STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 199

199/2024
s. 55–77

Szkoła Główna Handlowa w Warszawie
Kolegium Zarządzania i Finansów
https://econjournals.sgh.waw.pl/SiP

Piotr Zaskórski
Wojskowa Akademia Techniczna w Warszawie
ORCID: https://orcid.org/0000-0002-2598-1859

Jacek Woźniak
Wojskowa Akademia Techniczna w Warszawie
ORCID: https://orcid.org/0000-0001-7592-0109

Sprawność informacyjna a odporność na ryzyko utraty ciągłości działania współczesnej organizacji

Streszczenie

W artykule podjęto próbę holistycznego ujęcia problemu przeciwdziałania ryzyku utraty ciągłości działania współczesnych organizacji w szybkozmiennym otoczeniu. Środowisko systemów i współczesnych platform teleinformatycznych z wykorzystaniem usług cyberprzestrzeni determinują sprawność informacyjną organizacji. Autorzy przywołują kilka strategii bazujących na systemach różnych klas typu systemy dziedzinowe, zintegrowane systemy informatyczne zarządzania klasy OLTP oraz OLAP, a także rozwiązania klasy *big data*, zapewniające generowanie wiedzy, które są istotnym wzmocnieniem potencjału organizacji i zapewniania jej ciągłości działania. Odwołują się również do usług w chmurze obliczeniowej, eliminujących wykluczenie informacyjne małych podmiotów gospodarczych. Celem opracowania jest potwierdzenie, że szerokie wykorzystanie środowiska IT/ICT odgrywa kluczową rolę w transformacji współczesnych organizacji, a implementacja różnych platform i narzędzi zwiększa ich odporność na ryzyko utraty biznesowej ciągłości działania. W realizacji procesów badawczych wykorzystano analizę literatury przedmiotu (z wykorzystaniem metody przeglądu narracyjnego) oraz analizę *desk research*, sprowadzającą się do oceny stopnia przydatności narzędzi IT/ICT w kreowaniu ciągłości działania. Zastosowano także metody syntezy i redukcji. Autorzy chcą podkreślić fakt, że

narzędzia IT/ICT, w tym wybrane modele sztucznej inteligencji, mają istotne implikacje zarówno dla teorii, jak i praktyki zarządzania.

Słowa kluczowe: informacja, system, technologie IT/ICT, ryzyko, ciągłość działania
Kody klasyfikacji JEL: D81, M15

1. Wprowadzenie

Środowisko systemów i współczesnych platform teleinformatycznych determinują sprawność informacyjną organizacji. Sprawność ta wyznaczana jest w dużej mierze zdolnością do zbierania, selekcji, gromadzenia i utrzymywania danych wspierających funkcjonowanie i zarządzanie organizacjami z uwzględnieniem ich bezpieczeństwa i ciągłości działania. Przetwarzanie tych zasobów danych i bezpieczne udostępnianie informacji generowanej z nich bez ograniczeń czasu i miejsca jest walorem wyznaczającym systemową i biznesową ciągłość działania [zob. Zaskórski, 2012]. Wśród narzędzi wspierających procesy gromadzenia i eksploracji danych należy wyakcentować zarówno systemy dziedzinowe, jak i zintegrowane systemy informatyczne zarządzania klasy OLTP (ang. *on-line transaction processing*) oraz OLAP (ang. *on-line analytical processing*) [zob. Januszewski, 2008a, 2008b]. Szczególnego znaczenia nabierają aktualnie rozwiązania klasy *big data*, zapewniające przetwarzanie i wizualizację wyników analiz wielopostaciowych danych, a wybrane algorytmy analizy i wnioskowania prowadzą do generowania zasobów wiedzy [zob. Mayer-Schonenberger, Cukier, 2014]. Bazy wiedzy to istotne wzmocnienie potencjału organizacji i zapewniania jej ciągłości działania. Ciągłość działania może mieć wiele wymiarów, a wymiar informacyjny staje się dziś ważnym komponentem systemowej i biznesowej ciągłości funkcjonowania organizacji traktowanej jako złożony system działania. Stąd szczególnego znaczenia nabierają usługi w chmurze obliczeniowej, eliminujące poniekąd wykluczenie informacyjne wielu firm klasy MŚP [zob. Mateos, Rosenberg, 2011] oraz systemy i modele sztucznej inteligencji [zob. Świątkowski, 2021].

Celem opracowania jest potwierdzenie, że szerokie wykorzystanie środowiska IT/ICT (ang. *information technology/information and communication technology*) odgrywa kluczową rolę w transformacji współczesnych organizacji, a implementacja różnych platform i narzędzi zwiększa ich odporność na ryzyko utraty biznesowej ciągłości działania. Systemy IT/ICT wspomagają bowiem analizę danych, prognozowanie trendów rynkowych oraz identyfikację optymalnych strategii działania, co przekłada się na bardziej trafne i świadome decyzje.

Autorzy pragną wyeksponować także wnioski dla teorii i praktyki – przede wszystkim to, że narzędzia IT/ICT, w tym wybrane modele AI (ang. *artificial intelligence* – sztuczna inteligencja), mają implikacje zarówno dla teorii, jak i praktyki, wskazując na konieczność adaptacji firm do nowych technologicznych trendów celem utrzymania pozycji rynkowej.

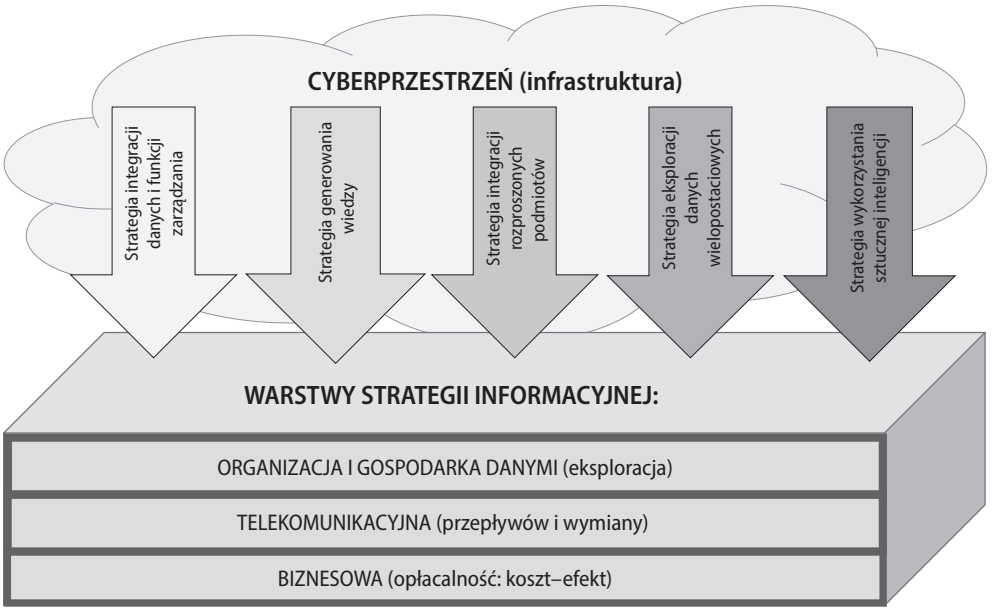
2. Strategie informacyjne współczesnych organizacji i ocena ich sprawności

Strategie informacyjne obejmują zarówno organizację zasobów danych i gospodarkę nimi, jak również sposób sprawnego przepływu danych i informacji z uwzględnieniem zasadności ekonomicznej tych procesów (rysunek 1). Biznesowa ciągłość działania współczesnych organizacji jest silnie warunkowana informacyjną ciągłością komunikowania się różnych podmiotów przy zapewnieniu bezpieczeństwa zasobów informacyjnych każdego podmiotu. Stąd strategie informacyjne powinny uwzględniać zagrożenia i materializację ryzyka utraty informacyjnej ciągłości działania [por. Liderman, 2017; Zaskórski, 2011, s. 67–98]. Gospodarka danymi jest bezpośrednio związana z poziomem rozwoju technologicznego firmy i stosowanymi narzędziami oraz platformami IT/ICT, a także zwykle ze statusem finansowym firmy i jej pozycją rynkową. Zaawansowane technologie niestety generują nowe zagrożenia dla bezpieczeństwa danych i systemów wymiany informacji. Zapewnianie poziomu poufności, niezawodności i integralności zasobów informacyjnych należy do ważnych komponentów strategii informacyjnych oraz ciągłości działania. Cały proces zarządzania współczesnymi organizacjami (często rozproszonymi, a nawet wirtualnymi) powinien być postrzegany kompleksowo, a strategie informacyjne powinny być stałym komponentem strategii biznesowych. Modele i systemy oraz narzędzia zapewniające informacyjną ciągłość działania poszczególnych podmiotów wymagają ciągłego pozyskiwania danych o środowisku i jego otoczeniu oraz o procesach i zagrożeniach w nim występujących. Jednocześnie ważne jest budowanie akceptowalnego poziomu odporności organizacji do skutecznego przeciwdziałania zagrożeniom i reagowania na nie we wszystkich podsystemach danej organizacji. Rozwój narzędzi i platform IT/ICT sprzyja doskonaleniu strategii informacyjnych ze szczególnym uwzględnieniem silnych mechanizmów komunikacyjnych zapewniających pożądany poziom bezpieczeństwa wymiany informacji [por. Tapscott, Tapscott, 2019], jak również mechanizmów eliminujących wykluczenie informacyjne. Idea koncepcji *X-engineeringu* wręcz wymusza integrację całego łańcucha wartości dodanej poprzez stosowanie coraz bardziej zaawansowanych technologii teleinformatycznych. Klasyczne zintegrowane systemy informatyczne zarządzania (ZSIZ) [zob. Januszewski, 2008a] zyskały stałą swoją obecność w strukturach zarządzania współczesną organizacją i zbudowano na nich strategię integracji danych i funkcji zarządzania. Był to ważny etap tworzenia strategii informacyjnych z wykorzystaniem zgromadzonych zasobów z różnych, autonomicznych systemów dziedzinowych (tzw. „wyspy" informacyjne, np. dla logistyki, procesów kadrowych, finansowych itp.). Systemy te wykorzystują dobrze sprawdzone w praktyce modele bazodanowe, które mogą gromadzić i obsługiwać wspólne, standardowo uporządkowane zasoby informacyjne, co może sprzyjać ich integralności oraz skuteczności całego procesu decyzyjnego w firmie.

Przejście na wyższy poziom przetwarzania sieciowego i technologii zgłębiania danych implikuje nowe wyzwania dla strategii informacyjnych, co oznacza, że powstaje strategia generowania wiedzy z wykorzystaniem coraz bardziej zaawansowanych modeli eksploracji

danych i odkrywania wiedzy dostosowanej do potrzeb organów decyzyjnych [Zaskórski, 2012, s. 74–75, 201–244, 247–277; Januszewski, 2008b]. Przechowywane dotychczas dane operacyjne w systemach klasy ZSIZ (ogólniej w bazach danych systemów OLTP) nie mogą „ginąć", a wręcz powinny zasilać sukcesywnie zasoby danych analitycznych (historycznych/utrzymywanych w hurtowniach danych wykorzystywanych w modelach OLAP). Dane te zyskują nową wartość (w tym wartość statystyczną) i mogą być podstawą do generowania obiektywnej wiedzy i wzmacniania odporności na ryzyko utraty ciągłości działania szczególnie organizacji procesowej [Woźniak, Zaskórski, 2018, s. 75–97].

Rysunek 1. Warstwy i wybrane klasy strategii informacyjnych



Źródło: opracowanie własne.

Reakcja świata na wykluczenie informacyjne, oprócz dostępu do podstawowych usług informacyjnych z poziomu sieci powszechnej typu Internet, zorientowana została na potrzeby firm klasy MŚP o ograniczonym poziomie zasobów (także finansowych). Powstaje zatem strategia integracji rozproszonych podmiotów poprzez dostęp do profesjonalnych usług informacyjnych w chmurze obliczeniowej (ang. *cloud computing*, CC) [Websecurity.pl, 2022; Mateos, Rosenberg, 2011, s. 38–39]. Jak już wspomniano, wspólne zasoby informacyjne mogą być wartością ważną dla skutecznego współdziałania w rozproszeniu. Dotyczy to zarówno utrzymywania baz danych transakcyjnych (bieżących), związanych z działalnością operacyjną, jak i hurtowni danych jako statystycznej bazy danych historycznych (analitycznych). Możliwość eksploracji zasobów własnych i potencjalnych partnerów (współdziałanie jako wyzwanie ery Industry 4.0) może wspierać procesy zapewniania ciągłości działania [Zaskórski i in., 2021, s. 123–158; Gilchrist, 2016].

Dotychczasowy tzw. „ład" informacyjny, czyli dobrze uporządkowane dane w postaci jednolitych struktur formalnych (rekordów, tabel faktów, wymiarów itp.), stawał się swoistym „gorsetem" ograniczającym wykorzystanie narastających lawinowo danych nieustrukturalizowanych lub słabo ustrukturalizowanych. Dlatego coraz większego znaczenia nabiera strategia eksploracji danych wielopostaciowych [por. ERP24.pl, 2022; Mayer-Schonenberger, Cukier, 2014] (tzw. systemy wielkiej objętości danych/*big data*, które obejmują oprócz tradycyjnych struktur także obrazy, filmy, teksty itp.). Zasoby te są gromadzone systematycznie w cyberprzestrzeni (nawet z pewnym naruszeniem prywatności), ale mogą być przetwarzane za pomocą aplikacji analitycznych, w tym z wykorzystaniem modeli i narzędzi sztucznej inteligencji, także w środowisku usług CC [zob. Chowdhury, 2018].

Współczesnym wyznacznikiem strategii informacyjnych jest wspomniana już era Industry 4.0 [Gilchrist, 2016], związana z ekspozycją procesów robotyzacji i automatyzacji oraz modeli sztucznej inteligencji. Era ta rozszerza strategię generowania wiedzy i poniekąd implikuje dużą dynamikę rozwoju strategii wykorzystania sztucznej inteligencji [zob. Goodfellow i in., 2016], w której zaawansowane technologicznie modele eksploracji wielkich/różnych zasobów danych i uczenia maszynowego mogą służyć trafnym procesom diagnostyczno-projekcyjnym i przewidywaniu dróg skuteczności/sprawności biznesowej. Zarówno dla strategii bazującej na idei systemów *big data*, jak i dla strategii bazującej na modelu AI, istotnym komponentem jest zbieranie i gromadzenie danych. Ilość (duża liczba obserwacji/duża objętość danych) jest wartością szczególną i stąd obie te strategie akceptują ideę Internetu rzeczy (IoT), Internetu wszechrzeczy (IoE), czy też tzw. Internetu przemysłowego (IIoT), jako możliwości zbierania wielu danych w czasie rzeczywistym [Miller, 2016, s. 33–62] z różnego typu sensorów/urządzeń monitorujących, również inteligentnych, ze wzbogaconymi funkcjami interpretacji.

Strategie informacyjne obejmują – jak już podkreślano – ze swej natury nie tylko problem organizacji danych i sposób ich przetwarzania, ale także sposób sprawnego przepływu danych i informacji z uwzględnieniem zasadności biznesowej (ekonomicznej) tych procesów. Każdy bowiem model strategii informacyjnej organizacji jest powiązany z systemami tworzenia i elektronicznego obiegu dokumentów, które powinny zapewniać bezpieczną wymianę danych. Stosowane są tu różne mechanizmy ochrony (podpis elektroniczny, szyfrowanie, hasła dostępu, kontrola dostępu itp.), co zapobiega materializacji ryzyka utraty ciągłości działania, jako konsekwencji utraty lub zniekształcenia informacji. Sprawność i efektywność strategii informacyjnych współczesnych organizacji wyznaczana jest jakością zasobów informacyjnych, a w tym także infrastruktury techniczno-technologicznej przeznaczonej dla gromadzenia, przetwarzania i udostępniania danych oraz generowanych na ich podstawie wiedzy i informacji.

Efektywna infrastruktura teleinformatyczna odgrywa kluczową rolę w możliwościach informatyzacji i usprawniania organizacji. Jej wpływ można rozpatrywać w różnych aspektach, a w szczególności pod kątem możliwości zapewniania wystarczającej przepustowości i wydajności, aby mogła obsługiwać rosnące zasoby danych generowanych przez urządzenia i różne systemy w organizacji. Dzięki temu systemy informatyczne wspierające procesy

zarządcze mogą działać wydajniej, a dostęp do danych i aplikacji można uzyskać szybko na odpowiednim poziomie niezawodności. Efektywna infrastruktura sieciowa umożliwia łatwą integrację nowych urządzeń i systemów z istniejącymi strukturami. Daje to także współczesnym organizacjom możliwość wprowadzenia nowych technologii i rozwiązań, takich jak IoT/IoE/IIoT bez zakłócania innych systemów. Ważnym czynnikiem jest również skalowanie rozumiane jako nadążanie i dostosowywanie się do rosnących potrzeb organizacji. Ponadto, dobrze zaprojektowana infrastruktura sieciowa zawiera mechanizmy bezpieczeństwa, które chronią dane i systemy organizacji przed zagrożeniami zewnętrznymi i wewnętrznymi, co wiąże się z zapewnianiem odpowiedniego poziomu ochrony informacji i prywatności danych. Powyższe atrybuty są komponentami sprawności strategii informacyjnych i dzięki temu organizacje mogą uzyskiwać pożądany poziom zaufania do wykorzystywanych systemów informatycznych z uwzględnieniem kryterium systemowej i biznesowej ciągłości działania warunkowanych nieprzerwaną obsługą klientów i pracowników. Dzięki niezawodnej i efektywnej infrastrukturze teleinformatycznej organizacje mogą analizować i przetwarzać dane w czasie rzeczywistym i ograniczać ryzyko utraty biznesowej ciągłości działania poprzez szybsze podejmowanie decyzji i reagowanie na zmieniające się warunki biznesowe. Ważnym komponentem jest tu także możliwość automatyzacji wybranych procesów biznesowych ze szczególnym uwzględnieniem ich efektywności i skrócenia czasu realizacji zadań. Te wartości przekładają się na wzrost efektywności operacyjnej organizacji i możliwość generowania wyższych zysków. Warto tu podkreślić, że efektywna infrastruktura sieciowa zapewnia fundament dla innowacji, umożliwiając organizacjom rozpoznawanie i wdrażanie nowych technologii i platform IT z założeniem rozwoju ich biznesu.

Niezawodność to kolejny atrybut sprawności strategii informacyjnej. Niezawodna infrastruktura teleinformatyczna gwarantuje ciągłość działania systemów informatycznych przy zachowaniu kryterium minimalizacji ryzyka różnego typu przestojów. Stąd tak ważne założenie, jakim jest zapewnienie redundancji i odporności na awarie. Ryzyko utraty danych lub przerw w usługach informacyjnych może negatywnie wpłynąć na obraz biznesowy całej firmy i dlatego procesy optymalizacji zasobów sieciowych są dominantą wydajności i efektywności infrastruktury. Oczywiście każdy poziom redundancji zasobów wiąże się ze wzrostem kosztów i dlatego współczesne organizacje muszą monitorować i zarządzać przepustowością, obciążeniem sieci oraz opóźnieniami, aby zapewnić płynną realizację usług informacyjnych. W codziennej realizacji tych usług zaleca się korzystanie z technologii równoważenia obciążenia eksploatowanej infrastruktury, aby zapewnić płynność pracy systemów. Ciągłe monitorowanie sieci pomaga w zapewnianiu ciągłości działania poprzez wykrywanie i rozwiązywanie problemów wydajnościowych oraz szybkie reagowanie na wszelkie nieprawidłowości przy założeniu odpowiedniej skalowalności infrastruktury sieciowej. Skalowalność infrastruktury sieciowej należy tu rozumieć jako zdolność dopasowania rozwiązań do faktycznych potrzeb organizacji według zmieniających się jej potrzeb. Elastyczność skalowania wskazuje na to, że infrastruktura powinna być zdolna do szybkiego zwiększenia lub zmniejszenia dostępnych zasobów. W tym miejscu należy odwołać się do rozwiązań chmurowych (CC), ponie-

waż pozwalają na łatwe skalowanie zasobów z możliwością elastycznego dostosowywania przepustowości, mocy obliczeniowej i przestrzeni pamięciowej w zależności od wymagań organizacji. Skalowalność ta pozwala organizacjom szybko integrować nowe technologie, a w tym technologie sztucznej inteligencji (AI) i przetwarzanie danych o bardzo dużej objętości (systemy *big data*) w czasie rzeczywistym [zob. Mayer-Schonenberger, Cukier, 2014]. Ponadto, usługi CC cechują się skutecznymi i sprawnymi mechanizmami bezpieczeństwa. W kontekście ciągłości działania należy widzieć proces zarządzania uprawnieniami oraz dostępem do sieci i danych jako kluczowe działanie dla ochrony organizacji przed atakami cybernetycznymi. Tak więc wydajność i skalowalność w kontekście strategii informatyzacji mają kluczowe znaczenie dla organizacji, które chcą zachować konkurencyjność połączoną ze wzrostem ich efektywności.

Wymiar biznesowy strategii informacyjnych wiąże się z analizą „koszt – efekt". Wykorzystywanie systemów klasy OLTP we współczesnej organizacji oznacza możliwość bieżącego i stałego monitorowania stanu realizacji procesów biznesowych i wykorzystania zasobów własnych firmy i jej partnerów oraz reagowania na różne nieprawidłowości lub awarie w czasie rzeczywistym. W aspekcie biznesowym może to oznaczać minimalizację wszelkiego typu strat, a więc utrzymanie odpowiedniego poziomu efektywności działań w różnych fazach i stanach ich realizacji. Dzięki tej klasy systemom możliwe jest unikanie ryzyka utraty ciągłości działania spowodowanej często np. brakiem zasobów materiałowych, nieterminowością dostaw, czy też zakłóceniami naruszającymi płynność realizacji innych procesów warunkujących działanie. Cała rodzina systemów klasy ZSIZ [por. Januszewski, 2008a] jest zbiorem sprawdzonych rozwiązań, począwszy od systemów pasywnych (inwentaryzacja zasobów typu IC/Inventory Control), a skończywszy na wielu aplikacjach systemów aktywnych, umożliwiających bieżącą ocenę efektów działania firmy oraz prognozowanie i planowanie potrzeb materiałowych (MRP I), planowanie innych zasobów produkcyjnych (MRP II) oraz planowanie wszystkich rodzajów zasobów firmy (ERP) ze szczególnym uwzględnieniem funkcji finansowych i zarządzania relacjami z klientami (CRM). Uaktualniane i rozwijane są kolejne aplikacje, które umożliwiają lepsze wykorzystanie potencjałów danej organizacji i efektywniejsze współdziałanie różnych podmiotów, począwszy od projektowania aż po monitorowanie i ocenę jakości wyników biznesowych na każdym etapie rozwoju produktu [Woźniak, Zaskórski, 2018, s. 35 i nast.]. Współczesne systemy OLTP to dobra platforma świadomego łączenia potencjałów i wykorzystanie zjawiska synergii we współdziałaniu różnych podmiotów. Pod względem biznesowym może to oznaczać możliwość pozyskiwania z otoczenia niezbędnych kompetencji i redukcję zapasów operacyjnych, a w ślad za tym wzrost efektywności operacyjnej z uwzględnieniem kryterium niskiego kosztu. Generowane w tych systemach oceny poprawiają trafność i pewność działania.

Strategia generowania wiedzy to rola systemów klasy OLAP, która bez wdrożenia strategii integracji (systemy OLTP) nie może być realizowana. Systemy te to droga do długofalowych ocen i projekcji działania na odległą perspektywę na bazie zasobów informacyjnych gromadzonych na różnych etapach procesów roboczych i decyzyjnych [Zaskórski i in., 2021,

s. 123–158]. Ten perspektywiczny ogląd sprzyja poprawie jakości, efektywności i ciągłości działania różnych realizowanych procesów. Cyklicznie lub zgodnie z harmonogramem gromadzenie danych z systemów OLTP do systemów OLAP [zob. Januszewski, 2008a, 2008b] umożliwia ich eksplorację i generowanie wiedzy analitycznej i prognostycznej z wykorzystaniem zaawansowanych technologii tzw. *data mining* (DM). Mogą powstawać zasoby wiedzy niejako eksperckiej, przydatnej nie tylko w ocenie zdarzeń z przeszłości (np. wykrywanie luk), ale przede wszystkim dla trafnego prognozowania (np. popytu w wielu wariantach wyznaczanych potrzebami rynku) i planowania potrzebnych działań dla realizacji ustalonego/wybranego wariantu prognozy w kontekście proefektywnościowych zmian.

Integracja i wirtualizacja podmiotów rozproszonych to przede wszystkim strategia poszukiwania potencjalnych partycypantów poprzez dostęp do zobiektywizowanych zasobów opisujących ich wartość kompetencyjno-rynkową [Zaskórski, Woźniak, 2023, s. 46 i nast.]. Profesjonalizacja usług CC przekłada się wprost na poziom integracji i ciągłości działania różnych, rozproszonych geograficznie i organizacyjnie podmiotów. Ponadto, chmura obliczeniowa powinna być traktowana jako alternatywne medium integracji z założeniem wzrostu poziomu niezawodności struktur i przez to ciągłości działania organizacji rozproszonych. Nie bez znaczenia jest także dostęp do zawansowanych technologii dla tzw. podmiotów klasy MŚP, które dotychczas nie były zdolne do pokrycia zbyt wysokich kosztów inwestycji teleinformatycznych. Skalowalność usług CC i adekwatność kosztów ich realizacji do skali/poziomu ich realizacji według indywidualnego zakresu – staje się argumentem biznesowym do wykorzystania tej klasy strategii [Miller, 2016]. Usługi CC są dynamicznie rozwijane i stanowią ważny komponent środowiska czwartej rewolucji przemysłowej [por. Gilchrist, 2016; Goodfellow i in., 2016], a także mogą znacząco wzmocnić bezpieczeństwo biznesowe i ciągłość działania.

Strategia eksploracji wielopostaciowych danych dużej objętości jest silnie związana ze zbieraniem i przetwarzaniem bardzo dużych ilości danych w różnych formatach do oceny sytuacji. Wartość tych zasobów dla potrzeb zarządzania jest wyznaczana liczbą obserwacji rzeczywistości nie tylko dla identyfikacji związków przyczynowo-skutkowych, ale przede wszystkim korelacji różnorodnych zjawisk/faktów, co jest atutem tzw. systemów klasy *big data* [por. Mayer-Schonenberger, Cukier, 2014; Chowdhury, 2018]. Funkcjonowanie tych systemów związane jest z wykorzystaniem zaawansowanych funkcji analitycznych (bazujących na modelach sztucznej inteligencji), które wymagają przetwarzania równoległego, co jest znaczącym nakładem. Oznacza to, że usługi tej klasy muszą być realizowane przez profesjonalne firmy z uwagi na skalę problemu i inwestycje z tym związane. Efektywność tych rozwiązań wyraża się wydajnością mechanizmów analitycznych, które mogą sprzyjać wzrostowi elastyczności oraz efektywności informacyjnej i decyzyjnej w turbulentnym otoczeniu dzięki wykorzystaniu np. modeli asocjacji, korelacji lub sekwencji czasowych, analizy skupień/dyspersji itp.

Strategia wykorzystania sztucznej inteligencji będzie częściowo przedmiotem dalszych rozważań z uwagi na rangę zalet, ale także rangę zagrożeń z niej płynących i możliwości przejmowania funkcji decyzyjnych. Jest to zarówno problem prawny, jak i etyczny w sferze

odpowiedzialności za skutki działania „podmiotu" tej klasy. Faktem jest, że liczba modeli AI i ich poziom zaawansowania technologicznego rosną bardzo szybko. Modele te zwykle związane są także z eksploracją dużych zasobów danych z wykorzystaniem złożonych algorytmów uczenia maszynowego różnych poziomów i przykładowo przetwarzania bardzo dużych wolumenów danych w czasie rzeczywistym (tzw. „strumieniowanie danych") w trybie interaktywnym przy użyciu zaawansowanych algorytmów, w połączeniu z wizualizacją wyników. Generowanie modeli zachowań różnych obiektów i zoptymalizowanego sposobu realizacji wybranych procesów staje się szczególną wartością biznesową, ale tak jak wspomniano – obarczoną ryzykiem.

Wszystkie zidentyfikowane wyżej strategie informacyjne warunkowane są dostępem do odpowiednich zasobów informacyjnych. Szczególnego znaczenia nabiera strategia gromadzenia danych bez ograniczeń czasu i miejsca zarówno z punktu widzenia systemów *big data*, jak i związanych z nimi modeli sztucznej inteligencji. Jedną z technologii pozyskiwania bardzo dużych ilości danych jest wspomniany Internet rzeczy [Miller, 2016] i inne jego pochodne. Systemy *big data* w połączeniu z funkcjami IoT dają w trybie *on-line* możliwość upowszechniania korygowanych na bieżąco zasobów wiedzy. Jest to swoista wartość biznesowa szczególnie dla podmiotów rozproszonych. Systemy zobrazowania i wizualizacji wyników analiz biznesowych (m.in. systemy informacji geoprzestrzennej – GIS) mogą odgrywać istotną rolę w komunikatywności przekazywanych wyników analiz wielowymiarowych ze szczególnym uwzględnieniem wykorzystania urządzeń mobilnych (czujniki, detektory itp.). Wykorzystanie różnych modeli geoanalizy pozwala na wykrycie korelacji, trendów czy zagrożeń, które są mniej dostrzegalne bez wizualizacji.

3. Usługi cyberprzestrzeni i cyberbezpieczeństwo jako determinanty ciągłości działania

Jak wcześniej akcentowano, zaawansowane technologie są integralnym elementem rozwijających się usług cyberprzestrzeni. Stąd zapewnianie cyberbezpieczeństwa w aspekcie poziomu poufności, niezawodności i integralności zasobów informacyjnych staje się ważną determinantą sprawności strategii informacyjnych oraz ciągłości działania. Niestety powstają tu nowe zagrożenia, ważne dla bezpieczeństwa danych i systemów wymiany informacji w środowisku sieci powszechnej typu Internet oraz w środowisku usług CC.

Istotną rolę odgrywają luki, słabości oraz wady systemowe, czyli braki i możliwe usterki całego systemu, które mogą występować w infrastrukturze techniczno-technologicznej, np. błędy w oprogramowaniu komputerowym lub wady proceduralne, np. błędne wytyczne, instrukcje, brak odpowiednich procedur komunikowania się. Tego typu zagrożenia w połączeniu z niskim poziomem odporności na nie i jednocześnie z podatnościami mogą prowadzić do materializacji ryzyka związanego z tymi zagrożeniami [UKSW, 2024]. We współczesnym, zglobalizowanym świecie, gdzie dominuje cyfryzacja procesów, systemów oraz różnych

procedur, istotne jest utrzymanie informacyjnej ciągłości działania, ponieważ niespełnienie tego kryterium może powodować skutki trudne do eliminacji szczególnie w wymiarze materialnym oraz funkcjonalnym. Dlatego z punktu widzenia zapewniania bezpieczeństwa usług informacyjnych istotnym kryterium staje się ryzyko utraty informacyjnej ciągłości działania. Należy przy tym mieć świadomość różnych ograniczeń zasobowych, przy czym ważna jest relacja między zagrożeniem oraz prawdopodobieństwem jego wystąpienia. Zwykłe zrozumienie mechanizmu przyczynowo-skutkowego pozwala na wychwycenie luk i słabości poszczególnych strategii informacyjnych, a w szczególności tych, które odwołują się do modeli sieciowych i usług w cyberprzestrzeni. Należy także podkreślić, że współczesne zagrożenia ulegają dynamicznym przekształceniom, a zmiany, które mają im się przeciwstawiać, zachodzą powoli, co wymusza ciągłość procesu monitorowania i analizy ryzyka.

Warto w tym miejscu zauważyć, że cyberprzestrzeń jest swoistym środowiskiem, które często jest dziś stawiane na równi z kategorią środowiska lądowego, wodnego, powietrznego, czy przestrzeni kosmicznej. Często cyberprzestrzeń traktuje się jako przestrzeń przetwarzania i wymiany informacji z wykorzystaniem różnych strategii działania i narzędzi w postaci rozwiązań teleinformatycznych wraz z powiązaniami pomiędzy nimi oraz relacjami z interesariuszami [Ustawa o stanie wyjątkowym, 2002, art. 2]. Coraz częściej eksponowany jest problem traktowania cyberprzestrzeni jako przede wszystkim przestrzeni komunikacyjnej tworzonej przez systemy powiązań internetowych i nawiązywanie relacji w czasie rzeczywistym [Marczyk, 2018, s. 59]. W zarządzaniu organizacjami biznesowymi ważna jest wirtualizacja współczesnych podmiotów i łączenie ich potencjałów, a cyberprzestrzeń rozumiana jest jako „wirtualny świat" [Gogołek, Cetera, 2014, s. 246]. Można zatem połączyć różne perspektywy postrzegania cyberprzestrzeni i uznać, że jest ona cyfrową przestrzenią przetwarzania i wymiany informacji, tworzoną przez różne platformy cyfrowe, systemy i sieci teleinformatyczne z uwzględnieniem powiązań pomiędzy nimi i relacji z aktualnymi i potencjalnymi użytkownikami według zaimplementowanych strategii informacyjnych [zob. Sienkiewicz, 2015]. Swoistym uzupełnieniem i pewnym kompleksowym domknięciem istoty cyberprzestrzeni jest jej potraktowanie jako globalnej domeny w środowisku informacyjnym z uwzględnieniem współzależnych sieci infrastruktury informatycznej i związanych z nimi zasobów danych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych urządzeń i obiektów techniczno-technologicznych takich jak: procesory, sensory i kontrolery [Joint Publication 1–02, 2010]. Przedstawione perspektywy postrzegania i wykorzystania cyberprzestrzeni skłaniają do uogólnienia, że cyberprzestrzeń stwarza warunki do sprawnej gospodarki zasobami informacyjnymi z wykorzystaniem odpowiednich narzędzi wspierających informacyjną ciągłość procesów decyzyjnych i ciągłość funkcjonowania całego podmiotu biznesowego. Cyberprzestrzeń jest zatem środowiskiem, na które składa się ląd, woda, powietrze, przestrzeń kosmiczna oraz pole elektromagnetyczne i umieszczone w tym środowisku obiekty (w tym ludzie), posiadające zdolności kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach [Liderman, 2023, s. 7].

Cyberbezpieczeństwo jest organicznie związane z pojęciem cyberprzestrzeni i powinno być traktowane jako dziedzina mająca na celu zapobieganie i ochronę przed skutkami negatywnego wykorzystania cyberprzestrzeni. Kategoria cyberzagrożeń dla funkcjonowania różnych podmiotów fizycznych lub prawnych w cyberprzestrzeni implikuje problem zapewniania cyberbezpieczeństwa i ciągłości działania. Cyberbezpieczeństwo bowiem należy traktować jako swoistą miarę odporności systemów informacyjnych (narzędzi IT/ICT) na różnorodne działania naruszające kryterium poufności, integralności, dostępności i autentyczności gromadzonych i przetwarzanych danych, a także związanych z nimi usług oferowanych przez te systemy [Ustawa o krajowym systemie cyberbezpieczeństwa, 2018, art. 2]. Zapewnianie cyberbezpieczeństwa wiąże się z zastosowaniem odpowiednich systemów, sieci, programów, urządzeń i technologii oraz procesów monitoringu/nadzorowania i procedur kontroli w celu ochrony zasobów informacyjnych przed atakami cybernetycznymi [Hackeru.pl, 2021] dla zachowania ciągłości funkcjonowania danej organizacji. Warto w tym miejscu wyakcentować szczególną rolę tego atrybutu cyberprzestrzeni i potwierdzić, że cyberbezpieczeństwo to pewien stan realizacji strategii (systemów) informacyjnych, związany z poziomem odporności przyjętych rozwiązań, przy określonym wcześniej poziomie zaufania, na wszelkie działania mogące naruszyć dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez wykorzystywane systemy informacyjne [Ministerstwo Klimatu i Środowiska, 2024]. Ponadto, eksponując globalne znaczenie kryterium cyberbezpieczeństwa, można stwierdzić, że jest to ważny wymiar bezpieczeństwa każdego systemu działania, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni wszystkich jego elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji zasobów informacyjnych i systemów teleinformatycznych) [BBN, 2023].

Reasumując, można stwierdzić, że bezpieczeństwo współczesnej organizacji i jej biznesowa ciągłość działania jest warunkowana poziomem cyberbezpieczeństwa, które należy traktować jako potrzebę realizacji zbioru zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Z tym pojęciem związana jest przede wszystkim potrzeba ochrony przestrzeni przetwarzania informacji oraz przepływów i interakcji w sieciach teleinformatycznych [Encyklopedia Zarządzania, 2024]. Ponadto, warto spojrzeć na wymiar cyberbezpieczeństwa jako strategię, politykę i zbiór norm dotyczących bezpieczeństwa zasobów i operacji w cyberprzestrzeni, które obejmują pełny zakres redukcji zagrożeń, zmniejszania podatności i nawet odstraszania potencjalnych „intruzów" z uwzględnieniem interakcji międzynarodowych/globalnych i natychmiastowej reakcji na incydenty, ponieważ ta kategoria nie zna granic państwowych i odnosi się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej [NIST SP 800–53 Rev. 5, 2020]. Cyberbezpieczeństwo jest stanem, w którym ryzyko może być minimalizowane lub eliminowane, a organizacja posiada zdolności zachowania ciągłości działania (BCM, ang. *business continuity management*) [BS 25999–1, 2006].

Cyberprzestrzeń i jej bezpieczeństwo w ujęciu potrzeb podmiotów biznesowych to alternatywny model usług informacyjnych czerpiących dane nie tylko z własnych systemów, ale także z otoczenia. Stąd ochrona danych osobowych oraz dążenie do zachowania prywatności uczestników procesów biznesowych stają się często wyzwaniem w aspekcie zarządzania bezpieczeństwem informacji. Stosowane procedury bezpiecznej wymiany informacji są koniecznym elementem przetwarzania danych o podwyższonym poziomie wrażliwości. Ogólnie w usługach publicznych tworzy się tzw. „labirynt" zagrożeń związanych z prywatnością. Stąd szczególnego znaczenia w trosce o zachowanie ciągłości działania organizacji nabierają zalecenia podnoszenia odporności organizacji w zakresie zapewniania bezpieczeństwa infrastruktury i urządzeń z nią powiązanych już na etapie powstawania bazy danych, wdrożenia odpowiednich metod i środków odpornych na ataki, w szczególności uniemożliwiających kradzież czy uszkodzenie danych, a także codzienna dbałość o ochronę danych i ich prywatność poprzez przetwarzanie zgodnie z przepisami, w ramach ściśle określonych celów [por. Skoczylas, 2023].

4. Atrybuty i kryteria ciągłości działania

Ciągłość działania jest kategorią systemową eksponującą prawo każdego systemu do zachowania zdolności funkcjonowania w zmieniających się warunkach [zob. Zaskórski i in., 2020, s. 14641 i nast.]. Zapewnianie i utrzymanie biznesowej ciągłości działania jest ważnym atrybutem cyberbezpieczeństwa. Przyjmuje się, że ciągłość działania może być traktowana w perspektywie zarówno strategicznej, jak i operacyjnej – jako zdolność organizacji do zaplanowania sposobu reagowania na różnego typu incydenty oraz zakłócenia w realizacji procesów biznesowych w celu zapewnienia nieprzerwanej działalności na akceptowalnym poziomie z założeniem możliwości przywracania potrzebnego potencjału (rezyliencji) i ograniczania strat w przypadku materializacji zaistniałych zagrożeń [Białas, 2013, s. 52]. Dość często mówi się o ciągłości działania jako o postulatywnym stanie odporności organizacji na zakłócenia [Maderak, 2018, s. 9]. Godną uwagi jest kategoria odporności systemu (organizacji) na zakłócenia (np. awarie w systemie produkcyjnym lub logistycznym przedsiębiorstwa), co będzie przedmiotem dalszych rozważań. Ciągłość działania można postrzegać także jako strategię zapewniającą możliwość przywrócenia zdolności wznowienia i kontynuacji działalności w przypadku wystąpienia zakłócenia w wyznaczonych ramach czasowych (tzw. RTO, ang. *recovery time objective*). Ważną w tym zakresie procedurą jest wznowienie (w ustalonym czasie RTO) działań zgodnie z planami zapewniania ciągłości działania (BCP, ang. *business continuity plan*), w których definiowane są zadania według różnych scenariuszy biznesowych z uwzględnieniem przedsięwzięć krytycznych [Malon Group, 2024]. Warto w tym miejscu postrzegać ciągłość działania jako „obiekt" zarządzania w organizacji związany z zapewnianiem utrzymania odpowiednich resursów gwarantujących ciągłość biznesu na założonym poziomie. Perspektywa cyberbezpieczeństwa wskazuje tu na potrzebę dostęp-

ności zasobów techniczno-technologicznych i informacyjnych (infrastruktura, sieć, systemy, oprogramowanie, dane) wspierających realizację i skuteczne zarządzanie krytycznymi procesami [Serwis Rzeczypospolitej Polskiej, 2024].

We współczesnej zglobalizowanej rzeczywistości warto też akcentować zwinność i elastyczność operacyjną współczesnych organizacji będących często partycypantami innych podmiotów współdziałających w realizacji wspólnego łańcucha wartości. Stąd biznesową ciągłość działania należy postrzegać jako swoistą procedurę zapewniania (w trybie dynamicznej rekonstrukcji procesów biznesowych i informacyjnych, np. metodą doraźnego *outsourcingu*) minimalnego, niezbędnego poziomu operacyjnego działania nawet w warunkach materializacji krytycznych zagrożeń lub ewentualnych zakłóceń wewnętrznych i zewnętrznych. Pewnym uogólnieniem interpretacyjnym jest BCM, rozumiany jako proces zarządzania biznesową ciągłością działania, który doczekał się standaryzacji i procedur opracowywania strategii, planów i działań, które sprzyjać mają ochronie lub alternatywnym sposobom działania dla tych przedsięwzięć biznesowych, które w przypadku ich skutecznego zakłócenia lub wręcz przerwania mogłyby implikować nieakceptowalny poziom szkód/strat [Bronson, MacDonald, 2014]. Warto tu zaznaczyć, że zachowanie biznesowej ciągłości działania wiąże się z opracowaniem planu awaryjnego organizacji dla sytuacji zagrożenia. Zasadne jest zatem określenie specyfikacji zasobów, które mają być objęte procedurą planowania z jednoczesnym ustaleniem granicy tolerancji dla ich dopuszczalnego poziomu. Stąd BCM powinno być traktowane jako zdolność organizacji do realizacji podstawowych przedsięwzięć biznesowych na wyznaczonym poziomie jakości z przerwami uznanymi za strategicznie lub operacyjnie dopuszczalne [Liderman, 2017, s. 239]. Realizację podstawowych zadań biznesowych należy utożsamiać z celami organizacji zgodnie z wyznaczonym poziomem jakości w ustalonym czasie (z przerwami nie dłuższymi niż dopuszczalne) według wyników analizy ryzyka. Należy przy tym pamiętać, że BCM wymaga odpowiednich zasobów informacyjnych. Stąd BCM jest determinowane poziomem zasobów informacyjnych i informacyjną ciągłością działania.

Jak wcześniej wspomniano, informacyjna ciągłość działania (ICD) związana jest ściśle z kryterium cyberbezpieczeństwa, obejmującego bezpieczeństwo zasobów informacyjnych i skuteczne zarządzanie organizacją w różnych warunkach. Zasoby informacyjne we współczesnej organizacji stanowią wartość chronioną z wielu powodów – zarówno formalnych, jak i merytorycznych, a w szczególności biznesowych, co przekłada się na utrzymanie ciągłości działania całej organizacji. Oznaczać to może potrzebę uruchamiania alternatywnych procesów według planu awaryjnego dostępu do innych zasobów i wykorzystania informacji. Należy tu wspomnieć, że pomimo rangi, jaką ma ICD w organizacji, dość często ekspozycja tego elementu biznesowego jest słabiej zauważalna. Mimo to ICD traktowana być powinna jako zdolność organizacji do reagowania na zagrożenia mające wpływ na przepływy rzetelnej i aktualnej informacji, aby tam, gdzie to możliwe, szybko przywrócić normalne warunki działania, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczej obsługi informacyjnej realizowanych zadań. ICD jest zatem zdolnością podmiotu do realizacji celów i zadań w warunkach zakłóconego operowania zasobami informacyjnymi

z uwzględnieniem alternatywnych procesów, które mogą zostać wdrożone w sytuacjach kryzysowych przy użyciu sił i środków w czasie niepowodującym obniżenia efektywności danego podmiotu. Z punktu widzenia ICD zasadne jest to, aby wszelkie działania mające na celu przywrócenie normalnego stanu organizacji nie powodowały zaburzenia relacji: „zakres działania – koszt (zasoby) – czas". Z tego samego powodu należy przyjąć za słuszne, że nie każde działanie „naprawcze" jest możliwe do wdrożenia, ponieważ zbyt duże odstępstwa w którymś elemencie ww. relacji mogą przełożyć się na utratę płynności finansowej lub pogorszą pozycję rynkową organizacji.

Ponadto, zasoby informacyjne mają szczególny charakter i powinny być bezpośrednio związane także z innymi wymiarami ciągłości działania, jak wymiar ekonomiczny, społeczno-kulturowy, organizacyjno-kadrowy, logistyczny (zasobowy, technologiczny, techniczny).

5. Wzmacnianie odporności organizacji na ryzyko naruszenia ciągłości działania z wykorzystaniem wybranych platform IT/ICT

Wzmacnianie odporności organizacji na ryzyko naruszenia ciągłości działania jest systemowym wymaganiem dla menedżerów. Wykorzystywanie do tego celu platform IT/ICT zgodnie z przyjętą strategią informacyjną powinno być priorytetem dla każdej współczesnej organizacji. Wiąże się to przede wszystkim z ograniczaniem różnego typu dysfunkcji w dostępie do zasobów i w przepływach informacyjnych. Dążyć bowiem należy do wzmacniania ciągłości działania w aspekcie zarówno pracowników, jak i utrzymania potencjału biznesowego całej organizacji. Stąd też niewiedza i nieadekwatność posiadanych sił i środków do realizacji założonych zadań może oznaczać wystąpienie sytuacji kryzysowej, co wyzwala naturalną potrzebę i konieczność technicznego lub organizacyjnego wsparcia. Często presja czasu w sytuacjach kryzysowych potęguje konieczność reagowania w czasie rzeczywistym przy dużej zmienności tzw. „warunków brzegowych". Świadomość, że czas jest zasobem nieodtwarzalnym, kieruje do konstatacji, że jego deficytu nie da się uzupełnić, a tym bardziej zniwelować. Zjawisko „zaskoczenia" wynikające z ograniczonych możliwości prognozowania zmian w przypadku braku lub niedostatecznego dostępu do niezbędnej informacji przy dużej dynamice zdarzeń – może implikować lawinowy wzrost poziomu ryzyka utraty ciągłości działania. Może to się wiązać ze wzrostem popytu na informację spełniającą określone wymagania jakościowe. Należy też zauważyć, że niewystarczalność lub nieadekwatność posiadanych środków/zasobów wraz z brakiem rzetelnej informacji o stanie posiadania powoduje ryzyko nieskutecznych decyzji dotyczących m.in. procesów logistycznych oraz racjonalnego dysponowania dostępnymi siłami i środkami. Dostęp do konkretnej, aktualnej, dedykowanej informacji może być istotny dla skrócenia cyklu decyzyjnego w warunkach dużej dynamiki i niepewności/nieprzewidywalności zdarzeń. Budowanie pożądanego poziomu odporności na ryzyko zerwania ciągłości działania wymaga świadomości wystą-

pienia zagrożeń i realnej oceny możliwości sterowania sytuacją kryzysową, co wymaga skutecznych działań predykcyjnych.

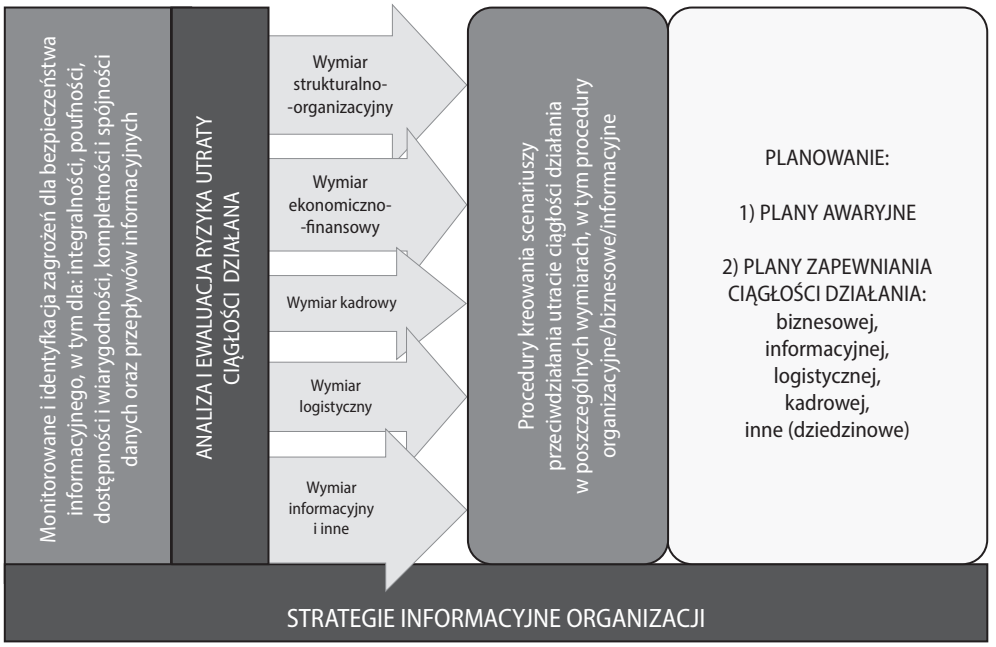
Dysponowanie zasobami danych w różnej postaci zarówno o sytuacji bieżącej, jak i różnego typu trendach i wynikach analiz oraz ocen biznesowych może skuteczniej wspierać zarządzanie ryzykiem utraty bezpieczeństwa i ciągłości działania w zależności od zaistniałych incydentów. W takich działaniach można posiłkować się tworzeniem scenariuszy możliwych zdarzeń poprzez opis rozwoju sytuacji w otoczeniu oraz opracowaniem projektu skutecznej reakcji organizacji. Wykorzystanie zasad analogii w podejmowaniu decyzji strategicznych umożliwia uwzględnianie zależności między czynnikami zewnętrznymi i wewnętrznymi wpływającymi na poziom przedmiotowego ryzyka. W przypadku ograniczonej i niepewnej informacji ważne mogą być modele symulacyjne bazujące często na trendach rozwoju podobnej sytuacji w przeszłości w firmie lub w podobnych podmiotach. Opracowywanie scenariuszy symulacyjnych odnosi się często do konkretnego problemu, dla którego ustala się listę istotnych czynników w otoczeniu, mających wpływ na działalność organizacji. Każdemu czynnikowi należy przy tym przypisać określoną rangę, zakres czasowy i obszar występowania. Konstruowanie takich scenariuszy odbywa się na podstawie testowania modelu zachowania organizacji, „symulującego" wzajemne zależności pomiędzy czynnikami opisującymi określone sytuacje krytyczne. Nie bez znaczenia dla kreowania odporności organizacji na ryzyko utraty ciągłości działania jest opracowanie scenariuszy stanów otoczenia. Podstawą ocen i oszacowań jest głównie wiedza analityczna zawarta np. w systemach klasy OLAP lub *big data*, a także wiedza ekspertów i twórców scenariuszy. Tej klasy scenariusze powinny być opracowane w wielu wariantach implikowanych różnymi rodzajami zagrożeń, a ponadto w wersji: optymistycznej, pesymistycznej, niespodziankowej oraz najbardziej prawdopodobnej.

Emanacją tych wszystkich założeń oraz wskazań jest opracowanie i przestrzeganie procedury przeciwdziałania ryzyku utraty ciągłości działania (rysunek 2) poprzez wskazanie podmiotu, w którym procedura ma funkcjonować oraz: (1) określenie identyfikatora procedury i celu procedury oraz wskazanie oczekiwanych efektów, (2) sprecyzowanie zakresu jej działania oraz określenie osób (stanowisk) odpowiedzialnych za działania objęte procedurą, (3) wskazanie głównych wykonawców oraz sposobu postępowania w sytuacji, której dotyczy procedura, (4) określenie podmiotów współpracujących (wewnętrznych i zewnętrznych), (5) określenie sposobu komunikowania się oraz wskazanie niezbędnych technicznych środków komunikacji, (6) dokumentowanie działań i wskazanie dokumentów wyższego rzędu, będących podstawą prawną opracowanej procedury, (7) wskazanie głównych zagrożeń spotykanych w trakcie realizowania procedury.

Jak wcześniej wspomniano, ciągłość działania może być postrzegana w wielu wymiarach, takich jak np. wymiar: ekonomiczno-finansowy, organizacyjno-strukturalny i personalny (w tym kompetencje i struktury organizacyjne podmiotu), a także logistyczny, społeczno-kulturowy oraz informacyjny. Odporność na ryzyko utraty ciągłości działania jest niejako „zobrazowaniem" możliwości przeciwdziałania temu ryzyku we wskazanych wyżej wymiarach. Wymiar ekonomiczno-finansowy jest dla zachowania ciągłości działania podstawowym

atrybutem wzmacniania odporności na ryzyko jej utraty poprzez kształtowanie poziomu kapitału finansowego z założeniem ograniczania marnotrawstwa i podatności na zakłócenia generujące sytuacje krytyczne. Wymiar organizacyjno-strukturalny to dążenie do elastyczności struktur, ekspozycja struktur procesowych/sieciowych i elastyczny, ale właściwy dobór kompetencji pracowniczych do zadań organizacji w każdym procesie. Zasoby ludzkie należy postrzegać przez pryzmat świadomości i celowości działań własnych na tle potrzeb organizacji z akcentem na racjonalność procesu decyzyjnego oraz niezawodność, trwałość i zdolność spełniania wymagań m.in. strategii informacyjnych i narzędzi IT/ICT w działaniu jako komponentu strategii biznesowej. Odporność na ryzyko w tym obszarze może być implikowana jakością zasobów kadrowych i instrumentami zapewniania kompetencji, a w tym: (1) ustaleniem ram kompetencyjnych dla stanowisk pracy, (2) adekwatnością kompetencji do złożoności zadaniowej, (3) procesem planowania zatrudnienia, który powinien bazować na precyzyjnym określeniu kompetencji na poszczególnych stanowiskach, (4) sposobem (algorytmami) weryfikacji poziomów kompetencji pracowników, (5) cykliczną oceną poziomu przyswojenia kompetencji przez pracowników, (6) metodami wykorzystywanymi do minimalizacji ryzyka związanego z tzw. luką kompetencyjną.

Rysunek 2. Procesy wzmacniania odporności na utratę ciągłości działania organizacji



Źródło: opracowanie własne.

Logistyczna ciągłość działania związana jest ze skutecznym i efektywnym zarządzaniem gospodarką materiałową/zamówieniami i dostawami, serwisem i eksploatacją oraz remontami, a także z transportem wewnętrznym i zewnętrznym oraz infrastrukturą. Zasoby rze-

czowe można postrzegać jako różnego typu nieruchomości, urządzenia techniczne, maszyny, surowce i materiały. Podstawową strategią wzmacniania odporności systemu na zakłócenia w systemie logistycznym jest redundancja jego newralgicznych elementów. Tak więc podstawowymi czynnikami skutecznego zarządzania ciągłością logistyczną jest traktowanie zapasów jako majątku obrotowego organizacji. Nadrzędnym bowiem celem utrzymywania zapasów w każdej organizacji jest zapewnienie prawidłowego przebiegu procesów podstawowych (np. projektowania, produkcji, sprzedaży itp.). Zapasy są składnikami aktywów przedsiębiorstwa w postaci materiałów, produkcji w toku lub wyrobów gotowych, które mają na celu zapewnienie ciągłości poszczególnych procesów. Ciągłość ta może wynikać z trafnego określenia zaopatrzenia materiałowego na podstawie prognoz popytu i faktycznych potrzeb rynkowych oraz z utrzymania materiałów na dobrym poziomie jakościowym i ze stałego identyfikowania aktualnych stanów. Planowanie potrzeb materiałowych w procesach wytwórczych/projektowych powinno zapewniać odporność na materializację ryzyka utraty ciągłości działania poprzez poszukiwanie alternatywnych rozwiązań z zachowaniem kryterium minimalizacji kosztów oraz kontrolę realizacji (np. procedura planistyczna bazująca na optymalizacji wielkości partii dostaw).

Wymienione wyżej wymiary są ze sobą powiązane. Jak wcześniej sygnalizowano, zachowanie informacyjnej ciągłości działania warunkuje inne wymiary ciągłości działania. Poszczególne strategie informacyjne dość precyzyjnie identyfikują obszar i zakres przydatności określonych typów narzędzi IT/ICT. Przestrzeganie tych zaleceń jest wskazaniem kierunków wzmacniania odporności organizacji na incydenty naruszające informacyjną ciągłość działania w każdej z trzech warstw:

1. W warstwie gospodarki danymi i ich organizacji ważne są mechanizmy zapewniania poufności, wiarygodności i integralności danych. W systemach wspomagania zarządzania eksponuje się modele zapewniania poufności danych różnymi metodami, w tym metodami szyfrowania. W systemach klasy BI (ang. *business intelligence*) stosuje się organizacje wielowymiarowe w postaci hurtowni danych, gdzie możliwe są do wykorzystania silne modele selekcjonowanego dostępu do wybranych partii danych zagregowanych. Szczególną kategorią narzędzi są usługi w chmurze obliczeniowej, gdzie gospodarka danymi i ich organizacja odbywają się na zasadzie usług objętych specjalną umową biznesową z silnymi warunkami zapewniania bezpieczeństwa informacyjnego użytkownikowi końcowemu. W strategii wykorzystania systemów *big data* można dążyć do podobnych poziomów wzmacniania odporności na ryzyko zerwania informacyjnej ciągłości działania. Eksploracja dużych zasobów wielopostaciowych danych przy wykorzystaniu sztucznej inteligencji (szczególnie modeli bazujących na sieciach neuronowych) może mieć dużą wartość biznesową generowanej wiedzy. Każda strategia informacyjna niesie ze sobą określone efekty w odniesieniu do nakładów ponoszonych na eksploatację związanych z nimi narzędzi. Im wyższy poziom zaawansowania technologicznego narzędzi, tym proporcjonalnie wyższy koszt, ale wartość analiz, ocen i prognoz staje się

też wyższa. Stąd w wymiarze biznesowym można uznać, że efektywność i użyteczność tych strategii informacyjnych rośnie.

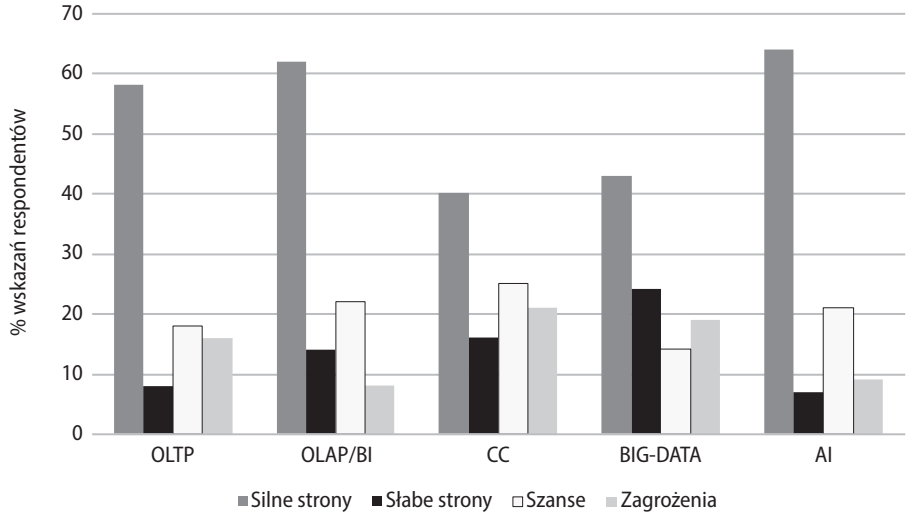
2. W warstwie przepływów informacyjnych należy uznać, że dobrze zaprojektowana infrastruktura sieciowa zapewnia szybką i niezawodną komunikację oraz elastyczne dostosowanie do zmieniających się potrzeb biznesowych przy jednoczesnej dbałości o bezpieczeństwo danych oraz systemów ich gromadzenia i utrzymywania [por. Szafrański, 2024]. Efektywne struktury sieciowe są kluczowe dla organizacji, które chcą skutecznie wdrażać strategie informatyzacji z wykorzystaniem m.in. Internetu rzeczy. Zastosowania efektywnych struktur sieciowych w różnych sektorach, np. w procesach produkcyjnych, umożliwia monitorowanie pracy maszyn oraz integrację urządzeń IoT z systemami zarządzania produkcją. Dzięki temu można w czasie rzeczywistym wykrywać potencjalne awarie i zminimalizować przestoje.
3. W warstwie biznesowej strategii informacyjnych warto zauważyć, że dzięki zintegrowanym sieciom organizacje mogą automatyzować procesy produkcyjne, co sprzyja redukcji kosztów. W obszarze logistyki produkcji i łańcucha dostaw struktury sieciowe umożliwiają śledzenie ruchu towarów, pojazdów i zasobów w czasie rzeczywistym. Pozwala to na optymalizację tras i lepsze zarządzanie zapasami. Ponadto, dzięki sensorom IoT w połączeniu z sieciami organizacje mogą monitorować warunki przewozu, takie jak temperatura czy wilgotność, co jest kluczowe dla utrzymania jakości produktów. W procesach sprzedaży tzw. „inteligentne półki" wyposażone w technologie IoT i połączone w modelu sieciowym pozwalają monitorować poziom zapasów i automatyzować zamówienia. Możliwa jest również analiza zachowania klientów i śledzenie ich ruchu w sklepie, co pomaga w zrozumieniu ich zachowań i personalizacji oferty. Dodatkowo, zintegrowane sieci umożliwiają automatyczne dostosowywanie stanu różnego typu urządzeń w zależności od bieżących warunków lub potrzeb z uwzględnieniem kryterium czasu i kosztów.

Ważnym aspektem zapewniania ciągłości działania organizacji są struktury procesowe (płaskie), które implikują zwiększoną elastyczność (zwinność) współczesnej organizacji. Strategie informacyjne mają dominujący wpływ na wdrażanie tego typu struktur z możliwością pracy wielu rozproszonych podmiotów na wspólnym repozytorium danych z ustalonymi prawami dostępu. Różnorodne błędy we wdrażaniu organizacji procesowych i generowanie nowych zagrożeń dla odporności organizacji na ryzyko zerwania ciągłości działania związane były często z brakiem równowagi między pożądaną szczegółowością a nadmierną redundancją informacyjną w procesach decyzyjnych, nieaktualnością, a dość często z niedostępnością planów awaryjnych, w tym brakiem alternatywnych możliwości działania z wykorzystaniem np. danych prognostycznych.

Wyniki badań empirycznych [Staruch, 2024] wskazują na dominację silnych stron (rysunek 3), a wywiady eksperckie (rysunek 4) – na wysoce pozytywną ocenę przydatności proponowanych strategii. Koncepcje poszukiwania odporności na ryzyko utraty ciągłości działania wiążą się z identyfikacją procesów wrażliwych o znaczącej wartości dla organizacji (*reengineering*), poszukiwaniem wzorców zachowania organizacji (*benchmarking*) lub z realizacją

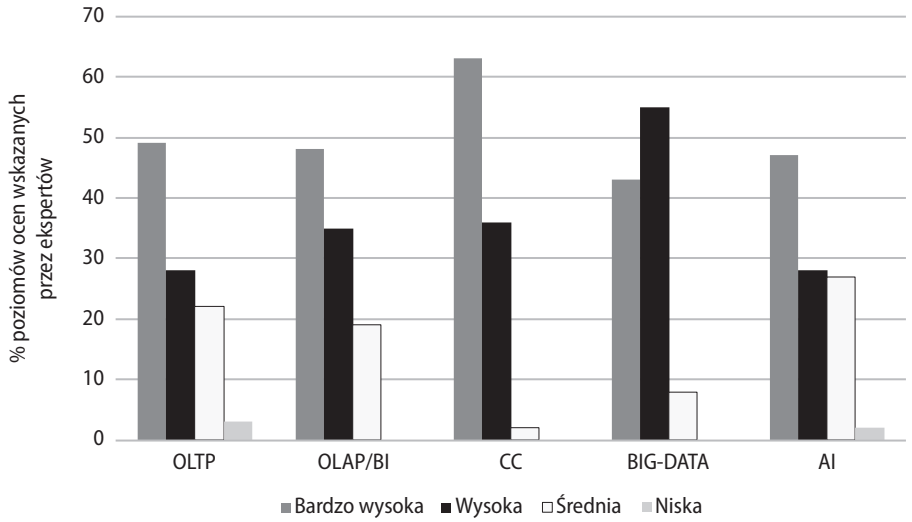
outsourcingu. Koncepcje te stanowią uproszczoną wersję działania. Stąd koncepcja organizacji procesowej, inteligentnej („uczącej się"), bazującej na dostępie do odpowiednich zasobów danych i informacji z możliwością generowania wiedzy wzmacniającej jej potencjał biznesowy i zdolności przeciwdziałania ryzyku zerwania informacyjnej ciągłości działania, wydaje się dobrą strategią.

Rysunek 3. Wyniki uogólnionej analizy w grupach skumulowanych atrybutów strategii informacyjnych w układzie modelu SWOT (*N* = 112 osób)



Źródło: opracowanie własne na podstawie Staruch [2024, s. 161–223].

Rysunek 4. Uogólnione wyniki analizy czynnikowej w grupach skumulowanych ocen w 4-stopniowej skali oceny poziomów przydatności strategii informacyjnych we wzmacnianiu odporności organizacji według grupy ekspertów (*N* = 7)



Źródło: opracowanie własne na podstawie Staruch [2024, s. 299–341].

6. Podsumowanie

Holistyczne ujęcie zarządzania ciągłością działania [Xing i in., 2019, s. 1–28] i jej uwarunkowania systemowe wiążą się z zapewnianiem bezpieczeństwa każdego systemu. Identyfikacja źródeł i charakteru zakłóceń dla ciągłości działania i konsekwencji incydentów bezpieczeństwa oraz ich przyczyn sprzyja wartościowaniu poziomu zakłóceń i obiektywizacji ocen. Zarządzanie ciągłością działania, a w tym: procesy planowania, organizowania zasobów oraz monitorowania i ewidencjonowania incydentów, powinny być zsynchronizowane z procesami kontroli i audytów. Metody oceny ryzyka na potrzeby zapewniania ciągłości działania i kształtowania pożądanego poziomu świadomości sytuacyjnej [por. Endsley, 2015, s. 101–111; McKay, McKay, 2015], a w tym określenie (wybór) strategii informacyjnej zapewniania ciągłości działania oraz ocena jej wpływu na działalność i przywracanie zdolności działania organizacji po incydencie, stanowią kluczowe wartości każdej organizacji. Integracja procesów zapewniania ciągłości działania w ujęciu holistycznym, w tym płaszczyzny integracji zasobów informacyjnych i wyboru strategii zapewniania ciągłości działania, powinna bazować na scenariuszach rozwoju sytuacji w warunkach zakłóceń, awarii systemów technicznych, czy zakłóceń dostaw itp. Ponadto, strategie i metody zapewniania ciągłości działania w wielowymiarowej perspektywie wymagają zgodności ze standardami i normami zapewniania ciągłości działania w aspekcie norm techniczno-technologicznych i materiałowo-sprzętowych, standardów procesów logistycznych i strukturalno-organizacyjnych.

Podsumowując, można przyjąć, że szerokie wykorzystanie środowiska IT/ICT odgrywa kluczową rolę w transformacji współczesnych organizacji, a implementacja różnych platform i narzędzi zwiększa ich odporność na ryzyko utraty biznesowej ciągłości działania.

Zasadniczym ograniczeniem badawczym jest zastosowanie głównie metody narracyjnego przeglądu literatury przedmiotu i jedynie uzupełnienie jej metodą *desk research* – aby zaznaczyć swoistą egzemplifikację analiz literaturowych w zakresie stosowania i przydatności poszczególnych technologii teleinformatycznych. Artykuł ma ograniczoną podbudowę empiryczną, jednak warto wyraźnie zaznaczyć, że jego zasadniczym celem było potwierdzenie, że szerokie wykorzystanie środowiska IT odgrywa kluczową rolę w transformacji współczesnych organizacji, a implementacja różnych platform i narzędzi zwiększa ich odporność na ryzyko utraty biznesowej ciągłości działania. W takim przypadku metoda narracyjnego przeglądu literatury przedmiotu może być uznana za wystarczającą.

W związku z powyższym dalsze badania we wskazanym przedmiocie analiz mogą bazować na metodach empirycznych (np. sondaż diagnostyczny z wykorzystaniem metody CAWI, ang. *computer-assisted web interview*), przede wszystkim w zakresie identyfikacji technologii teleinformatycznych, które w opinii respondentów (np. menedżerów i właścicieli przedsiębiorstw z najbardziej innowacyjnych sektorów w Polsce) mają potencjalnie największy wpływ na zapewnianie i utrzymanie ciągłości procesów biznesowych i zarządczych.

Bibliografia

Dokumenty prawne

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.
2. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. 2002, nr 117, poz. 985.

Wydawnictwa zwarte

1. BS 25999–1:2006(2006). *Business continuity management. Part 1: Code of practice*. London.
2. Chowdhury, N. (2018). *Factors Influencing the Adoption of Cloud Computing Driven by Big Data Technology. A Quantitative Study*, Ph.D. Thesis. Minneapolis: Capella University.
3. Gilchrist, A. (2016). *Industry 4.0. The Industrial Internet of Things*. New York: Apress.
4. Gogołek, W., Cetera, W. (2014). *Leksykon tematyczny. Zarządzanie, IT*. Warszawa: Wydawnictwo Wydziału Dziennikarstwa i Nauk Politycznych UW.
5. Goodfellow, I., Bengio, Y., Courville, A. (2016). *Deep Learning*. Cambridge: MIT Press.
6. Januszewski, A. (2008a). *Funkcjonalność informatycznych systemów zarządzania. T.1. Zintegrowane systemy transakcyjne*. Warszawa: PWN.
7. Januszewski, A. (2008b). *Funkcjonalność informatycznych systemów zarządzania. T.2. Systemy Business Intelligence*. Warszawa: PWN.
8. Liderman, K. (2017). *Bezpieczeństwo informacyjne. Nowe wyzwania*. Warszawa: PWN.
9. Liderman, K. (2023). *O istocie cyberprzestrzeni*. Warszawa: Instytut Teleinformatyki i Cyberbezpieczeństwa WAT.
10. Maderak, K. (2018). *Zapewnienie ciągłości działania*. Warszawa: Departament Funduszy Inwestycyjnych i Funduszy Emerytalnych.
11. Mateos, A., Rosenberg, J. (2011). *The Cloud at Your Service. The when, how, and why of enterprise cloud computing*. New York: Manning Publications.
12. Mayer-Schonenberger, V., Cukier, K. (2014). *Big Data: A Revolution That Will Transform How We Live, Work*. Boston: Mariner Books.
13. Miller, M. (2016). *Internet Rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*. Warszawa: PWN.
14. Skoczylas, D. (2023). *Krajowy System Cyberbezpieczeństwa*. C.H. Beck: Warszawa.
15. Staruch, M. (2024). *Kształtowanie świadomości sytuacyjnej w systemach zarządzania kryzysowego z wykorzystaniem wybranych platform IT*, rozprawa doktorska napisana pod kierunkiem prof. dr. hab. inż. P. Zaskórskiego i dr. J. Woźniaka. Warszawa: Wojskowa Akademia Techniczna.
16. Szafrański, B. (red.) (2024). *Cyberbezpieczeństwo vs. sztuczna inteligencja: prawo, informatyka, zarządzanie*. Warszawa: Wojskowa Akademia Techniczna.
17. Tapscott, D., Tapscott, A. (2019). *Blockchain rewolucja*. Warszawa: PWN.
18. Woźniak, J., Zaskórski, P. (2018). *Projektowanie organizacji procesowej. Perspektywa systemów analityczno-decyzyjnych*. Warszawa: Wojskowa Akademia Techniczna.
19. Zaskórski, P. (2012). *Asymetria informacyjna w zarządzaniu procesami*. Warszawa: Wojskowa Akademia Techniczna.

20. Zaskórski, P. (red.) (2011). *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*. Warszawa: Wojskowa Akademia Techniczna.
21. Zaskórski, P., Zaskórski, W., Woźniak, J. (2021). *Świadomość sytuacyjna a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*. Warszawa: CeDeWu.

Artykuły naukowe

1. Białas, A. (2013). Zarządzanie ciągłością działania oraz bezpieczeństwem informacji i innych zasobów w górnictwie, *Mechanizacja i Automatyzacja Górnictwa*, 8(51), s. 50–64.
2. Endsley, M.R. (2015). Final reflections: Situation awareness models and measures, *Journal of Cognitive Engineering and Decision Making*, 9(1), s. 101–111.
3. Marczyk, M. (2018). Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, *Przegląd Teleinformatyczny*, 1–2(46), s. 59–72.
4. Sienkiewicz, P. (2015). Ontologia cyberprzestrzeni, *Zeszyty Naukowe. Warszawska Wyższa Szkoła Informatyki*, 13(9), s. 89–102.
5. Świątkowski, A.M. (2021). Warunki rozwoju i wpływ sztucznej inteligencji na pracę, zatrudnienie i inne niektóre prawnie nieuregulowane w Unii Europejskiej. Zagadnienia społeczne, technologiczne i gospodarcze, *Roczniki Administracji i Prawa*, XXI, 113–127.
6. Xing, J., Zeng, Z., Zio, E. (2019). Dynamic business continuity assessment using condition monitoring data, *International Journal of Disaster Risk Reduction*, 41, s. 1–28. DOI: 10.1016/j.ijdrr.2019.101334.
7. Zaskórski, P., Woźniak, J. (2023). Wirtualizacja współczesnych organizacji w aspekcie synergii potencjałów biznesowych, *International Journal of New Economics and Social Sciences*, 8(24), s. 45–60. DOI: 10.5604/01.3001.0054.5139.
8. Zaskórski, P., Woźniak, J., Zaskórski, W. (2020). Informational Continuity of Operations in the Context of Safety and Security Research in Contemporary Organizations, *International Business Information Management – IBIMA 2020 Conference*, 1–2.04.2020, Seville, Spain, s. 14641–14653.

Materiały internetowe

1. BBN (2023). https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (dostęp: 20.06.2023).
2. Bronson, J., MacDonald, T. (2014). *Business Continuity and Disaster Recovery. Trends, Considerations & Leading Practices*, https://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/11-13-14-audit/business-continuity.pdf (dostęp: 17.03.2024).
3. Encyklopedia Zarządzania (2024). https://mfiles.pl/pl/index.php/Cyberbezpiecze%C5%84stwo (dostęp: 19.05.2024).
4. ERP24.pl (2022). https://www.erp24.pl/rynek-it-swiat/5-kluczowych-systemow-big-data-na-swiecie.html (dostęp: 21.09.2022).
5. Hackeru.pl (2021). https://hackeru.pl/cyberbezpieczenstwo-dla-poczatkujacych (dostęp: 11.04.2024).

6. Joint Publication 1–02(2010). Department of Defense Dictionary of Military and Associated Terms, https://irp.fas.org/doddir/dod/jp1_02.pdf (dostęp: 09.06.2024).
7. Malon Group (2024). https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/zarzadzanie-ryzykiem/bs-25999/ proces-wdrazania-bcms/ (dostęp: 15.02.2024).
8. McKay, B., McKay, K. (2015). https://www.artofmanliness.com/articles/how-to-develop-the-situational-awareness-of-jason-bourne (dostęp: 17.01.2024).
9. Ministerstwo Klimatu i Środowiska (2024). https://www.gov.pl/web/klimat/wspolpraca-krajowa (dostęp: 21.01.2024).
10. NIST SP 800-53 Rev. 5(2020). https://csrc.nist.gov/pubs/sp/800/53/r5/final (dostęp: 17.02.2024).
11. Serwis Rzeczypospolitej Polskiej (2024). https://www.gov.pl/web/baza-wiedzy/zapewnienie-ciaglosci-dzialania (dostęp: 10.05.2024).
12. UKSW (2024). https://uksw.edu.pl/images/artykuly/uniwersytet/RODO/Ryzyko-w-ochronie-danych-osobowych-AK-29.01.2018.pdf (dostęp: 01.02.2024).
13. Websecurity.pl (2022). http://websecurity.pl/tag/historia-chmury/ (dostęp: 10.10.2022).

Information Efficiency and Resilience to the Risk of Losing the Continuity of the Contemporary Organization's Operations

Abstract

The article holistically addresses the problem of counteracting the risk of losing the continuity of contemporary organizations in a rapidly changing environment. The environment of systems and modern ICT platforms, along with the use of cyberspace services, determines the information efficiency of organizations. The authors cite several strategies based on systems of various classes, such as domain systems, integrated management information systems (OLTP and OLAP classes), and *big data* solutions, which ensure knowledge generation, significantly strengthen the organization's potential, and ensure business continuity. They also refer to cloud computing services that eliminate the information exclusion of small business entities. The aim of the study is to confirm that the wide use of the IT/ICT environment plays a crucial role in the transformation of modern companies and that the implementation of various platforms and tools increases the organization's resilience to the risk of losing business continuity. In implementing the research processes, an analysis of the literature (using the narrative review method), as well as a desk research analysis were conducted to assess the degree of usefulness of IT/ICT tools in creating business continuity. Synthesis and reduction methods were also used. The authors emphasize that IT/ICT tools, including selected artificial intelligence models, have significant implications for management theory and practice.

Keywords: information, system, IT/ICT technologies, risk, business continuity