BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718 2024
ISSN 1899-6264 Nr 1 (LIV)

DOI: 10.48269/2451-0718-btip-2024-1-004
Data wpłynięcia: 31.05.2023
Data akceptacji: 10.09.2023

Andrzej Chodyński

prof. dr hab., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-4962-5143

Wpływ koncepcji zarządzania na architekturę bezpieczeństwa biznesu – programy zapobiegania awariom przemysłowym

Wprowadzenie

Koncepcje zarządzania znajdują swoje odbicie w zarządzaniu bezpieczeństwem. Ryszard Wróblewski rozpatruje je na poziomie bezpieczeństwa narodowego, przywołując koncepcje: systemową, organizacji działającej w środowisku chaotycznym, organizacji sieciowej, organizacji opartej na wiedzy oraz zarządzania strategicznego[1]. Koncepcje zarządzania są rozpatrywane jako pomysły (recepty, sposoby) na zarządzanie, które na niższych poziomach realizowane są poprzez metody i techniki zarządzania[2]. Prezentowany jest pogląd włączający do koncepcji zarządzania idee, pomysły na zarządzanie, modele, metody, a także techniki[3]. Nauki o zarządzaniu odnoszą pojęcie koncepcji m.in. do jakości, nastawienia na klienta, są ukierunkowane na współdziałanie (w tym sieciowość), na wyszczuplanie organizacji (*lean management*), na wiedzę (wykorzystanie uczenia się i zarządzania innowacjami). Uwzględnia się także podejście procesowe[4]. Na procesowe i systemowe podejście

1 R. Wróblewski, *Elementy koncepcji zarządzania bezpieczeństwem narodowym*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2021, t. 7, nr 1, s. 7–26.

2 J. Lichtarski, *Koncepcje zarządzania czy funkcje przedsiębiorstwa*, „Przegląd Organizacji" 2001, nr 9, s. 27–28.

3 K. Łobos, *Koncepcje zarzadzania*, Wydawnictwo Wyższej Szkoły Bankowej w Poznaniu, Poznań 2021, s. 7.

4 A. Chodyński, *Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja smart*, „Bezpieczeństwo. Teoria i Praktyka" 2019, nr 4 , s. 39–62.

do zarządzania bezpieczeństwem zwraca uwagę Mirosław Kwieciński[5]. Aktualnie orientacja na klienta przyjmuje formę nastawienia na wszystkich interesariuszy w postaci koncepcji społecznej odpowiedzialności organizacji (CSR). Coraz częściej, w związku z nastawieniem proekologicznym, przyjmuje ona postać ECSR (Environmental Corporate Social Responsibility). Koncepcja ta jest rozpatrywana w biznesie korporacyjnym w kontekście *sustainability*[6]. Zwraca się uwagę, że realizacja poszczególnych koncepcji zarządzania jest możliwa dzięki posiadanemu kapitałowi intelektualnemu opartemu na wiedzy[7]. Agnieszka Giszterowicz wskazuje na kulturę bezpieczeństwa jako jeden z elementów kapitału intelektualnego przedsiębiorstwa[8].

Podkreśla się fakt, że w ramach zarządzania bezpieczeństwem ekonomicznym informacje, wiedza oraz kompetencje, a także kapitał intelektualny służą budowie przewagi konkurencyjnej przedsiębiorstwa[9].

Działania na rzecz zapewnienia bezpieczeństwa są oparte na istniejącym modelu architektury biznesu. Wskazywane są związki architektury biznesu z działaniami na rzecz wykorzystania kapitału intelektualnego, uczenia się czy stosowania rutyn i praktyk organizacyjnych, budowy kompetencji oraz związki z rezyliencją organizacyjną. Analizy obejmują również zasoby i procesy. Architektura biznesu opiera się na strategicznych założeniach organizacji. Podkreśla się, że architektura powinna uwzględniać możliwość wystąpienia sytuacji kryzysowej[10]. Oznacza to, że na przyjętą architekturę biznesu wpływ mają wymienione powyżej koncepcje zarządzania. Wobec możliwości wystąpienia zagrożeń dla bezpieczeństwa organizacji analizie powinny być poddane poszczególne elementy architektury biznesu związane z konfiguracją techniczno-ekonomiczną dla utrzymania ciągłości działania w zakresie wytwarzania produktów, konfiguracją społeczną opartą na relacjach między pracownikami (i otoczeniem) oraz konfiguracją organizacyjną dotyczącą m.in.

---

5 M. Kwieciński, *Procesowe i systemowe ujęcie procesu zarządzania bezpieczeństwem*, „Bezpieczeństwo. Teoria i Praktyka" 2012, nr 2, s. 57–64.

6 I.Z. Rela *et al.*, *Effects of environmental corporate social responsibility on environmental well-being perception and the mediation role of community resilience*, „Corporate Social Responsibility and Environmental Management" 2020, vol. 27, nr 5, s. 2176–2187.

7 A. Chodyński, *Sieciowość w koncepcjach biznesu – aspekty społeczne i ekologiczne*, [w:] *Zarządzanie odpowiedzialnym rozwojem przedsiębiorstwa*, red. A. Chodyński, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2012, s. 83–110.

8 A. Giszterowicz, *Operationalising a safety culture in the management of a business entity (case study)*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 91–102.

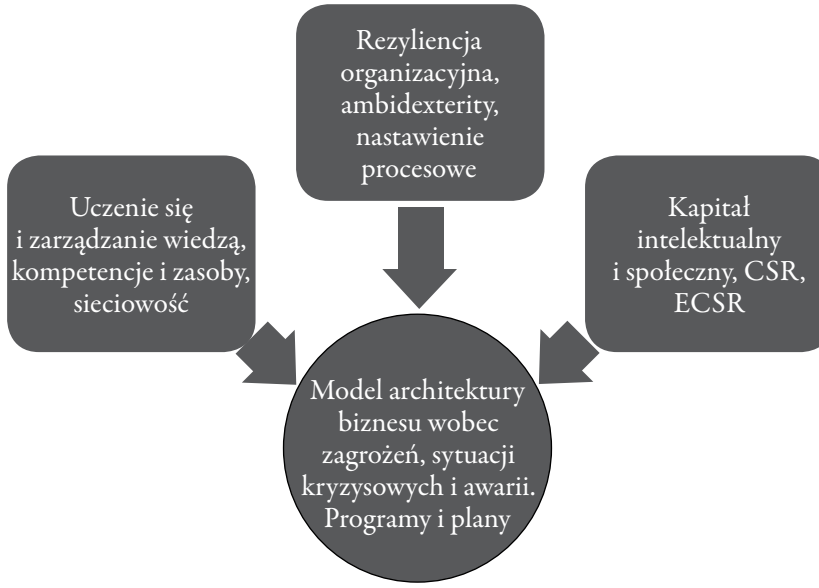
9 H. Wyrębek, *Narzędzia wspomagające proces zarządzania wiedzą i bezpieczeństwem ekonomicznym w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie" 2015, t. 32, nr 105, s. 227–240.

10 A. Chodyński, *Kreowanie odpowiedzialnego biznesu*, Oficyna Wydawnicza AFM, Kraków 2016, s. 93–109.

dostosowania struktur organizacyjnych do nowych sytuacji, w tym realizacji programów przeciwdziałania zagrożeniom, m.in. możliwości wystąpienia awarii.

Rozpatrzono wpływ współczesnych koncepcji zarządzania na budowę architektury bezpieczeństwa biznesu (rysunek 1).

Rysunek 1. Wpływ współczesnych koncepcji zarządzania na architekturę bezpieczeństwa biznesu



Źródło: opracowanie własne.

Utrzymanie ciągłości działania przedsiębiorstwa w sytuacji zagrożeń wymaga nastawienia o charakterze *ambidexterity*, umiejętnego łączenia zadań bieżących i przyszłościowych, także w odniesieniu do problematyki bezpieczeństwa. Podkreśla się znaczenie współpracy z partnerami (w tym w obszarze dostępności do zasobów) i działań innowacyjnych[11].

W sytuacji wystąpienia zagrożeń o charakterze niezwiązanym z czynnikami ekonomicznymi przedsiębiorstwo staje wobec groźby tzw. kryzysu pozaekonomicznego. Jego wystąpienie jest związane ze skrajną turbulencją otoczenia, w tym przejawiającą się różnego typu kataklizmami o charakterze naturalnym (np. silne wiatry czy powodzie) lub spowodowanych np. pandemią, sytuacją wojenną lub atakami terrorystycznymi. Kryzys pozaekonomiczny może być wywołany także katastrofami przemysłowym i wielkimi awariami. Podejmowane przez przedsiębiorstwa działania zarówno

[11] Idem, *Using ambidexterity in the ecological security management of organisations*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 49–59.

w fazie przed, jak i w trakcie takiego kryzysu przyjmują charakter rezylientny[12], w postaci zachowań odpornościowych (*resistance*, czasem określanych jako *robustness*), łączących opór z adaptacyjnością i elastycznością (*adaptability and flexibility*), lub sprężystych (stabilnych, *stability*). Z tym drugim przypadkiem mamy do czynienia np. dla organizacji wysoce niezawodnych (jak elektrownie jądrowe) czy innych podmiotów infrastruktury krytycznej, dla których brak jest możliwości odejścia od realizacji wykonywanych funkcji.

Zdaniem Jacka Milewskiego dla przedsiębiorstw infrastruktury krytycznej zagrożenia mogą mieć m.in. charakter: naturalny, techniczny (odnoszą się przede wszystkim do awarii różnego typu obiektów: przemysłowych, komunalnych, budowlanych, a także urządzeń związanych z transportem) oraz podłoże terrorystyczne[13].

Zwraca się uwagę na rolę nadmiarowości zasobów (*redundance*) i zapewnienia szybkiego dostępu do tych zasobów. Powinny być one ponadto silne (krzepkie, *robust*). Problemem jest fakt rozproszenia tych zasobów, co powoduje trudności w ich wykorzystaniu w sytuacji kryzysowej[14].

Tworzone są programy pozwalające realizować rezylientne zachowania przedsiębiorstw.

Hipoteza: programy na rzecz bezpieczeństwa mogą być realizowane w ramach tworzonej architektury biznesu z wykorzystaniem współczesnych koncepcji zarządzania, w szczególności w aspekcie zasobowym.

Celem pracy jest wskazanie możliwości wykorzystania modeli architektury biznesu opartych na tworzeniu nadmiarowych, niematerialnych zasobów organizacji dla realizacji programów na rzecz bezpieczeństwa.

Rola nadmiarowości zasobów w sytuacjach zagrożeń

W niniejszym opracowaniu zwrócono uwagę na rolę tworzenia nadmiarowych zasobów w przypadku działań praktycznych w ramach programów zapobiegania poważnym awariom przemysłowym. Mogą one mieć miejsce zarówno w przedsiębiorstwach zaliczanych, jak i niezaliczanych do infrastruktury krytycznej. W tym pierwszym przypadku mowa jest o szczególnym typie zagrożeń dla bezpieczeństwa i funkcjonowania państwa. Nadmiarowość zasobów powinna być uwzględniana w realizowanych modelach architektury biznesu. Nadmiarowe zasoby mogą mieć

---

[12] Idem, *Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezyliencji organizacyjnej*, [w:] *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw*, red. A. Chodyński, D. Fatuła, M.A. Leśniewski, Oficyna Wydawnicza AFM, Kraków 2022, s. 11–31.

[13] J. Milewski, *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe AON" 2016, nr 4 (105), s. 99–115.

[14] A. Chodyński, *Kryzys pozaekonomiczny przedsiębiorstwa...*, *op. cit*.

charakter materialny, ale także, co niezwykle istotne – niematerialny. W literaturze przedmiotu w rozważaniach o strategiach przedsiębiorstw przewiduje się możliwość mobilizowania zasobów niematerialnych, a więc wiedzy, zasobów relacyjnych, lojalności pracowniczej, a także kultury organizacyjnej[15]. Można w tym przypadku wykorzystać także poglądy Aleksandry Sus odnośnie do roli dynamicznych zdolności (*dynamics capabilities*) organizacji w kontekście konieczności utrzymywanie redundancji zasobów, aby móc szybko je wykorzystać w odpowiednim w momencie[16]. Ważną rolę będzie odgrywać kultura bezpieczeństwa organizacji[17]. Proponowane jest pojęcie rezylientnej kultury bezpieczeństwa, istotnej w przypadku możliwości wystąpienia wydarzeń nieoczekiwanych, w szczególności w przemysłach o wysokiej niezawodności funkcjonowania, w tym w przemyśle petrochemicznym[18]. W analizach przypadku huraganu Katrina (USA, 2005) i jego skutków dla przemysłu petrochemicznego w USA podkreśla się, że cechą charakterystyczną posiadania niezależnej kultury rezyliencji jest uwzględnienie konieczności szybkości działań, wraz z tworzeniem prostych reguł. Na znaczeniu, w ramach kultury rezyliencji, zyskują: integralność, praca zespołowa, wyniki, uczenie się i odwaga[19]. Rezyliencja wobec sytuacji kryzysowych jest rozpatrywana także jako element kompetencji menadżerskich[20]. Kompetencje te mogą być traktowane jako zasób organizacyjny.

Istotna rolę ogrywać będą powiązania sieciowe. Na ich funkcjonowanie może mieć wpływ architektura biznesu potencjalnych uczestników sieci. W sytuacjach kryzysowych ważny będzie dostęp do zasobów partnerów. Przykładowo dla organizacji hi-tech celowo tworzony nadmiar zasobów silnie wpływa na relacje koopetycyjne z partnerami, co pozwala na tworzenie nowych zasobów[21]. W tym przypadku przydatne może być wykonanie audytu zasobów niematerialnych (informacji, wiedzy

---

15 R. Krupski, *Okazje w zarządzaniu strategicznym przedsiębiorstwa*, „Organizacja i Kierowane" 2011, nr 4(147), s. 11–24.

16 A. Sus, *Dynamika modeli biznesu*, „Nauki o Zarządzaniu/ Management Sciences" 2014, nr 1(18), s. 90–99.

17 A. Chodyński, *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*, Oficyna Wydawnicza AFM, Kraków 2021, s. 133–148.

18 Gh. A Shirali, M. Shekari, K.A. Angali, *Quantitative assessment of resilience safety culture using principal components analysis and numerical taxonomy: A case study in a petrochemical plant*, „Journal of Loss Prevention in the Process Industries" 2016, vol. 40, s. 277–284.

19 H.P. Knapp, *Designing and implementing an interdependent resilience culture*, „Journal of Business Continuity & Emergency Planning" 2016, vol. 10, nr 1, s. 76–83.

20 J. Bugaj, A. Witek, *Rezyliencja jako element modelu kompetencji menedżera do zarządzania kryzysem*, „Studia i Prace Kolegium Zarządzania i Finansów SGH" 2022, nr 184, s. 9–19, https://econjournals.sgh.waw.pl/SiP/article/view/2939/2605 [dostęp: 17.07.2023]. W publikacji nie wskazano różnic w zarządzaniu kryzysem w ramach działalności publicznej i biznesowej.

21 A. Zakrzewska-Bielawska, *Zasobowe uwarunkowania koopetycji w przedsiębiorstwach high-tech*, „Przegląd Organizacji" 2013, nr 2, s. 3–8.

i kapitału intelektualnego), także w kontekście sieciowym, który proponuje Anna Ujwary-Gil[22].

Działalność organizacji uczącej wiąże się z zarządzaniem wiedzą. W szczególności zwraca się uwagę na tworzenie redundancji tego zasobu, podkreślając rolę organizacji uczącej się w tworzeniu zasobów rzadkich, oryginalnych i atrakcyjnych[23]. W sposób oczywisty tego typu zasoby mogą być wykorzystane w ramach zachowań rezylientnych w sytuacji kryzysu pozaekonomicznego, w tym przez przedsiębiorstwa infrastruktury krytycznej. Wykorzystać można także dorobek w zakresie planowania miejskiego i budowy miasta rezylientnego. Rozwój miast napotyka na przeszkody w postaci takich stresorów jak różnego typu zagrożenia, ryzyka i katastrofy. Współcześnie związane są one m.in. ze zmianami klimatycznymi, zagrożeniami terrorystycznymi czy pandemiami. Aby zaproponować strategie działania, konieczna jest identyfikacja stresorów, określenie wrażliwości systemu miasta na ich oddziaływanie, a także analiza skutków tego oddziaływania. Wskazuje się przy tym na znaczenie nadmiarowości zasobów w systemie miasta do wykorzystania w sytuacji kryzysowej[24]. Tworzenie zasobu niematerialnego w postaci wiedzy wynikającej z uczenia się opisano na przykładzie awarii oczyszczalni ścieków miejskich w Warszawie[25].

Nadmiarowość zasobów dotyczyć może kapitału intelektualnego i kapitału społecznego. Istnieje wiele definicji kapitału intelektualnego, przy czym najczęściej jako elementy składowe wymienia się kapitał ludzki, strukturalny (organizacyjny) i relacyjny. Występuje też podział kapitału intelektualnego na kapitał ludzki, kapitał organizacyjny (strukturalny) i kapitał społeczny. Kapitał społeczny dotyczy powiązań zarówno wewnątrz, jak i na zewnątrz organizacji[26]. Kapitał społeczny oparty jest na współpracy między ludźmi, bazuje na zaufaniu, normach społecznych i zaangażowaniu we wspólne przedsięwzięcia[27].

Na rolę kapitału relacyjnego w sytuacjach kryzysowych przedsiębiorstwa oraz wpływu różnych rodzajów kapitału społecznego na rezyliencję biznesu w przypadku

---

22 A. Ujwary-Gil, *Audyt zasobów niematerialnych z wykorzystaniem analizy sieci organizacyjnej*, Wydawnictwo Naukowe PWN, Warszawa 2017, s. 74–142.

23 K. Olejczyk-Kita, *Uczenie się organizacji – aspekt zasobowy*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2013, nr 310, s. 83–90.

24 L. Mierzejewska *et al.*, *City resilience – aspekty planistyczne*, „Rozwój Regionalny i Polityka Regionalna" 2020, nr 50, s. 83–99.

25 A. Chodyński, *Uczenie się i wpływ społeczny a bezpieczeństwo na poziomie lokalnym – zarządzanie w sytuacji awarii zagrażającej środowisku naturalnemu*, „Bezpieczeństwo. Teoria i Praktyka" 2021, nr 4, s. 61–80.

26 A.M. Libertowska, *Wpływ kapitału społecznego na zarządzanie wartością przedsiębiorstw z branż zaawansowanych technologii w Wielkopolsce*, rozprawa doktorska, Politechnika Poznańska, 2019, s. 30–34, 54, https://sin.put.poznan.pl/dissertations/details/d171 [dostęp: 14.08.2023].

27 A. Chodyński, *Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym*, „Bezpieczeństwo. Teoria i Praktyka" 2014, nr 1, s. 13–27.

zagrożenia (huragan Katrina) zwrócono uwagę w publikacji Andrzeja Chodyńskiego[28]. Znaczenie kapitału intelektualnego dla bezpieczeństwa ekonomicznego podmiotu gospodarczego podkreśla Jacek Woźniak[29]. Kapitał intelektualny i kapitał społeczny są wykorzystywane w trakcie bieżącej działalności podmiotów gospodarczych. Ich nadmiarowość może być wykorzystywana w ramach architektury biznesu w sytuacji trudno przewidywalnych zagrożeń. Kapitał intelektualny pomiotu gospodarczego wymaga ochrony w cyberprzestrzeni[30]. Rozpatrywane jest znaczenie kapitału intelektualnego w aspekcie bezpieczeństwa na poziomie państwowym[31]. Zwraca się uwagę na rolę kapitału społecznego w działaniach na rzecz bezpieczeństwa państwa wykorzystujących współpracę i tworzenie sieci formalnych i pozaformalnych organizacji społecznych[32].

Programy dla sytuacji awaryjnych

Pojęcie programu w aspekcie ekonomicznym, technicznym lub prawnym często kojarzone jest z projektem, choć program jest pojęciem szerszym. Może on stanowić odpowiednie zestawienie (konsolidację) powiązanych projektów. Zarządzanie programem dotyczy w tym przypadku zarządzania grupą projektów[33]. Tomasz Jabłoński wskazuje, że program stanowi ramę do działania, wskazywane w nim cele mają charakter ogólny, kierunkowy, a ich konkretyzacja następuje poprzez realizację planów[34]. Program może być rozumiany jako plan zamierzonych czynności lub przedsięwzięć[35].

Programy zapobiegania awariom przemysłowym są tworzone przez zakłady o zwiększonym lub dużym ryzyku wystąpienia tych awarii i wdrażane w oparciu o systemy zarządzania bezpieczeństwem jako elementy ogólnego systemu zarządzania zakładem. Program obejmuje m.in. ogólne cele i zasady działania odnoszone do

---

[28] Idem, *Kryzys pozaekonomiczny przedsiębiorstwa...*, *op. cit.*

[29] J. Woźniak, *Bezpieczeństwo ekonomiczne organizacji gospodarczych a koncepcje przedsiębiorczości*, „Nowoczesne Systemy Zarządzania" 2013, t. 8, nr 1, s. 49–63.

[30] K. Renaud, B. von Solms, R. von Solms, *How does intellectual capital align with cyber security?*, „Journal of Intellectual Capital" 2019, vol. 20, nr 5, s. 621–641.

[31] W.K. Jaruszewski, *Rola kapitału intelektualnego i kultury w rozwoju bezpieczeństwa narodowego*, „Studia Gdańskie. Wizje i rzeczywistość" 2016, t. 13, s. 9–29.

[32] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, s. 15–16, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 18.08.2023].

[33] C.J. Letavec, *The Program Management Office: Establishing, Managing And Growing the Value of a PMO*, J. Ross Publishing, Fort Lauderdale, FL 2006.

[34] T. Jabłoński, *Zarządzanie programami i projektami jako instrument realizacji celów publicznych*, „Współczesne Zarządzanie" 2013, nr 1, s. 212–221.

[35] *Program*, [hasło w:] Słownik języka polskiego PWN, https://sjp.pwn.pl/slowniki/program.html [dostęp: 18.08.2023].

prowadzącego zakład, z określeniem zadań i odpowiedzialności jego kierownictwa. Zadania i odpowiedzialność obejmują kontrolę zagrożeń awariami przemysłowymi oraz zapewnienie odpowiedniego do zagrożeń poziomu ochrony ludzi i środowiska. Kolejnym elementem jest określenie prawdopodobieństwa zagrożenia awarią przemysłową, wraz zasadami zapobiegania i sposobami ograniczania jej skutków[36]. Działania związane z zapobieganiem, zwalczaniem i ograniczaniem skutków awarii przemysłowej precyzuje wewnętrzny i zewnętrzny plan operacyjno-ratowniczy[37].

Właściciele zakładów o dużym ryzyku wystąpienia awarii są zobowiązani do przeprowadzania analizy takiego ryzyka i jego oceny. Analizy te są przeprowadzane na podstawie wytypowanych, reprezentatywnych zdarzeń i scenariuszy awaryjnych. Zwraca się uwagę na konieczność uwzględnienia awarii przemysłowych w planowaniu i zagospodarowaniu przestrzennym. Proces oceny ryzyka obejmuje następujące etapy: 1. charakterystyki instalacji, 2. identyfikacja źródeł zagrożeń, 3. scenariusze awaryjne, w tym wybór zdarzeń awaryjnych oraz reprezentatywnych zdarzeń awaryjnych i sporządzenie dla każdego z nich modelu scenariusza awaryjnego, 4. przygotowanie zintegrowanej ocena ryzyka dla wszystkich reprezentatywnych scenariuszy. Rozpatruje się wynikowe kategorie ryzyka oznaczające: ryzyko akceptowane, ryzyko tolerowane – akceptowane, ryzyko tolerowane – nieakceptowane oraz ryzyko nieakceptowane, prowadzące do zatrzymania instalacji[38].

Należy zwrócić uwagę na występowanie w Ustawie o zarządzaniu kryzysowym zapisu o zestawieniu sił i środków planowanych do wykorzystania w sytuacjach kryzysowych. Można go rozpatrywać z punktu widzenia teoretycznych podstaw związanych z koncepcjami: zasobową organizacji (firmy) i redundancji zasobów[39].

---

[36] Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, tekst jedn. Dz.U. z 2021 r., poz. 1973, art. 251, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210001973/U/D20211973Lj.pdf [dostęp: 18.08.2023]. „Prowadzący instalację lub zakład – właściciel instalacji lub zakładu albo podmiot, który włada instalacją lub zakładem na podstawie innego tytułu prawnego (definicja ustawy – POŚ)", *Informacje ogólne – Definicje*, Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, https://www.ciop.pl/CIOPPortalWAR/appmanager/ciop/pl?_nfpb=true&_pageLabel=P15000156221346925948558&html_tresc_root_id=25314&html_tresc_id=25315&html_klucz=25314&html_klucz_spis=25314 [dostęp: 9.08.2023].

[37] Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, art. 248, 249, 250, 251, 252, 260.

[38] W. Wiśniewski, G. Sobieszek, B. Połeć, *Zapobieganie poważnym awariom przemysłowym – studium przypadku na przykładzie województwa mazowieckiego*, „Bezpieczeństwo i Technika Pożarnicza" 2018, t. 51, nr 3, s. 150–169.

[39] W Ustawie o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (Dz.U. z 2007 r., nr 89, poz. 590) wymienione są elementy składowe planów (w tym odnośnie do zagrożeń infrastruktury krytycznej). Zawarto w niej także element związany z zestawieniem sił i środków planowanych do wykorzystania w sytuacjach kryzysowych.

Studia przypadków

Zgodnie z art. 248 Ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska i kryteriami określonymi w rozporządzeniu Ministra Rozwoju[40] zakłady należące do Orlen S.A. (do 3 lipca 2023 r. Polski Koncern Naftowy Orlen) zakwalifikowano jako zakłady o dużym ryzyku wystąpienia poważnej awarii przemysłowej (ZDR)[41]. Koncern przygotował m.in. program zapobiegania awariom, raport o bezpieczeństwie i wewnętrzny plan operacyjno-ratowniczy. W instrukcji zawarto m.in. opis postępowania w przypadku awarii (w tym: powiadomienia, obowiązki kierownictwa i obsługi, a także tworzenie zespołów awaryjnych i technicznych). W Orlen S.A. nie wystąpiły zdarzenia, które stanowiły istotne naruszenie bezpieczeństwa infrastruktury krytycznej (IK). Po kontroli czterech zdarzeń dwa z nich zakwalifikowano jako poważne awarie.

Odnośnie do planu zarządzania kryzysowego w koncernie Orlen S.A za lata 2013–2016[42], Najwyższa Izba Kontroli pozytywnie oceniła wykonanie zadań w zakresie zabezpieczenia infrastruktury krytycznej.

W ramach planu ochrony infrastruktury krytycznej odniesiono się do informacji o zasobach materiałowych organów administracji publicznej możliwych do wykorzystania przez Orlen w celu ochrony IK. Jako zasoby wymienia się m.in. samochody, radiostacje, syreny, zestawy ratownicze i autobusy. Wskazuje się na wykorzystanie zasobów ludzkich pochodzących m.in. z jednostek Ochotniczych Straży Pożarnych czy Straży Miejskiej. Wykorzystanie zasobów informacyjnych może dotyczyć np. systemów alarmowych czy rozgłośni radiowych, ponadto podkreśla się możliwość wykorzystania wskazanych punktów ewakuacyjnych. Operator IK może zwrócić się o pomoc do wójta, burmistrza lub prezydenta właściwego dla terenu. Wskazuje się na współpracę koncernu Orlen z administracja publiczną, mając na względzie przekazywanie informacji o zagrożeniach, ale także danych o posiadanych zasobach sprzętowych i materiałowych, które mogą być wykorzystane w sytuacji zagrożenia. Odnośnie do zakłóceń w dostępie do zewnętrznych źródeł zaopatrzenia, Orlen podjął działania zmniejszające uzależnienie funkcjonowania IK od zewnętrznych usług zaopatrzenia

---

[40] Rozporządzenie Ministra Rozwoju z dnia 29 stycznia 2016 r. w sprawie rodzajów i ilości znajdujących się w zakładzie substancji niebezpiecznych, decydujących o zaliczeniu zakładu do zakładu o zwiększonym lub dużym ryzyku wystąpienia poważnej awarii przemysłowej, Dz.U. z 2016 r., poz. 138.

[41] NIK Delegatura w Bydgoszczy, *Wystąpienie pokontrolne. P/16/093 – Bezpieczeństwo obiektów infrastruktury krytycznej* (jednostka kontrolowana: Polski Koncern Naftowy ORLEN S.A., Płock), https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,lby~p_16_093_20160428081222146183114 2~id2~01,typ,kj.pdf [dostęp: 14.08.2023]. Wykaz 200 zakładów o dużym ryzyku wystąpienia poważnej awarii przemysłowej w poszczególnych województwach w Polsce według stanu na 31.12.2021 opublikował Główny Inspektorat Ochrony Środowiska: *Poważne awarie*, Główny Inspektorat Ochrony Środowiska, http://www.gios.gov.pl/pl/25-powazne-awarie [dostęp: 10.08.2023].

[42] NIK Delegatura w Bydgoszczy, *Wystąpienie pokontrolne. P/16/093...*, *op. cit.*, s. 10–11.

w energię elektryczną, wodę i parę wodną, ropę naftową, gaz ziemny. W ramach IK zbudowano redundantną (nadmiarowa) sieć komputerową, posiadającą zasilanie awaryjne. Wprowadzono zasady wykonywania prac w ramach IK, uwzględniając zaangażowanie podmiotów zewnętrznych.

Współdziałanie z jednostkami zewnętrznymi pozwala na wzmacnianie roli kapitału o charakterze relacyjnym. Kapitał strukturalny opiera się na elementach struktury organizacyjnej wraz z podejściem procesowym i wsparciem materialnym polegającym na tworzeniu nadmiarowych zasobów. W szczególności w sytuacji zagrożenia na znaczeniu będzie zyskiwał kapitał społeczny. W przyjętych dokumentach zwraca się uwagę na znaczenie powiązań sieciowych, również na poziomie lokalnym.

Grupa Lotos S.A. stanowi pionowo zintegrowany koncern naftowy, obejmujący także spółki zależne. Ta grupa kapitałowa zajmuje się wydobyciem i przerobem ropy naftowej oraz sprzedażą produktów naftowych. Zakład jest zakwalifikowany jako charakteryzujący się dużym ryzykiem wystąpienia poważnej awarii przemysłowej, stwarzającej zagrożenie dla ludzi i środowiska. Grupa Lotos jest operatorem trzech obiektów infrastruktury krytycznej[43]. Opisane zostały kluczowe dokumenty stanowiące podstawę działań dla zapewnienia bezpieczeństwa w zakładzie. Wśród nich wymienia się „Program zapobiegania poważnym awariom przemysłowym" – obejmuje on określenie prawdopodobieństwa zagrożenia awarią przemysłową, zasady zapobiegania oraz zwalczania skutków awarii przemysłowych; wskazuje się także na częstotliwość przeprowadzania analiz. Kolejnym dokumentem jest „Raport o bezpieczeństwie" obejmujący analizę możliwości wystąpienia awarii różnego typu. Zawiera on scenariusze możliwych awarii urządzeń produkcyjnych wraz z możliwymi scenariuszami rozwoju zdarzenia. Obejmuje także skutki awarii i działania ratownicze. Zakłada się cykliczne remonty całego zakładu produkcyjnego co cztery lata[44]. Podawane są także przykłady dotyczące infrastruktury krytycznej podmiotów w grupie Lotos. Przykładowo dotyczy to Energobaltic Sp. z o.o. we Władysławowie, wchodzącej w skład grupy Lotos Petrobaltic S.A.[45]. Energobaltic jest zakładem o zwiększonym ryzyku powstania poważnej awarii przemysłowej. Główne zagrożenia są związane z pożarami i wybuchami w przypadku rozszczelnienia instalacji. Przygotowany plan zapobiegania poważnym awariom odnosi się także do zapewnienia zasobów: finansowych, materialnych i intelektualnych.

W lipcu 2020 r. Orlen S.A. otrzymał od Komisji Europejskiej warunkową zgodę na przejęcie Grupy Lotos, związaną m.in. z wydzieleniem części aktywów Lotosu

---

[43] R. Wódkiewicz, *Ochrona obiektu infrastruktury krytycznej na przykładzie Grupy LOTOS S.A.*, „Wiadomości Naftowe i Gazownicze" 2018, nr 6(236), s. 4–9, https://www.cire.pl/pliki/2/2018/wnig_06_2018_6_11.pdf [dostęp: 14.08.2023].

[44] *Ibidem*, s. 6–9.

[45] *Informacja dotycząca zakładu zwiększonego ryzyka*, Energobaltic, https://energobaltic.orlen.pl/pl/o-firmie/Nasze-standardy/Informacja-dotyczaca-zakladu-zwiekszonego-ryzyka [dostęp: 14.08.2023].

na rzecz partnerów zewnętrznych. Partnerów tych Orlen zaprezentował w styczniu 2022 r.[46]. Od 1 sierpnia 2022 r. Grupa Lotos S.A. jest częścią Grupy Orlen. W tej sytuacji rozwiązania dotyczące grup Orlen i Lotos można rozważać łącznie. Inicjatywy te mają charakter strategiczny i długookresowy. Równocześnie przygotowywane są programy i plany mające na celu zapewnienie bieżącego funkcjonowania przedsiębiorstw i utrzymania ciągłości działania nawet w sytuacjach awaryjnych. Takie podejście nawiązuje do zachowań o charakterze *ambidexterity*.

W dokumentach dotyczących Orlen S.A. oraz Grupy Lotos S.A. występują elementy składające się na funkcjonowanie architektury bezpieczeństwa biznesu, a więc odnoszące się do utrzymania ciągłości działania, relacji społecznych i dostosowania struktur organizacyjnych do zagrożeń awariami przemysłowymi.

Podsumowanie

Działania strategiczne organizacji rezylientnej, przygotowanej na możliwość wystąpienia kryzysu, także pozaekonomicznego, powinny uwzględniać możliwości tkwiące we współczesnych koncepcjach zarządzania. Można je wykorzystywać w programach zapobiegania ewentualnym awariom przemysłowym.

Realizacja tych koncepcji ma odzwierciedlenie w budowanej architekturze bezpieczeństwa biznesu, z wykorzystaniem dostępnych zasobów i procesów. Narzędziem zarządzania pozwalającym na ich ocenę jest audyt. Obejmować on może także ocenę szczególnie ważnych dla bezpieczeństwa biznesu zasobów niematerialnych.

W organizacjach stwarzających ryzyko poważnych awarii przemysłowych tworzenie nadmiarowych zasobów niematerialnych odbywać się może poprzez ciągłe doskonalenie kapitału intelektualnego. Do oceny tego kapitału można włączyć aspekty związane z zapewnieniem bezpieczeństwa. Na jego poziom będzie mieć wpływ zdobywanie i podnoszenie kompetencji przez pracowników i kierownictwo, korzystanie z doświadczeń innych podmiotów, uczenie się poprzez ćwiczenia i symulacje, rozwijanie powiązań sieciowych. Rozwój kapitału intelektualnego powinien dotyczyć orientacji ekologicznej podmiotów gospodarczych związanych z ECSR. Koncepcja ta jest nastawiona innowacyjnie, uwzględnia rolę współpracy z interesariuszami. Przyjęcie założeń ECSR może być dla firm, w których występuje zagrożenie awarią przemysłową, wskazówką do budowy nadmiarowych zasobów w ramach kapitału intelektualnego. ECSR wywodzi się z założeń CSR i odnosi się do podmiotów odpowiedzialnych społecznie – warto zwrócić uwagę, że operatorzy działań na rzecz

[46] *Wielka fuzja Orlenu i Lotosu na ostatniej prostej. Zgoda Brukseli na przejecie*, Parkiet, 20.06.2022, https://www.parkiet.com/surowce-i-paliwa/art36538361-wielka-fuzja-orlenu-i-lotosu-na-ostatniej-prostej-zgoda-brukseli-na-przejecie [dostęp: 14.08.2023].

infrastruktury krytycznej są traktowani jako odpowiedzialni społecznie[47]. Nastawienie strategiczne, z równoczesnym zapewnieniem ciągłości działania w sytuacjach awaryjnych, można odnosić do koncepcji *ambidextrity*.

Redundancję zasobów w powiązaniach sieciowych, w tym w oparciu o kapitał intelektualny, można analizować z wykorzystaniem zapisów Narodowego Programu Ochrony Infrastruktury Krytycznej. Jedną z najważniejszych zasad programu jest współpraca polegająca na wymianie informacji w oparciu o: 1. forum ochrony IK, 2. bezpośrednie kontakty stron (jako element mechanizmu ochrony IK), 3. wspólne szkolenia, konferencje, doradztwo, a także organizację ćwiczeń[48].

Występujące w Programie pojęcie wymiany informacji można wiązać z koncepcją zarządzania wiedzą. Przepływ informacji ma istotne znaczenie w budowie kapitału intelektualnego – jako element składowy kapitału strukturalnego czy relacyjnego – a podkreślane w dokumencie pojęcie zaufania nawiązuje wprost do roli kapitału społecznego.

Bibliografia

Bugaj J., Witek A., *Rezyliencja jako element modelu kompetencji menedżera do zarządzania kryzysem*, „Studia i Prace Kolegium Zarządzania i Finansów SGH" 2022, nr 184, s. 9–19, https://econjournals.sgh.waw.pl/SiP/article/view/2939/2605 [dostęp: 17.07.2023].

Chodyński A., *Dynamika przedsiębiorczości i zarządzania innowacjami w firmach. Odpowiedzialność – prospołeczność – ekologia – bezpieczeństwo*, Oficyna Wydawnicza AFM, Kraków 2021.

Chodyński A., *Kreowanie odpowiedzialnego biznesu*, Oficyna Wydawnicza AFM, Kraków 2016.

Chodyński A., *Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezyliencji organizacyjnej*, [w:] *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw*, red. A. Chodyński, D. Fatuła, M.A. Leśniewski, Oficyna Wydawnicza AFM, Kraków 2022, s. 11–31.

Chodyński A., *Sieciowość w koncepcjach biznesu – aspekty społeczne i ekologiczne*, [w:] *Zarządzanie odpowiedzialnym rozwojem przedsiębiorstwa*, red. A. Chodyński, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2012, s. 83–110.

Chodyński A., *Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym*, „Bezpieczeństwo. Teoria i Praktyka" 2014, nr 1, s. 13–27.

Chodyński A., *Uczenie się i wpływ społeczny a bezpieczeństwo na poziomie lokalnym – zarządzanie w sytuacji awarii zagrażającej środowisku naturalnemu*, „Bezpieczeństwo. Teoria i Praktyka" 2021, nr 4, s. 61–80.

Chodyński A., *Using ambidexterity in the ecological security management of organisations*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 49–59.

Chodyński A., *Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja smart*, „Bezpieczeństwo. Teoria i Praktyka" 2019, nr 4 , s. 39–62.

[47] *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity*, 2023, s. 20, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 8.02.2024].

[48] *Narodowy Program Ochrony Infrastruktury Krytycznej*, *op. cit.*, s. 32.

Giszterowicz A., *Operationalising a safety culture in the management of a business entity (case study)*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 91–102.

Informacja dotycząca zakładu zwiększonego ryzyka, Energobaltic, https://energobaltic.orlen.pl/pl/o-firmie/Nasze-standardy/Informacja-dotyczaca-zakladu-zwiekszonego-ryzyka [dostęp: 14.08.2023].

Informacje ogólne – Definicje, Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, https://www.ciop.pl/CIOPPortalWAR/appmanager/ciop/pl?_nfpb=true&_pageLabel=P15000156221346925948558&html_tresc_root_id=25314&html_tresc_id=25315&html_klucz=25314&html_klucz_spis=25314 [dostęp: 9.08.2023].

Jabłoński T., *Zarządzanie programami i projektami jako instrument realizacji celów publicznych*, „Współczesne Zarządzanie" 2013, nr 1, s. 212–221.

Jaruszewski W.K., *Rola kapitału intelektualnego i kultury w rozwoju bezpieczeństwa narodowego*, „Studia Gdańskie. Wizje i rzeczywistość" 2016, t. 13, s. 9–29.

Knapp H.P., *Designing and implementing an interdependent resilience culture*, „Journal of Business Continuity & Emergency Planning" 2016, vol. 10, nr 1, s. 76–83.

Krupski R., *Okazje w zarządzaniu strategicznym przedsiębiorstwa*, „Organizacja i Kierowane" 2011, nr 4(147), s. 11–24.

Kwieciński M., *Procesowe i systemowe ujęcie procesu zarządzania bezpieczeństwem*, „Bezpieczeństwo. Teoria i Praktyka" 2012, nr 2, s. 57–64.

Letavec C.J., *The Program Management Office: Establishing, Managing And Growing the Value of a PMO*, J. Ross Publishing, Fort Lauderdale, FL 2006.

Libertowska A.M., *Wpływ kapitału społecznego na zarządzanie wartością przedsiębiorstw z branż zaawansowanych technologii w Wielkopolsce*, rozprawa doktorska, Politechnika Poznańska, 2019, s. 30–34, 54, https://sin.put.poznan.pl/dissertations/details/d171 [dostęp: 14.08.2023].

Lichtarski J., *Koncepcje zarządzania czy funkcje przedsiębiorstwa*, „Przegląd Organizacji" 2001, nr 9, s. 27–28.

Łobos K., *Koncepcje zarzadzania*, Wydawnictwo Wyższej Szkoły Bankowej w Poznaniu, Poznań 2021.

Mierzejewska L., Sikorska-Podyma K., Wdowicka M., Lechowska E., Modrzewski B., *City resilience – aspekty planistyczne*, „Rozwój Regionalny i Polityka Regionalna" 2020, nr 50, s. 83–99.

Milewski J., *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe AON" 2016, nr 4 (105), s. 99–115.

Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity, 2023, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 8.02.2024].

NIK Delegatura w Bydgoszczy, *Wystąpienie pokontrolne. P/16/093 – Bezpieczeństwo obiektów infrastruktury krytycznej* (jednostka kontrolowana: Polski Koncern Naftowy ORLEN S.A., Płock), https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,lby~p_16_093_2016042808122214618311 42~id2~01,typ,kj.pdf [dostęp: 14.08.2023].

Olejczyk-Kita K., *Uczenie się organizacji – aspekt zasobowy*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2013, nr 310, s. 83–90.

Poważne awarie, Główny Inspektorat Ochrony Środowiska, http://www.gios.gov.pl/pl/25-powazne-awarie [dostęp: 10.08.2023].

Rela I.Z., Awang A.H., Ramli Z., Md Sum S., Meisanti M., *Effects of environmental corporate social responsibility on environmental well-being perception and the mediation role of community resilience*, „Corporate Social Responsibility and Environmental Management" 2020, vol. 27, nr 5, s. 2176–2187.

Renaud K., von Solms B., von Solms R., *How does intellectual capital align with cyber security?*, „Journal of Intellectual Capital" 2019, vol. 20, nr 5, s. 621–641.

Shirali Gh. A., Shekari M., Angali K.A., *Quantitative assessment of resilience safety culture using principal components analysis and numerical taxonomy: A case study in a petrochemical plant*, „Journal of Loss Prevention in the Process Industries" 2016, vol. 40, s. 277–284.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 18.08.2023].

Sus A., *Dynamika modeli biznesu*, „Nauki o Zarządzaniu/ Management Sciences" 2014, nr 1(18), s. 90–99.

Ujwary-Gil A., *Audyt zasobów niematerialnych z wykorzystaniem analizy sieci organizacyjnej*, Wydawnictwo Naukowe PWN, Warszawa 2017.

Wielka fuzja Orlenu i Lotosu na ostatniej prostej. Zgoda Brukseli na przejecie, Parkiet, 20.06.2022, https://www.parkiet.com/surowce-i-paliwa/art36538361-wielka-fuzja-orlenu-i-lotosu-na-ostatniej-prostej-zgoda-brukseli-na-przejecie [dostęp: 14.08.2023].

Wiśniewski W., Sobieszek G., Połeć B., *Zapobieganie poważnym awariom przemysłowym – studium przypadku na przykładzie województwa mazowieckiego*, „Bezpieczeństwo i Technika Pożarnicza" 2018, t. 51, nr 3, s. 150–169.

Woźniak J., *Bezpieczeństwo ekonomiczne organizacji gospodarczych a koncepcje przedsiębiorczości*, „Nowoczesne Systemy Zarządzania" 2013, t. 8, nr 1, s. 49–63.

Wódkiewicz R., *Ochrona obiektu infrastruktury krytycznej na przykładzie Grupy LOTOS S.A.*, „Wiadomości Naftowe i Gazownicze" 2018, nr 6(236), s. 4–9, https://www.cire.pl/pliki/2/2018/wnig_06_2018_6_11.pdf [dostęp: 14.08.2023].

Wróblewski R., *Elementy koncepcji zarządzania bezpieczeństwem narodowym*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2021, t. 7, nr 1, s. 7–26.

Wyrębek H., *Narzędzia wspomagające proces zarządzania wiedzą i bezpieczeństwem ekonomicznym w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie" 2015, t. 32, nr 105, s. 227–240.

Zakrzewska-Bielawska A., *Zasobowe uwarunkowania koopetycji w przedsiębiorstwach high-tech*, „Przegląd Organizacji" 2013, nr 2, s. 3–8.

Akty prawne

Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, tekst jedn. Dz.U. z 2021 r., poz. 1973, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210001973/U/D20211973Lj.pdf [dostęp: 18.08.2023].

Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007, Dz.U. z 2007 r., nr 89, poz. 590.

Rozporządzenie Ministra Rozwoju z dnia 29 stycznia 2016 r. w sprawie rodzajów i ilości znajdujących się w zakładzie substancji niebezpiecznych, decydujących o zaliczeniu zakładu do zakładu o zwiększonym lub dużym ryzyku wystąpienia poważnej awarii przemysłowej, Dz.U. z 2016 r., poz. 138.

Wpływ koncepcji zarządzania na architekturę bezpieczeństwa biznesu – programy zapobiegania awariom przemysłowym

Streszczenie

Określono wpływ koncepcji zarządzania na budowę architektury bezpieczeństwa biznesu zapewniającej rezylientne zachowania podmiotów gospodarczych w sytuacji zagrożeń o charakterze pozaekonomicznym. Przeanalizowano rolę nadmiarowych

zasobów, w szczególności o charakterze niematerialnym, na budowę tej architektury. Podkreślono znaczenie takich zasobów jak kapitał intelektualny, kapitał społeczny, powiązania sieciowe czy zarządzanie wiedzą, a także CSR i ECSR. Zwrócono uwagę na możliwości ich wykorzystania w sytuacji kryzysowej. Uwzględniono rolę koncepcji *ambidexterity*, łączącej myślenie strategiczne z zapewnieniem ciągłości działania w przypadku sytuacji awaryjnej. Szczególną uwagę zwrócono na możliwość wystąpienia awarii przemysłowych w podmiotach infrastruktury krytycznej. Na podstawie studiów przypadków zaprezentowano programy i plany dla wybranych przedsiębiorstw przemysłu petrochemicznego o dużym ryzyku wystąpienia poważnej awarii przemysłowej. Programy odniesiono do elementów architektury biznesu.

Słowa kluczowe: koncepcje zarządzania, model architektury bezpieczeństwa biznesu, zasoby niematerialne organizacji, rezyliencja organizacyjna, awarie przemysłowe

Impact of management concepts on business safety architecture: industrial accident prevention programmes

Abstract

The influence of management concepts on the construction of a business security architecture ensuring the resilient behaviour of business entities in a situation of non-economic threats was determined. The role of redundant resources, especially of an intangible nature, on the construction of this architecture was analysed. The importance of resources such as intellectual capital, social capital, network connections or knowledge management, as well as CSR and ECSR was emphasised. Attention was drawn to the possibility of using them in a crisis situation. The role of the concept of ambidexterity, combining strategic thinking with ensuring business continuity in the event of an emergency, was considered. Special attention was given to the possibility of industrial accidents for critical infrastructure entities. Based on case studies, programmes and plans were presented for selected petrochemical companies with a high risk of a major industrial accident. The plans and programmes were related to the elements of the business architecture.

Keywords: management concepts, business safety architecture model, intangible resources of an organisation, organisational resilience, industrial accidents