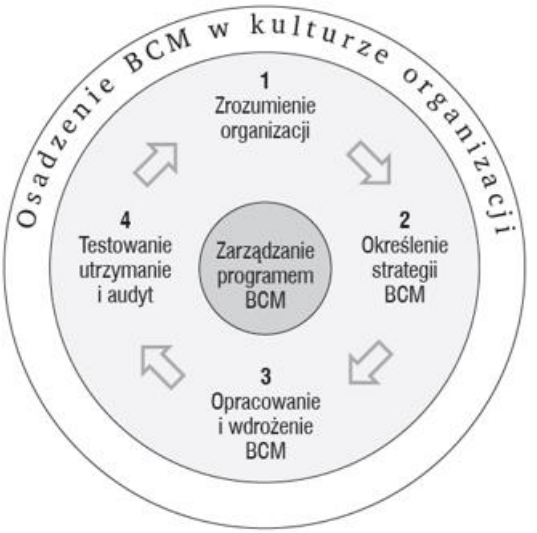
1) zrozumienie organizacji,
2) określenie strategii,
3) opracowanie i wdrożenie reakcji,
4) ćwiczenia, utrzymanie i przegląd[27].

Wszystkie te zadania, wykonywane w odpowiedniej kolejności, pomagają w zarządzaniu przedsiębiorstwem w razie wystąpienia sytuacji mogących zakłócić ciągłość funkcjonowania firmy[28].

Żeby zachować ciągłość funkcjonowanie przedsiębiorstwa, należy je na taką okoliczność przygotować. Zgodnie z przeprowadzonymi badaniami przez Janusza Zawiła-Niedźwieckiego, autora książki o zarządzaniu ryzykiem operacyjnym, możemy wyróżnić pięć podstawowych czynności składających się na plan przygotowań przedsiębiorstwa na wypadek wystąpienia sytuacji kryzysowej[29]:

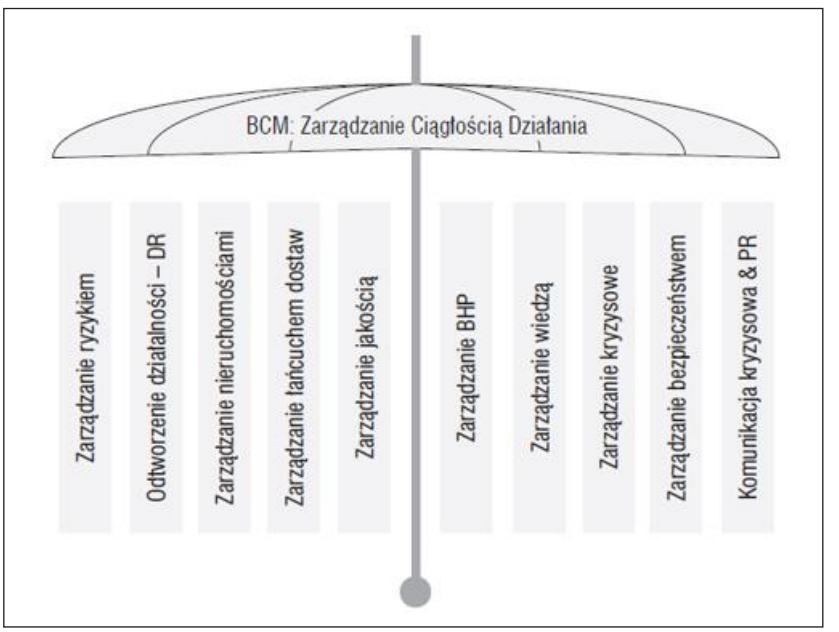
1) ustalenie, co jest krytyczne dla organizacji, jakie zasoby i procesy mogłyby zostać zagrożone i w jakiej sytuacji,
2) określenie, w jaki sposób organizacja będzie osiągać cel, jak spełni biznesowe wymagania związane z zapewnieniem ciągłości, w jakiej kolejności oraz w jaki sposób,

26 P. Waniowski, D. Sobotkiewicz, M. Daszkiewicz, *Marketing – teoria i przykłady*, Warszawa, 2010, s. 34.
27 BS 25999-2: Business Continuity Management – Specification, London 2007, s. 3.
28 P. Waniowski, D. Sobotkiewicz, M. Daszkiewicz, op. cit., s. 35.
29 J.L. Lambin, *Strategiczne zarządzanie marketingowe*, Warszawa 2001, s. 21–22.



Źródło: Norma BS 25999: Business Continuity Management – Specification, London 2007.

Schemat 3. Modelowy cykl zarządzania zapewnianiem ciągłości działania (BCM)



Źródło: *Business Continuity Institute*, https://www.thebci.org [dostęp: 15.02.2025].

Schemat 4. Holistyczny proces zarządzania zapewnianiem ciągłości działania

3) stworzenie rozwiązań, które zapewnią ciągłość i będą ściśle powiązane z charakterem organizacji,

4) implementacja tych rozwiązań, przeprowadzenie testów zazwyczaj w warunkach symulowanych, co pomaga przyszykować się do sprostania zagrożeniu w sytuacji rzeczywistej,

5) założenie, że problematyka dotyczy wszystkich pracowników, dlatego każdy z nich powinien znać rozwiązania odnośnie do jego obszaru i stanowiska. Powinien również aktywnie uczestniczyć w ich opracowaniu[30].

Zakłócenia są obiektem działań określanych jako powszechnie rozumiana polityka zapewniania ciągłości działania. Wobec tego można stwierdzić, że postępowanie, które służy zapewnianiu ciągłości działania, jest podobne do postępowania mającego na celu zabezpieczanie przed zagrożeniami. Różni je jedynie czas i charakter oddziaływania na zagrożenia. Obydwa uzupełniają się tak, żeby zapewnić przedsiębiorstwu oczekiwaną odporność na czynniki zewnętrzne, które mogą zakłócić codzienną działalność[31].

Podstawowe obszary zapewniania ciągłości działania to:

– mechanizm reagowania organizacji na zakłócenia,

– proces rozwijania ww. mechanizmu zdolności reagowania na zakłócenia,

– proces zarządzania bieżącą zdolnością zapewniania ciągłości działania oraz jej stałym doskonaleniem.

Z kolei na reagowanie na zakłócenia składają się:

– struktura organizacyjna odpowiednia do zadania zapewniania ciągłości, uzupełniająca ogólną strukturę organizacyjną,

– formalne uregulowania określające relacje w strukturze organizacyjnej związane z zadaniem zapewniania ciągłości,

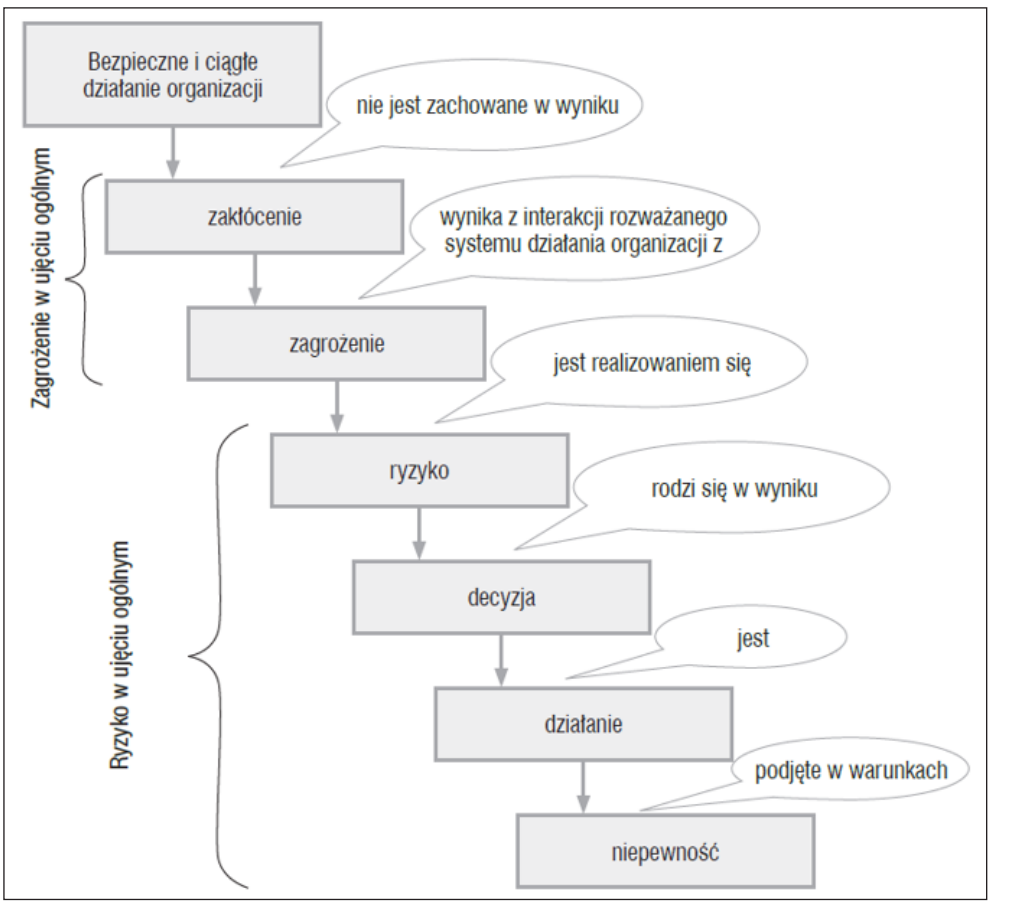
– utrwalona praktyka postępowania w sytuacjach, gdy wymagana jest reakcja na zaistniałe zakłócenie[32].

Należy zaznaczyć, że reagowanie na zakłócenia, jako zapewnianie ciągłości działania, trzeba rozumieć nie tylko jako bezpośrednie postępowanie wobec występujących zakłóceń, lecz także jako aktywność o charakterze prewencyjnym, związaną z analizą ryzyka, zagrożeń i podatności oraz z poszukiwaniem

30 J. Zawiła-Niedźwiecki, op. cit., s. 166.
31 Ibidem, s. 92.
32 J.L. Lambin, op. cit., s. 32.

metod i rozwiązań zapobiegania powstaniu zakłóceń. W tym znaczeniu starania o ciągłość działania i bezpieczeństwo się splatają[33].

Z punktu widzenia ciągłości działania rozwiązania bezpieczeństwa zapewniają prewencję wobec zagrożeń, natomiast z punktu widzenia bezpieczeństwa rozwiązania ciągłości działania stanowią dodatkowe zabezpieczenie wówczas, gdy zawodzą nominalne rozwiązania bezpieczeństwa[34] (schemat 5).



Źródło: J. Zawiła-Niedźwiecki, op. cit., s. 121.

Schemat 5. Mechanizm logiczny naruszania poprawne działania organizacji

33 Ibidem, s. 97.
34 J. Zawiła-Niedźwiecki, op. cit., s. 96–97.

W związku z tym, jeżeli mowa o ciągłości działania, to mamy na myśli stan odporności organizacji na zakłócenie, jeżeli mowa o zapewnieniu ciągłości działania, to chodzi o ciąg planowanych działań, które zmierzają do usuwania zakłóceń, a gdy mowa o zarządzaniu zapewnianiem ciągłości działania, wówczas jest to proces polegający na określaniu zadań, przygotowaniu planu i monitorowaniu rozwiązań mających na celu zapewnienie ciągłości.

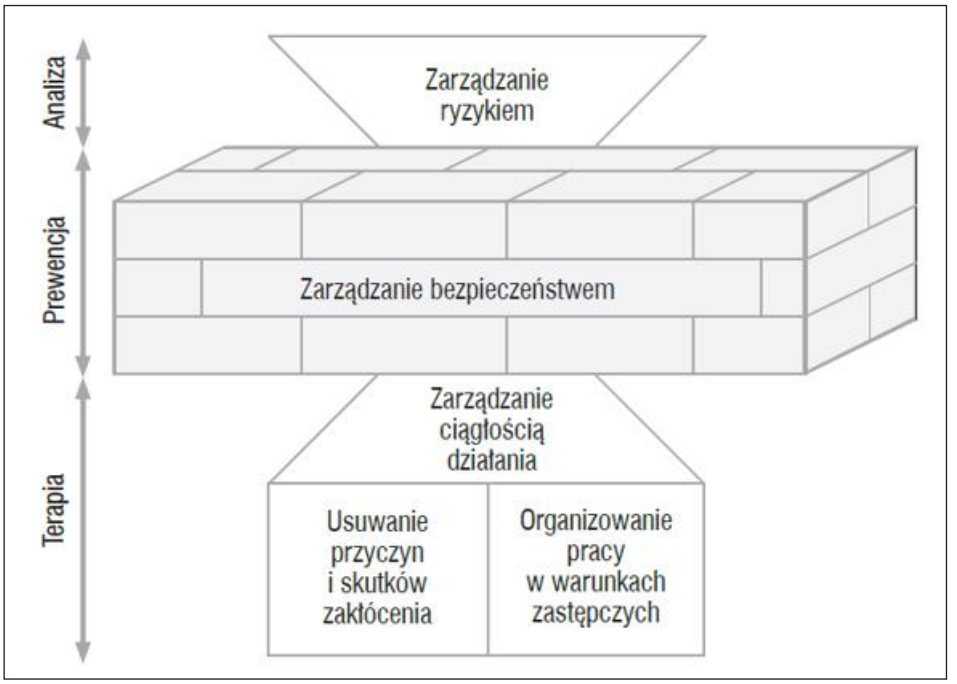
Kiedy mowa o ciągłości działania jako narzędziu biorącym udział w zabezpieczaniu przedsiębiorstwa, nie można pominąć również kwestii ryzyka. W zależności od przedziału czasowego możemy wyróżnić różne dyscypliny zajmujące się naturą ryzyka, bezpieczeństwem i ciągłością działania.

Kiedy mówimy o czasie odległym, wtedy będzie to kwestia z dziedziny ekonomii, ponieważ mamy na myśli odległe skutki i przyczyny (wzrost i rozwój). Gdy przyjmiemy perspektywę bliską czasowo, wówczas jest to kwestia z zakresu nauk o zarządzaniu, ponieważ ryzyko operacyjne jest traktowane jako ryzyko niewystarczającej skuteczności działania z punktu widzenia celu bieżącego tego działania. Tym samym w tym ujęciu ryzyko polega na możliwości niespełnienia wymogów czy oczekiwań[35].

Konsekwencją tego jest zabezpieczenie się i przygotowanie odpowiednich rozwiązań, dlatego pojawia się synergiczny związek ciągłości działań i bezpieczeństwa. Wszelkie działania na rzecz bezpieczeństwa mają charakter prewencyjny. Kiedy ochrona okazuje się nieskuteczna, wtedy rozwiązania ciągłości działania będą reakcją naprawczą (schemat 6)[36].

Triada: ryzyko – bezpieczeństwo – ciągłość oznacza zatem panowanie nad ryzykiem polegające na racjonalnym rozłożeniu akcentów między prewencję wobec zagrożeń dla działania organizacji a zaprojektowane reagowanie na występowanie zakłóceń.

35 J. Zawiła-Niedźwiecki, op. cit., s. 55.
36 Ibidem, s. 56.



Źródło: J. Zawiła-Niedźwiecki, op. cit., s. 121.

Schemat 6. Relacje zadań zapewniania bezpieczeństwa i ciągłości działania

Analiza ryzyka w przedsiębiorstwie

Analiza ryzyka ma na celu rozpoznać procesy i działy w firmie, które są najbardziej narażone na nieprzewidziane negatywne sytuacje. Pokazuje stopień odporności przedsiębiorstwa na sytuacje trudne do przewidzenia i groźne dla firmy[37]. Istnieje wiele rodzajów analiz, które mogę pomóc osobom zarządzającym w firmie dobrze przygotować odpowiednie procesy i zapobiec przerwaniu funkcjonowania firmy[38].

Jedną z najbardziej popularnych analiz jest Business Impact Analysis (BIA), która pozwala zdefiniować oraz sklasyfikować wszystkie nieprawidłowości. Dzięki tej analizie można określić działania o charakterze operacyjnym i strategicznym. Ważnym atutem BIA jest możliwość określenia czasu

37 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 58.

38 S. Zapłata, M. Kaźmierczak, *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Warszawa 2011, s. 153.

wystąpienia zagrożenia, a także zakresu jego oddziaływania na poszczególne podsystemy w firmie[39]. Dzięki niej można pozyskać informacje dotyczące procesów, zasobów i ludzi[40].

Pierwszym krokiem BIA jest poznanie rzeczywistej sytuacji firmy, gdy analiza dostarczy już wystarczającą ilość szczegółowych danych. Na ich podstawie zostaje wdrożona odpowiednia strategia i zostają podjęte odpowiednie działania. Dzięki tej analizie możemy także oszacować czas występowania sytuacji niepożądanej i zakres jej oddziaływania na poszczególne działy organizacji[41]. Celem ostatecznym BIA jest wskazanie krytycznych z punktu widzenia prowadzonego biznesu i niekrytycznych zdarzeń i sytuacji, z którymi spotyka się firma[42]. W zdarzeniach zaliczanych jako krytyczne możemy wyróżnić dwie zmienne:

– RPO (Recovery Point Objective) – określa minimalną ilość zasobów, które przedsiębiorstwo musi odzyskać w danym przedziale czasowym,

– RTO (Recovery Time Objective) – określa maksymalny czas przeznaczony na odbudowę najważniejszych procesów czy też na odzyskanie zasobów w firmie.

Taką analizę należy przeprowadzić nie tylko w przypadku zdarzeń nieprzewidzianych, np. klęska żywiołową, ale warto ją wdrożyć również przed podjęciem codziennych działań biznesowych takich, jak np.:

– wprowadzanie nowego produktu,
– zmiana strategii bądź struktury organizacyjnej,
– zmiana głównego dostawcy lub firm podwykonawczych,
– wdrożenie nowej technologii.

Wyniki z analizy BIA pomagają ocenić ewentualne straty finansowe spowodowane kryzysowym zdarzeniem i odnaleźć słabe elementy w organizacji (Single Point of Failure – SPOF).

Analiza istniejącej sytuacji (analiza luki – Gap Analysis) pomaga organizacjom określić jak najlepiej osiągać swoje cele biznesowe. W tej analizie należy zacząć od stanu faktycznego, zazwyczaj sytuacji wyjściowej znacznie

39 https://www-arch.polsl.pl/wydzialy/ROZ/ZN/Documents/z97/38_po_rec_056_Starosta.pdf [dostęp: 9.06.2024].
40 J.L. Lambin, op. cit., s. 45.
41 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 57.
42 Ibidem, s. 56.

odbiegającej od docelowej[43]. Kolejnym etapem będzie szukanie obszarów niespełniających wymagań, w których zauważymy luki. Następnie, po zaangażowaniu jak największej liczby osób, wspólnie jest opracowywany plan, który trzeba wdrożyć, żeby zapełnić dotychczasowe luki.

Uzyskane informacje będą bardzo potrzebne do kolejnej analizy, tj. analizy SWOT[44]. To analiza popularna i często używana w organizacjach. Polega ona na określeniu mocnych i słabych stron oraz możliwości i zagrożeń. Podczas opracowywania strategii należy również uwzględnić czynniki zewnętrzne. Po przeprocesowaniu analizy możemy znaleźć w wynikach słabe punkty i zagrożenia, które mogą mieć wpływ na ciągłość zarządzania. Analizę warto przeprowadzać zawsze po pojawieniu się zmian w firmie[45].

Do kompletu analiz, które mają za zadanie wspierać organizację i zapobiec ewentualnemu przerwaniu funkcjonowania organizacji, zaliczymy również analizę oceny ryzyka. Można wykonać ją w pięciu następujących krokach:

- zebranie potrzebnych informacji,
- identyfikacja zagrożeń,
- oszacowanie ryzyka,
- określenie działań eliminujących lub ograniczających ryzyko,
- dokumentowanie wyników[46].

Wynikiem tej analizy jest macierz, która w stopniach pokazuje poziom ryzyka.

Analiza systemowa, która jest oficjalnym, a także jawnym badaniem mającym wspomóc działanie osób odpowiedzialnych za decyzje w danej sytuacji, charakteryzuje się niepewnością. Polega na określeniu pożądanego działania poprzez rozważenie wielu wariantów oraz porównanie ich scenariuszy w celu przewidzenia skutków[47].

Aby utrzymać prawidłowo funkcjonujące procesy, musimy znać powiązania i zależności między nimi; tutaj przyda się analiza powiązań i zależności.

43 Ibidem, s. 125.

44 SWOT – akronimem od angielskich wyrazów określających cztery elementy analizy: S – Strengths (mocne strony), W – Weaknesses (słabe strony), O – Opportunities (możliwości), T – Threats (zagrożenia).

45 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 126.

46 *Ocena ryzyka zawodowego*, https://www.pip.gov.pl/dla-pracodawcow/niezbednik-pracodawcy/ocena-ryzyka-zawodowego [dostęp: 20.05.2025].

47 W. Findeisen, *Analiza systemowa. Podstawy i metodologia*, Warszawa 1985, s. 13.

W sytuacjach kryzysowych, gdy ciągłość może zostać zachwiana, należy dążyć do przywrócenia łańcucha procesów, które funkcjonowały w przedsiębiorstwie przed wystąpieniem kryzysu.

Wszystkie wymienione analizy mają za zadanie przygotować organizację na ewentualne sytuacje kryzysowe, które mogą pojawić się na ich biznesowej drodze. Żeby odpowiednio to zrozumieć, warto przyjrzeć się procesowi zarządzania ryzykiem[48].

Przede wszystkim organizacja musi zidentyfikować, przeanalizować i ocenić kategorie ryzyka, na które może być narażone. Kolejnym krokiem jest wypracowanie odpowiednich działań, a także metod, które pozwolą zminimalizować ryzyko i jednocześnie maksymalizować zyski. Zaproponowane rozwiązania muszą zgadzać się ze specyfiką firmy[49].

Celem analizy ryzyka jest zmniejszenie potencjalnego zagrożenia i jego konsekwencji na funkcjonowanie przedsiębiorstwa. Poprawnie przeprowadzona analiza ryzyka bazuje na najlepszych dostępnych źródłach informacji takich, jak: doświadczenia, dane z poprzednich lat, prognozy i opinie ekspertów, informacje zwrotne od wszystkich interesariuszy czy obserwacje[50].

Analiza ryzyka obejmuje m.in. czynniki ludzkie i kulturowe[51]. W założeniu powinna być:

– przejrzysta i kompleksowa,
– dynamiczna i powtarzalna,
– elastyczna, łatwo dostosowująca się do zmian oraz dopasowana do wewnętrznych i zewnętrzach uwarunkowań organizacji,
– bazująca na najlepszych z dostępnych źródłach informacji[52].

48 J.L. Lambin, op. cit., s. 46.

49 https://uhy-pl.com/blog-posts/4-metody-na-zidentyfikowanie-ryzyka-w-przedsiebiorstwie/ [dostęp: 10.06.2021].

50 B. Szlachcic, *Analiza ryzyka w zarządzaniu kryzysowym*, [w:] *Analiza informacji w zarządzaniu bezpieczeństwem*, red. nauk. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2013, s. 92–114.

51 B. Szlachcic, *Analiza ryzyka i zarządzania ryzykiem jako element systemu zarządzania kryzysowego w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie" 2014, nr 103, s. 233.

52 J.L. Lambin, op. cit., s. 51.

Zarówno analiza ryzyka, jak i wszystkie wspomniane jej cechy prowadzone w sposób systematyczny mogą przyczynić się do poprawy efektywności, a także uzyskania jednolitych i wiarygodnych rezultatów[53].

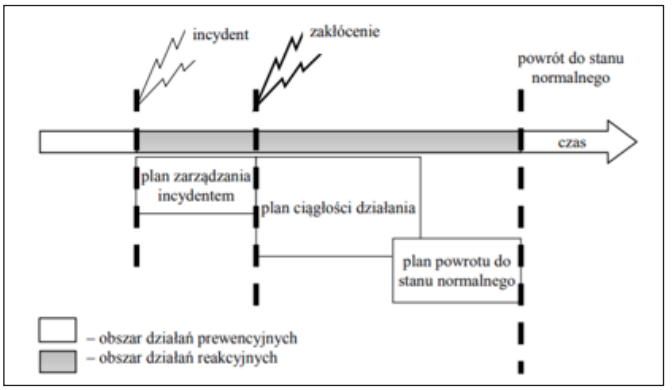
Analiza ryzyka pomaga przygotować się do kryzysu, w którym jeżeli nadejdzie, to będzie można szybko uruchomić procedury naprawcze i wdrożyć plany kryzysowe, a następnie plany naprawcze[54].

Procedury i plany awaryjne w procesie zarządzania bezpieczeństwem przedsiębiorstwa

Jeżeli dojdzie do sytuacji kryzysowej bądź przed taką sytuacją w celach prewencyjnych, to należy mieć przygotowany udokumentowany plan naprawczy, który jest w stanie złagodzić lub naprawić skutki powstałego zdarzenia. Każda firma dostosowuje plany i procedury na podstawie dogłębnych analiz w zależności od swoich potrzeb oraz rodzaju przewidywanego zagrożenia. W celu efektywnego zarządzania ciągłością działania konieczne jest stworzenie takich planów[55].

Zgodnie z wymaganiami ISO 22301 jednym z niezbędnych dokumentów jest posiadanie planu ciągłości biznesowej zawierającego procedury i informacji, które zostaną wykorzystane w razie wystąpienia zagrożenia. Drugim jest plan zarządzania zdarzeniem/incydentem, czyli udokumentowany plan działania obejmujący personel i zasoby organizacji, stosowany w przypadku wystąpienia incydentu. Plan zarządzania incydentem jest uruchamiany każdorazowo po jego wystąpieniu. Pomiędzy obydwoma planami występują zależności (schemat 7). Jeżeli incydent przeradza się w kryzys, to podejmuje się działania określone w planie ciągłości działania[56]. Nowy standard do tej normy zwany ISO 22301 kładzie również nacisk na elementy dotyczące komunikacji oraz zwiększenie odpowiedzialności. Dodatkowo stawia na bardzie aktywne przywództwo kierowników wyższego szczebla.

53 Ibidem, s. 233.
54 Ibidem, s. 238.
55 K. Białecki, *Instrumenty marketingu*, Bydgoszcz–Warszawa 2006, s. 18.
56 S. Zapłata, *Systemowe zarządzanie ciągłością działania BS 25999 w działalności usługowej*, Poznań 2012, s. 250.



Źródło: S. Zapłata, M. Kaźmierczak, *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Warszawa 2011, s. 152.

Schemat 7. Plany w systemie zarządzania ciągłością działania

Ponieważ plany awaryjne służą możliwości odtworzenia działalności organizacji na nowo, dlatego tak ważne jest określenie rodzajów incydentów, które mogą tę ciągłość zakłócić. Oprócz procedur mających minimalizować straty plany te obejmują dokładne instrukcje jak odtworzyć dany proces[57].

Podczas tworzeniu procedur w planach dotyczących ciągłości działania musimy pamiętać, że w sytuacji kryzysowej nie wszystkie zasoby mogę być dostępne. Warto również zwrócić uwagę na dwa zagadnienia, tj. zarządzanie organizacją w sytuacji kryzysowej wymagające szybkich działań, stąd pojawia się konieczność uproszczenia schematu decyzyjnego, oraz komunikację w sytuacji kryzysowej obejmująca wymianę z klientami zewnętrznymi dostawcami, administracją czy mediami, a także komunikację wewnętrzną w firmie[58].

Zgodnie z *good practice guide*[59] wszystkie plany i koncepcje utrzymania ciągłości działania powinny opierać się na krytycznej ocenie głównych obszarów aktywności przedsiębiorstwa (Mission Critical Activities – MCA), a także na ocenie skutków zaistniałych i możliwych strat (Business Impact Analysis – BIA). Ponieważ środowisko i rynek się zmieniają, zatem odpowiednie części planu powinny być na bieżąco aktualizowane. Wszystkie te czynności tworzą

57 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 21.
58 Ibidem, s. 21.
59 Kodeks dobrych praktyk tu odnosi się do konkretnych opracowań dotyczących zarządzania ciągłością działania.

jeden proces, o którym mowa również w normie ISO 22301. Obejmuje on następujące fazy:

– zrozumienie założeń prowadzonego biznesu,
– zdefiniowanie strategii utrzymania ciągłości działania,
– przygotowanie planu oraz jego wdrożenie,
– stworzenie kultury utrzymania ciągłości działania,
– wprowadzenie planu w życie, dodatkowo testy i audyty[60].

Ważna kwestią w wymienionych fazach jest istota testów i audytów. Wszystkie przygotowane plany powinny być dobrze znane, a ludzie pracujący w organizacji powinni być z nich przeszkoleni. Praktyka będzie tutaj najlepszym nauczycielem. W wielu firmach organizuje się szkolenia na ten temat. Podstawowym celem testów i ćwiczeń jest stwierdzenie, czy sprawne są programy UCD, plany kontynuacji, zarządzania ryzykiem i zarządzania kryzysowego czy w dostatecznym stopniu jest zabezpieczone całe przedsiębiorstwo przed negatywnymi skutkami nieprzewidzianych zdarzeń losowych[61].

Wszystkie te fazy są modyfikowane zgodnie z potrzebami do czasu aż cała organizacja osiągnie akceptowalny poziom utrzymania ciągłości działania. Przyczynami zmian są różne zdarzenia i okoliczności zarówno te pozytywne, jak i negatywne[62]. Jeżeli plan skutecznie nie zadziała, to firmie grożą poważne konsekwencje, a nawet zakończenie działalności, dlatego omawiane fazy powinny być tak sformułowane, żeby wyraźnie wynikała z nich ochrona głównego interesu przedsiębiorstwa[63]. Ważne jest utworzenie zespołu, który będzie koordynował i opracowywał szczegółowe procedury w sytuacjach awaryjnych[64]. Według koncepcji BCP (Business Continuity Planning) przedsiębiorstwo ma możliwość rozstrzygnięcia wielu pytań odnoszących się do przyszłości w oparciu o poniższe pojęcia:

– Business Continuity Planning (BCP) – planowanie kontynuacji działania (pol. UCD),

– Disaster Recovery Planning (DRP) – planowanie odzyskania podstawowych zasobów po incydencie,

60 T.T. Kaczmarek, G. Ćwiek, op. cit. s. 46.
61 Ibidem, s. 45.
62 Ibidem, s. 48.
63 Ibidem, s. 55.
64 J. Zawiła-Niedźwiecki, op. cit., s. 156.

– Contingency Planning (CP) – planowanie działań na wypadek nieprzewidzianych zdarzeń[65].

Opracowanie planu UCD jest procesem wieloaspektowym, który obejmuje następujące najważniejsze fazy:

– założenia do przyszłych analiz (Business Impact Analysis – BIA),
– plan odtworzenia zniszczonego majątku (Disaster Recovery Plan – DRP),
– zespół ds. Disaster Recovery – testowanie sytuacji awaryjnych;
– utrzymanie planu UCD w stałej gotowość do stosowania[66].

Posiadanie planów UCD adekwatnych do wielkości firmy i skali ma większe znaczenie w mniejszych firmach niż w przypadku korporacji, dlatego że są one bardziej narażone i zazwyczaj w mniejszym stopniu przygotowane na kryzysy, które mogą je spotkać. Ponadto jest istotna kwestia możliwości finansowania, czyli pobierania funduszy w celu dokonania przedsięwzięć w przedsiębiorstwie[67] Dla kadry zarządzającej jest ważne jak w razie kryzysu bądź zagrożenia firma zostanie odebrana przez środowisko, jak sobie poradzi i jakie opinie negatywne może spowodować wydarzenie? W tym punkcie warto przyjrzeć się marketingowi jako procesowi ważnemu w naprawie skutków kryzysu. Dział ten często bywa angażowany w plany naprawcze, ponieważ każda negatywna sytuacja może wpłynąć na markę, a zadaniem marketingu jest budować dobry wizerunek.

Zakończenie

Każde przedsiębiorstwo posiada założone cele, mimo to jednym z głównych jest osiąganie konkretnego zysku finansowego. Żeby organizacja mogła działać i osiągać zysk, jest konieczne prowadzenie właściwie zaplanowanych działań marketingowych.

Równie ważne jest to, żeby organizacja mogła działać w sposób bezpieczny i przewidywalny, zwłaszcza wtedy, kiedy bierze się pod uwagę to, że funkcjonując w turbulentnym otoczeniu, jest narażona na występowanie licznych sytuacji kryzysowych.

65 Ibidem, s. 66.
66 Ibidem, s. 72–74.
67 Ibidem, s. 71.

Dzięki zastosowaniu odpowiednich narzędzi marketingowych przedsiębiorstwo może uzyskać stałą przewagę konkurencyjną. Tworzenie pozycji konkurencyjnej i działanie w niestabilnym otoczeniu powoduje, że każde przedsiębiorstwo musi dbać o sprawy związane z zarządzaniem ciągłością działania. Jednakże, chcąc sprostać konkurencji, a tym samym dbać o bezpieczeństwo, należy przedsiębiorstwo zabezpieczać wieloaspektowo. Z jednej strony jego działania muszą się koncentrować na pogłębianiu zaufania klientów, żeby nie stracić przychodów, z drugiej, zapobiegać ewentualnym przyszłym sytuacjom kryzysowym.

Żeby zapobiec niekorzystnym sytuacjom, firmy tworzą analizy ryzyka, w których określają ewentualne problemy lub zagrożenia w bieżącej działalności firmy. Identyfikacja ryzyk pozwala na opracowanie procedur i planów zarządzania ciągłością działania, co ma uchronić przedsiębiorstwo na wypadek incydentów i sytuacji kryzysowych mogących wystąpić w funkcjonowaniu organizacji.

Wobec tego można się zastanowić, czy w planach zarządzania ciągłością działania jest miejsce na marketing? Wydaje się, że na tak postawione pytanie należy odpowiedzieć pozytywnie, dzięki bowiem działaniom marketingowym można stosować plan naprawczy, który pomoże organizacji przetrwać i budować nową pozycję na rynku. Każda organizacja musi być zabezpieczona na różne okoliczności, w tym jak skutecznie sobie radzić z sytuacjami kryzysowymi, w jaki sposób kształtować komunikację kryzysową, w którym kierunku prowadzić działania rozwojowe.

Celem niniejszego artykułu było pokazanie roli marketingu w procesie zarządzania ciągłością działania. Autor przeanalizował dziesięć spółek kapitałowych pod kątem sposobu podchodzenia do tego zagadnienia ze szczególnym uwzględnieniem roli i znaczenia działań marketingowych. Żeby realizować proces zarządzania ciągłością działań, należy stale doskonalić przedsiębiorstwo. Pomaga w tym skuteczny i efektywny marketing, który może być wdrażany w organizacji na różne sposoby. Ta doskonałość co prawda pozostaje w strefie niedoścignionego ideału, ale dążą do niego firmy, które samodzielnie decydują o sposobie doskonalenia swojej działalności.

Ważne jest pozyskanie w miarę pełnej wiedzy o wszystkich zjawiskach. Oczywiście, pełne przewidywanie takich zjawisk jest niemożliwe, dlatego że ich różnorodność zagraża osiągnięciu zamierzonych celów przez przedsiębiorstwo.

Niebezpieczeństwa te rodzą się w różnych uwarunkowaniach organizacyjno-prawnych, ekonomiczno-finansowych, techniczno-technologicznych i innych. Oznacza to powstawanie nowych rodzajów ryzyka i przeobrażenie już istniejących. W tym kontekście przedsiębiorstwa podejmują określone wzorce, z których najbardziej powszechna jest metoda BCMM, dzięki której można wprowadzić model oceny dojrzałości zarządzania ryzykiem. We wdrażaniu tych narzędzi może pomóc skuteczny i nowoczesny marketing. Oczywiście, nie istnieje złota metoda na implementację takiego samego rozwiązania w każdej firmie, mimo to efektywnie prowadzony marketing ma wpływ na sprawność realizacji procesu ciągłości działania.

Bibliografia

Białecki K., *Instrumenty marketingu*, Bydgoszcz–Warszawa 2006.

Bieniok H. i in., *Metody sprawnego zarządzania*, Warszawa 2004.

Blim M., Byczkowski M., Zawiła-Niedźwiecki J., *Zintegrowane zarządzanie bezpieczeństwem organizacji*, [w:] *Systemy informatyczne. Bankowość i finanse*, red. F. Marecki, J.K. Grabara, J. Nowak, Warszawa 2005.

Findeisen W., *Analiza systemowa. Podstawy i metodologia*, Warszawa 1985.

https://uhy-pl.com/blog-posts/4-metody-na-zidentyfikowanie-ryzyka-w-przedsiebiorstwie/ [dostęp: 10.06.2021].

Kaczmarek T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania*, Warszawa 2015.

Kotler Ph., Armstrong G., Saunders J., Wong V., *Marketing. Podręcznik europejski*, Warszawa 2002.

Lambin J.L., *Strategiczne zarządzanie marketingowe*, Warszawa 2001.

Lidermann K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017.

Marketing przedsiębiorstw przemysłowych, red. W. Mantura, Poznań 2000.

Michalski E., *Marketing*, Warszawa 2004.

Ocena ryzyka zawodowego, https://www.pip.gov.pl/dla-pracodawcow/niezbednik-pracodawcy/ocena-ryzyka-zawodowego [dostęp: 20.05.2025].

Rydel M., *Komunikacja jako element marketingu*, [w:] *Komunikacja marketingowa*, red. M. Rydel, Gdańsk 2001.

Ryzyko operacyjne w naukach o zarządzaniu, red. nauk. I. Staniec, J. Zawiła-Niedźwiecki, Warszawa 2015.

Szlachcic B., *Analiza ryzyka i zarządzania ryzykiem jako element systemu zarządzania kryzysowego w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie" 2014, nr 103.

Sznajder A., *Marketing. Encyklopedia biznesu*, t. 1, Warszawa 1995.

Waniowski P., Sobotkiewicz D., Daszkiewicz M., *Marketing – teoria i przykłady*, Wydawnictwo Placet, Warszawa 2010.

Zapłata S., *Systemowe zarządzanie ciągłością działania BS 25999 w działalności usługowej,* Poznań 2012.
Zapłata S., Kaźmierczak M., *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Warszawa 2011.
Zaskórski P. *Informacyjno-biznesowa ciągłość działania firmy*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2011, nr 5.
Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*, Kraków 2013.

Business Continuity in the Enterprise from a Security Perspective

Abstract

Due to the rapidly changing environment, enterprises are paying more and more attention to the issue of business continuity management. Much is said about the threat of the modern world, which is the dependence on technology, which causes business continuity to become a fundamental factor of success for many organisations. Conscious enterprises protect themselves in many layers so as not to lose trust among customers, not to lose revenue, and also to prevent the loss of potential benefits.

The article addresses the issue of proper operation of the enterprise from a security perspective. Therefore, managing your business continuity becomes important, which directly translates into the security of the enterprise.

Keywords: enterprise, security, management