

Nowoczesne Systemy Zarządzania
Zeszyt 20 (2025), nr 1 (styczeń-marzec)
ISSN 1896-9380, s. 15-32
DOI: 10.37055/nsz/207072

Modern Management Systems
Volume 20 (2025), No. 1 (January-March)
ISSN 1896-9380, pp. 15-32
DOI: 10.37055/nsz/207072

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Zasoby informacyjne i ich eksploracja w cyberprzestrzeni jako komponent potencjału biznesowego współczesnych organizacji

Information resources and their exploration in cyberspace as a component of the business potential of modern organizations

Sebastian Łukasik

Wojskowa Akademia Techniczna, Warszawa, Polska
sebastian.lukasik@wat.edu.pl; ORCID: 0009-0009-3787-9403

Piotr Zaskórski

Wojskowa Akademia Techniczna, Warszawa, Polska
piotr.zaskorski@wat.edu.pl; ORCID: 0000-0002-2598-1859

Abstrakt:

Cel badań i hipotezy/pytania badawcze

Celem badań było określenie roli zasobów informacyjnych w budowaniu potencjału biznesowego współczesnych organizacji, analizując, jak ich eksploracja w cyberprzestrzeni wpływa na doskonalenie procesów biznesowych i podejmowanie decyzji. Całość opracowania jest profilowana hipotezą, że zasoby informacyjne i ich eksploracja determinują wzrost potencjału biznesowego współczesnych przedsiębiorstw.

Metody badawcze

Do weryfikacji sformułowanej hipotezy wykorzystano metody badawcze związane z krytyczną analizą piśmiennictwa naukowego, raportów branżowych oraz innych źródeł związanych z tematyką badawczą, a także własne badania cząstkowe typu sondaże diagnostyczne według przedmiotowego profilu potrzeb.

Główne wyniki

Potwierdzenie hipotezy, że zasoby informacyjne i ich eksploracja determinują wzrost potencjału biznesowego współczesnych przedsiębiorstw.

Implikacje dla teorii i praktyki

Eksploracja danych w cyberprzestrzeni, wspierana przez rozwój technologii sztucznej inteligencji, umożliwia firmom nie tylko optymalizację procesów biznesowych, lecz również wprowadzanie innowacyjnych modeli operacyjnych.

Słowa kluczowe: zasoby informacyjne, cyberprzestrzeń, sztuczna inteligencja, cyberbezpieczeństwo, analityka biznesowa

Abstract:**Research objectives and hypothesis/research questions**

The purpose of the research was to determine the role of information resources in building the business potential of modern organizations, analyzing how their exploration in cyberspace affects the improvement of business processes and decision-making. The entire study is profiled with the hypothesis that information resources and their exploration determine the growth of business potential of modern enterprises.

Research methods

To verify the formulated hypothesis, research methods related to critical analysis of scientific literature, industry reports and other sources related to the research topic were used, as well as our own sub-studies like diagnostic surveys according to the needs profile in question.

Main results

Confirmation of the hypothesis that information resources and their exploration determine the growth of business potential of modern enterprises.

Implications for theory and practice

Data mining in cyberspace, supported by the development of artificial intelligence technologies, enables companies not only to optimize business processes, but also to introduce innovative operating models.

Keywords: information resources, cyberspace, artificial intelligence, cybersecurity, business analytics

Wprowadzenie

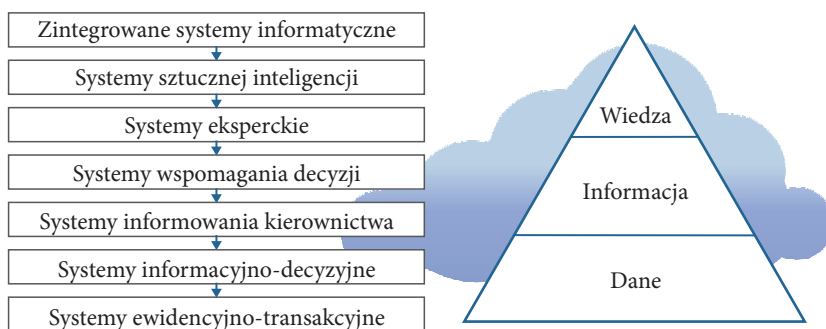
Współczesne organizacje biznesowe działają w dynamicznie zmieniającym się środowisku, w którym informacja stała się jednym z najcenniejszych zasobów. Zdolność do efektywnego gromadzenia, przetwarzania i wykorzystywania danych stanowi kluczowy element budowania przewagi konkurencyjnej. W erze cyfrowej zasoby informacyjne odgrywają fundamentalną rolę w doskonaleniu procesów decyzyjnych, optymalizacji operacyjnej oraz personalizacji usług. Jednocześnie rozwój technologii, takich jak sztuczna inteligencja (AI) oraz eksploracja wielopostaciowych danych (ang. *data mining*), otwierają nowe możliwości analityczne, które przekształcają modele biznesowe i wspierają innowacje. Cyberprzestrzeń staje się naturalnym środowiskiem, w którym organizacje nie tylko prowadzą działalność operacyjną, lecz również eksplorują zasoby informacyjne i nimi zarządzają. W związku z tym rośnie znaczenie zarówno zabezpieczania tych zasobów, jak i efektywnego korzystania z zaawansowanych narzędzi analitycznych. Mimo to pojawiają się, poza wieloma możliwościami, także liczne zagrożenia, takie jak cyberprzestępczość czy nadużycia związane z nieetycznym wykorzystaniem danych i technologii AI. Celem artykułu jest analiza roli zasobów informacyjnych i możliwości ich eksploracji w cyberprzestrzeni jako komponentu potencjału biznesowego współczesnych organizacji. Przedstawione zostaną nie tylko aspekty związane z cyberbezpieczeństwem i zarządzaniem danymi, lecz również perspektywy rozwoju analityki biznesowej bazującej na AI, umożliwiającej optymalizację modeli biznesowych. W publikacji zostaną także omówione szanse i zagrożenia wynikające z wykorzystania sztucznej inteligencji w dostarczaniu usług w cyberprzestrzeni.

1. Istota i rola potencjału informacyjnego współczesnej organizacji biznesowej

W dobie transformacji cyfrowej i zarządzania nowoczesnymi organizacjami, wynikającej z powszechności oraz rozwoju nowoczesnych technologii, istotną rolę odgrywają zasoby informacyjne. Kluczowym aspektem jest ich poprawne zdefiniowanie oraz kategoryzacja i selekcja, co wpływa na skuteczne zarządzanie tym obszarem. Uporządkowanie wspomnianych zasobów dotyczy nie tylko systemów analityczno-decyzyjnych, lecz również wszelkich systemów transakcyjnych wykorzystywanych w organizacji. Zgodnie z literaturą przedmiotu do zasobów informacyjnych organizacji zaliczają się użyteczne dane niezbędne do skutecznego podejmowania decyzji (Adamik, 2019) z uwzględnieniem narzędzi umożliwiających ich eksplorację.

Obecnie informację należy traktować jako zasób strategiczny współczesnych organizacji i dlatego też zwraca się dużą uwagę na sposób operowania informacją oraz na selektywny dostęp do niej. W dobie Industry 4.0, czyli szybkiego rozwoju technologicznego, narzędzia oraz systemy informatyczne usprawniają proces utrzymywania, przetwarzania i udostępniania zasobów informacyjnych, co ma również bezpośredni wpływ na zapewnianie informacyjnej i w związku z tym także biznesowej ciągłości działania. Determinuje to dążenie przedsiębiorstw do implementacji skutecznych jakościowo rozwiązań informatycznych, które cechują się wielozadaniowością, co w praktyce oznacza zbieranie, gromadzenie, przetwarzanie i udostępnianie odpowiednich danych konkretnym adresatom z uwzględnieniem przedziału czasu. Wśród narzędzi i systemów informatycznych dominuje model sieciowy, który umożliwia dostęp interesariuszom bez ograniczeń zarówno geograficznych, jak i czasowych. Poziom oraz zakres przetwarzanej informacji są wypadkową zadań danych osób lub zespołów, a także stopnia zaawansowania wykorzystania technologii informatycznych w procesach informacyjno-decyzyjnych w organizacji (Zaskórski, Zaskórski, Woźniak, 2021, s. 159-161). Dlatego też zasoby informacyjne i inne zasoby niematerialne mogą być powiązane funkcjonalnie z różnymi systemami informatycznymi (zob. rys. 1).

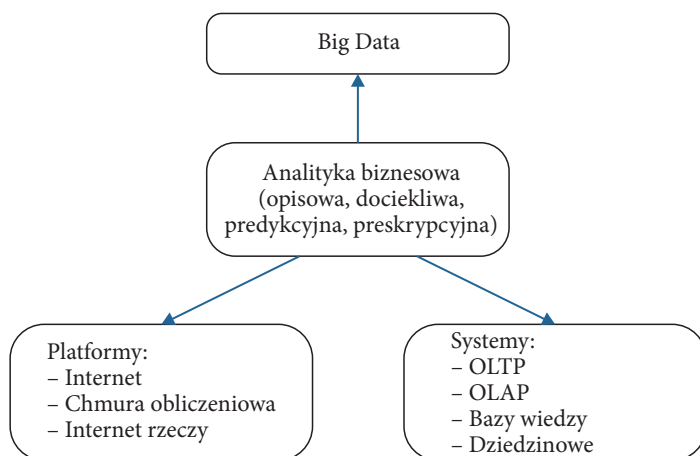
Jednym ze współczesnych wymagań stawianych technologiom informacyjnym w erze czwartej rewolucji technologicznej jest środowisko sztucznej inteligencji, a w tym rola systemów Big Data oraz integracja i współdzielenie różnorodnych zasobów informacyjnych (zob. rys. 2) jako kluczowy element strategii biznesowej.



Rys. 1. Niematerialne zasoby organizacji i systemy informatyczne wspomagające ich utrzymywanie i eksplorację

Źródło: opracowanie własne na podstawie: Kisielnicki, 2013, s. 27

Wykorzystanie zaawansowanych algorytmów uczenia maszynowego umożliwia szybsze dostosowanie produktów i usług do zmieniających się oczekiwań klientów. Przedsiębiorstwa mogą bowiem tworzyć spersonalizowane rekomendacje, co z kolei prowadzi do zwiększenia satysfakcji klientów oraz np. wzrostu sprzedaży. Zaawansowane techniki analizy danych, takie jak eksploracyjna analiza danych (EDA) czy głębokie uczenie, pozwalają na odkrywanie ukrytych wzorców i zależności (Krystian, Zaskórski, 2023).



Rys. 2. Integracja i współdzielenie wielopostaciowych zasobów informacyjnych

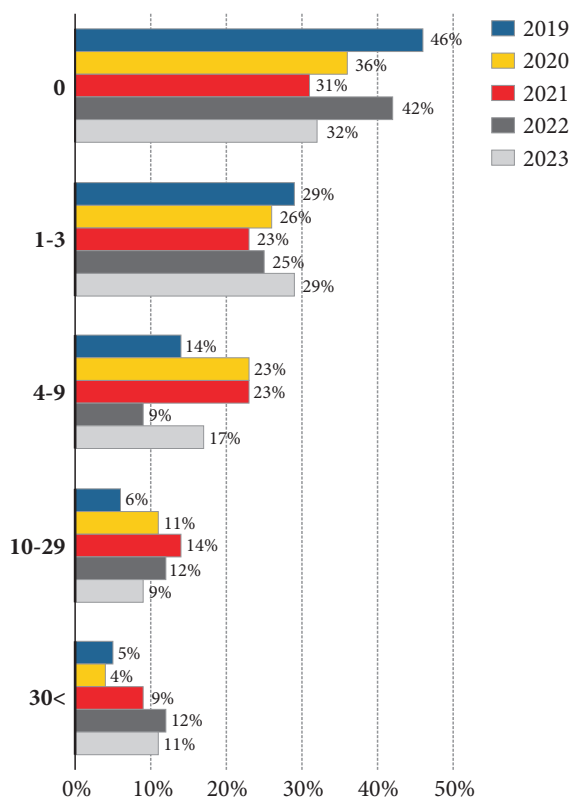
Źródło: opracowanie własne na podstawie: Krystian, Zaskórski, 2023

Rozwój nowoczesnych technologii i rozwiązań spowodował również zmiany w podejściu do zarządzania informacją. Tradycyjne zarządzanie informacją, oparte w dużej mierze na intuicji lub osobistych doświadczeniach kadry kierowniczej, zostało zastąpione organizacją *data-driven*. Organizacja *data-driven* oznacza zarządzanie przedsiębiorstwem przez pełne wykorzystanie dostępnych oraz wysoko przetworzonych danych, które potrzebne są do podejmowania właściwych decyzji strategicznych oraz taktycznych. Podstawową różnicą pomiędzy tradycyjnym podejściem do zarządzania informacją a organizacjami *data-driven* jest traktowanie danych jako wspomnianego już wcześniej zasobu strategicznego (Adamczewski, 2018). Zarządzanie zasobami informacyjnymi w warunkach rewolucji technologicznej wiąże się z wykorzystaniem narzędzi i rozwiązań, które obrabiają i prezentują dane, przekształcając je w wiedzę. To właśnie zarządzanie wiedzą stanowi w praktyce bazę działania organizacji *data-driven*. Wiedza, podobnie jak potencjał informacyjny, może być podstawą przewagi konkurencyjnej przedsiębiorstw, a także podstawą do podnoszenia efektywności zarówno procesów realizowanych w ramach firmy, jak i efektywności całej organizacji (Adamczewski, 2018).

2. Cyberbezpieczeństwo zasobów i usług informacyjnych oraz identyfikacja środowiska analityki biznesowej w cyberprzestrzeni

Cyberbezpieczeństwo to nie tylko nieodłączny komponent, lecz także jeden z najważniejszych obszarów współczesnych organizacji, które funkcjonują w dobie rewolucji Industry 4.0. Traktowane jest jako nowe podejście do projektowania systemów, już od ich najmniejszych elementów, aż do dużych struktur sieciowych. Zgodnie z literaturą przedmiotu cyberbezpieczeństwo powinno być wbudowane w każdą część systemu cyfrowego od początku jego projektu, ponieważ obecnie systemy cyfrowe mogą być „dziurawe”, a bezpieczeństwo danych w wielu systemach jest iluzoryczne (Gregor, Kaczorowska-Spychalska, 2020).

Wagę obszaru cyberbezpieczeństwa w obecnych czasach potwierdza raport Barometr Cyberbezpieczeństwa wykonywany przez firmę KMPG. Warto odnotować, że zgodnie z tym raportem liczba przedsiębiorstw, które nie zauważyły żadnego cyberataku w 2023 roku, zmniejszyła się o 10 punktów procentowych w porównaniu z rokiem 2022. Kluczową informacją z perspektywy naruszenia cyberbezpieczeństwa jest fakt, że 66% organizacji zarejestrowało przynajmniej jeden incydent związany z naruszeniem wewnętrznej cyberprzestrzeni w 2023 roku, co stanowi wzrost o 8 punktów procentowych. Dokładny rozkład wyników raportu przedstawiono na rysunku 3. Duża częstotliwość ataków w cyberprzestrzeni jest możliwa dzięki różnorodności metod, którymi posługują się cyberprzestępcy.



Rys. 3. Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa (wartości na wykresie nie sumują się do 100%, a 2% stanowi odmowa odpowiedzi)

Źródło: opracowanie własne na podstawie: KPMG, 2024

Do najbardziej popularnych metod cyberataków można zaliczyć przede wszystkim (Antczak, 2020):

- boty i wirusy – złośliwe rodzaje oprogramowania, którego głównym celem jest przejęcie częściowej lub całkowitej kontroli nad systemem oraz kradzież danych, mogą zostać aktywowane na różne sposoby, np. przez kliknięcie w wiadomość e-mail lub przeniesione przez zewnętrzne nośniki pamięci bądź aplikacje;
- *phishing* oraz *pharming* – wyłudzenie danych uwierzytelniających odbywające się przez podszywanie się pod zaufane źródło. Do pishingu wykorzystywana jest poczta mailowa. Polega to na tym, że cyberprzestępcy wysyłają maile ze specjalnie przygotowanym linkiem oraz wiadomością mającą zachęcić do kliknięcia w link i przekazania wrażliwych danych. Z kolei *pharming* wykorzystuje przekierowania na fałszywe strony i serwisy www, na które adresat jest kierowany przez złośliwe oprogramowanie;

- *ransomware* – oprogramowanie blokujące dostęp do systemu komputerowego i uniemożliwiające odczyt danych. Oprogramowanie to następnie żąda od użytkownika zapłaty za przywrócenie pierwotnego stanu. Instalowane jest głównie za pomocą załącznika w wiadomości mailowej lub przeglądarki internetowej;
- wycieki danych za pośrednictwem złośliwego oprogramowania (ang. *malware*) – oprogramowanie powodujące szkodę sprzętu użytkownika lub sieci internetowej, co dla hakerów jest powodem do żądania zapłaty okupu za odzyskanie danych;
- zaawansowane ukierunkowane ataki (APT), które są rodzajem trwałego zagrożenia – jest to przede wszystkim ukryty, celowy atak na sieć komputerową, w przypadku którego niepożądane osoby uzyskują dostęp do sieci, a co ważne, pozostają niewykryte przez dłuższy okres, ponieważ są bardzo trudne do zdefiniowania (mogą być niezauważone nawet przez lata).

Metody cyberataków różnią się od siebie stopniem szkód, które mogą wyrządzić zaatakowanym przedsiębiorstwom. Firma KMPG w swoim raporcie przedstawiła cyberzagrożenia stanowiące największe ryzyko dla organizacji na podstawie przeprowadzonych badań ankietowych (zob. rys. 4). Aktualnie to kradzież danych przez *phishing* stanowi główne zagrożenie dla cyberbezpieczeństwa współczesnych organizacji. Z raportu wynika, że kradzież danych w wyniku *phishingu* pozostała głównym zagrożeniem. Z kolei wzrost znaczenia zanotowały kradzież danych związana z naruszaniem bezpieczeństwa fizycznego, a także wycieki danych wynikające z kradzieży bądź utraty nośników.

Konsekwencje utraty danych wrażliwych mogą być dla organizacji bardzo dotkliwe i wiązać się między innymi z utratą pozycji na rynku lub stratami finansowymi. Dlatego też kluczowym aspektem jest skuteczna ochrona i wdrożenie czynników zapobiegawczych. Można do nich zaliczyć środki ochronne (Cadd, 2020), takie jak:

- uwierzytelniania wieloskładnikowe (ang. MFA – *multifactor authentication*) – sposób ochrony cyfrowych zasobów polegający na dodawaniu kolejnych elementów lub kroków do sekwencji logowania (np. dodanie kodu z usługi SMS), co ma na celu utrudnić cyberprzestępcom dostęp do danej usługi lub zbioru danych;
- zapory sieciowe (ang. *firewall*) – zestawienie ochrony sprzętowej, a także programowej monitorujące przychodzący oraz wychodzący ruch sieciowy. Zapory stanowią pierwszą linię obrony sieci komputerowych i są podstawowym elementem struktury cyberbezpieczeństwa nowoczesnych organizacji;
- tworzenie kopii oraz dublowanie (ang. *backup and mirroring*) – działania okresowe wykonywane przez administratorów systemów w przedsiębiorstwach, szczególnie w dobie *cloud computing*, dzięki czemu tworzenie kopii

- zapasowej jest szybsze i prostsze. Dodatkowym działaniem jest również tworzenie środowiska będącego idealnym odwzorowaniem głównej aplikacji, co pozwoli na jej szybką reaktywację w przypadku cyberataku;
- piaskownica (ang. *sandboxing*) – technika pozwalająca na izolowanie i wykluczanie potencjalnie niebezpiecznych plików lub programów, co zmniejsza materializację zagrożeń i skutków ryzyka z nimi związanego.

Wyludzanie danych uwierzytelniających (*phishing*)



Wycieki danych za pośrednictwem złośliwego oprogramowania (*malware*)



Kradzież danych przez pracowników



Zaawansowane ukierunkowane ataki (*advanced persistent threat, APT*)



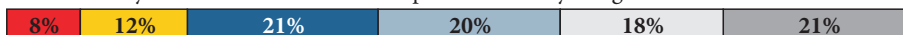
Wyciek danych w wyniku kradzieży lub zgubienia nośników czy urządzeń mobilnych



Ogólne kampanie *ransomware*



Kradzież danych na skutek naruszenia bezpieczeństwa fizycznego



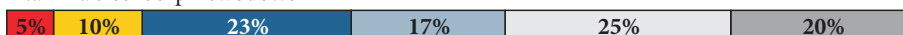
Ataki wykorzystujące błędy w aplikacjach



Włamania do urządzeń mobilnych



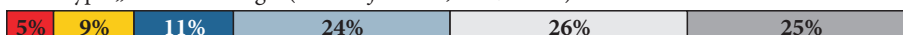
Ataki na sieci bezprzewodowe



Podłuchiwanie ruchu i ataki „człowiek po środku” (*man in the middle, MitM*)



Ataki typu „odmowa usługi” (*denial of service, DoS/DDoS*)



Ataki na łańcuch dostaw za pośrednictwem partnerów biznesowych



Legenda:

■ 5 – najwyższe ryzyko ■ 4 ■ 3 ■ 2 ■ 1 ■ 0 – brak ryzyka

Rys. 4. Cyberzagrożenia stanowiące największe ryzyko dla organizacji

Źródło: KPMG, 2024

W cyberprzestrzeni ważną rolę odgrywa również szeroko pojęta analityka danych, która skupia się na badaniu surowych danych w celu potwierdzania hipotez, znajdowania wzorców, czy też prognozowania oraz wnioskowania (generowania wiedzy) dotyczącego rzeczywistości, co ma miejsce w danej organizacji. Eksploracja i analiza danych to jedna z funkcji współczesnych organizacji odpowiadająca za zdobywanie i poszerzanie wiedzy, która jest niezbędnym elementem przy tworzeniu strategii i planów biznesowych. Literatura przedmiotu wyróżnia dwa podejścia do analityki biznesowej: deskrypcyjne oraz predykcyjne.

Podejście deskrypcyjne ma za zadanie pomóc w identyfikacji i zrozumieniu rzeczywistości dzięki charakterystyce danych, a następnie wyróżnienie zawartych w nich wzorców. Podejście to ogranicza się z reguły do określonego punktu w czasie lub konkretnego przedziału czasowego. Wyniki analizy deskrypcyjnej, które mogą dotyczyć między innymi rezultatów sprzedażowych lub finansowych, wspomagają procesy decyzyjne w organizacjach.

Podejście predykcyjne ukierunkowane jest natomiast na tworzenie i budowanie modeli pozwalających na przewidywanie i symulowanie zdarzeń na podstawie danych teraźniejszych oraz historycznych. Analiza predykcyjna korzysta ze statystyki, uczenia maszynowego bądź techniki *data mining*, a w organizacjach wykorzystuje się ją na przykład do prognozowania zachowań klientów (Pawełszek, 2018).

3. Rola i możliwości środowiska eksploracji wielopostaciowych danych w doskonaleniu procesów biznesowych

Dane, które są ważnym elementem funkcjonowania współczesnych organizacji, mogą występować w różnych formach. Wyróżnić można dane strukturalne pochodzące z baz danych, magazynów danych, a także innych źródeł historycznych, które mają standardowy format dostarczania informacji, a także dane niestrukturalne pozyskiwane ze źródeł, takich jak sensory, media społecznościowe oraz inne strumienie danych w czasie rzeczywistym (Wolniak, 2023). Rozwój nowoczesnych technologii oraz kanałów komunikacji sprawił, że dane zaczęły stawać się wielowymiarowe oraz wielopostaciowe. Dlatego też współczesne organizacje rozwijają obszar analityki danych, która zgodnie z procesem Business Intelligence może wpłynąć na usprawnienie procesów biznesowych realizowanych w ramach danego przedsiębiorstwa oraz na podejmowane decyzje biznesowe. Na szczycie piramidy Business Intelligence (obok systemów OLAP, systemów pytająco-raportujących i hurtowni danych) znajdują się zaawansowane systemy eksploracji danych *data mining*. Nazwa *data mining* definiowana jest jako analiza bardzo dużych zbiorów danych w celu znalezienia nieznanych dotąd związków oraz usystematyzowania i prezentacji otrzymanych wyników (modeli lub wzorców) w formie przydatnej dla ich ostatecznych użytkowników (Zaskórski, 2012).

W kontekście szeroko pojętej analizy danych ważnym aspektem jest procedura przygotowania danych, która zgodnie z literaturą przedmiotu obejmuje osiem etapów (Pyle, 1999):

- uzyskanie dostępu do potrzebnych danych (ang. *accessing data*) – import danych źródłowych do programu analitycznego;
- sprawdzanie danych (ang. *auditing data*) – w praktyce oznacza weryfikację między innymi liczby zmiennych, pomiaru zmiennych czy też zakresów wartości zmiennych ilościowych. Jest to etap, w którym na podstawie przeprowadzonej weryfikacji użytkownik powinien podjąć decyzję, czy dostępny zbiór danych pozwoli na rozwiązanie problemu badawczego;
- uzupełnienie zbioru zmiennych (ang. *enhancing and enriching data*) – dołączenie zmiennych pochodzących ze źródeł zewnętrznych lub tworzenie zmiennych pochodnych;
- poszukiwanie błędów w doborze próby (ang. *looking for sampling bias*) – w praktyce oznacza sprawdzenie sposobu podziału zbioru danych na próbę uczącą i zbiór testowy;
- ustalenie struktury danych (ang. *determining data structure*) – identyfikacja oraz określenie relacji między zmiennymi w zbiorze danych;
- przygotowanie środowiska danych do analizy (ang. *building prepared information environment*) – obejmuje czynności, takie jak na przykład normalizację zmiennych, zastępowanie braków danych lub redukcję liczby zmiennych;
- przegląd danych (ang. *surveying data*) – ponowne sprawdzenie rozkładów zmiennych, identyfikacja oraz weryfikacja rzadko występujących wartości zmiennych i zakłóceń;
- budowa modelu (ang. *modeling data*).

Dane stanowią więc dla organizacji bardzo dużą wartość, a liczba generowanych w ramach organizacji danych stale rośnie. Wiąże się to przede wszystkim z transformacją technologiczną w ramach rewolucji Industry 4.0, a na wartości zyskują różnego rodzaju zbiory danych, zarówno małe, duże, jak i te bardzo duże, czyli *big data*. Sformułowaniem *big data* określa się wielowymiarowe zbiory, a także przetwarzanie danych, takich jak porządkowanie, poszukiwanie, eksploracja, analiza, wykorzystanie, wzbogacanie, wnioskowanie, walidacja, prezentacja, wizualizacja, ekstrakcja informacji, wspomaganie podejmowania decyzji lub optymalizowanie procesów. *Big data* jest więc kluczowym elementem digitalowego ekosystemu społeczeństwa wiedzy, który rozciąga się od poboru danych z Internetu Rzeczy, przez rozproszone gromadzenie oraz przetwarzanie danych w chmurze, po zastosowanie uczenia maszynowego, analityki obliczeniowej czy też przetwarzanie języka naturalnego lub multimedialnych obrazów (Gregor, Kaczorowska-Spychalska, 2020).

Dlatego też koncepcja *big data* dokonała zmiany postrzegania danych przez odejście od usuwania danych i regulowania przestrzeni dyskowej i zachowywania wszystkich danych mogących okazać się wartościowymi oraz szukanie dla nich zastosowania. W ten sposób dzięki przechowywaniu surowych danych w „jeziorach” danych organizacje zapewniają sobie możliwość dowolnego skorzystania z tych danych w przyszłości (Stephenson, 2020).

4. Perspektywy rozwoju modeli analityki biznesowej z wykorzystaniem wybranych narzędzi AI w doskonaleniu modeli biznesowych współczesnego przedsiębiorstwa

Rozwój analityki biznesowej w dobie nowoczesnych technologii, a przede wszystkim w erze sztucznej inteligencji powinien przebiegać zgodnie z ustalonymi etapami tego procesu. Dlatego też ważne jest odniesienie bezpośrednio do danych źródłowych. W większości organizacji podstawowym źródłem danych są wewnętrzne systemy informacyjne. Z reguły są to systemy zintegrowane klasy ERP (ang. *enterprise resource planning*), które mogą dostarczać informacje z wielu obszarów funkcjonujących w organizacji, np. z finansów, kadr, produkcji, logistyki czy też zarządzania relacjami z partnerami lub klientami. W takim przypadku organizacje implementują przemysłowe aplikacje informatyczne oparte na danych z sensorów. Przykładem tego może być firma Predix (Wodecki, 2018), która oferuje rozwiązania łączące infrastrukturę IoT (ang. *Internet of Things*) z systemami komunikacji danych oraz środowiskami umożliwiającymi tworzenie specjalnych aplikacji. W praktyce oznacza to, że firmy produkcyjne korzystające z tych rozwiązań mogą tworzyć zaawansowane rozwiązania analityczne (np. prognostyczne), a dodatkowo mogą tworzyć aplikacje umożliwiające zarządzanie urządzeniami lub linią produkcyjną. Przedsiębiorstwa te mogą ponadto integrować wskazane rozwiązanie z istniejącym już systemem klasy ERP (Wodecki, 2018).

Oprócz danych wewnętrznych występuje wiele źródeł zewnętrznych. Rewolucja technologiczna sprawiła, że organizacje zaczęły na nowo definiować doświadczenia klienta z wykorzystaniem dostępnych rozwiązań technologicznych, takich jak aplikacje mobilne, Internet Rzeczy lub wirtualna rzeczywistość. Według firmy IBM to te cyfrowe obszary kontaktu z klientami, na podstawie raportu wykonanego w 2017 roku, stanowią nowe źródła danych, zarówno ustrukturyzowanych, jak i nieustrukturyzowanych. Sztuczna inteligencja pozwala na pozyskanie wiedzy na temat preferencji indywidualnych klientów, a także ich zachowań i postaw oraz wykorzystanie jej do poprawy doświadczenia klientów w relacjach z organizacją (IBM, 2024).

W odniesieniu do źródeł zewnętrznych należy podkreślić dużą przydatność danych publicznych, które mogą służyć do analiz strategicznych, a także być zasobem wykorzystywanym do rozwoju własnych systemów uczenia się i sztucznej inteligencji.

Istnieje wiele komercyjnych, zewnętrznych źródeł danych wartych wskazania, na przykład firmy oferujące dostęp do obrazów satelitarnych oraz ich analizę, takie jak Planet.os lub CapeAnalytics, przedsiębiorstwa oferujące rozwiązania agregujące dane z milionów źródeł zewnętrznych (np. DataSift lub Bottlenose) czy też systemy, które umożliwiają automatyczną analizę treści stron internetowych (np. import.io lub DiffBot). Rozwiązania te znacznie rozszerzają spektrum narzędzi analitycznych wykorzystywanych we współczesnych organizacjach, stając się jednocześnie coraz tańszym źródłem uzyskania przewagi konkurencyjnej na rynku (Wodecki, 2018). Warto zwrócić również uwagę na pomoc systemów AI w analizowaniu wielkich zbiorów danych, które z reguły zawierają dane nieustrukturyzowane, w postaci zdjęć, dokumentów tekstowych czy też logów sieciowych. Kolekcje te mają postać danych surowych i są przekształcane lub wyciągane w celu uzyskania konkretnych informacji w zależności od czasu i potrzeb użytkowników. Tradycyjne metody analityczne wymagają w tym przypadku danych rozdzielonych na cechy, na przykład płeć, wiek lub adres. W celu lepszego dopasowania modelu analitycy wykorzystują w takich przypadkach inżynierię danych, czyli tworzą dodatkowe cechy, takie jak średnie wydatki podczas jednej wizyty lub czas od ostatniego zakupu. Sztuczna inteligencja wychodzi w tym przypadku naprzeciw, ponieważ niektóre metody AI nie wymagają podziału danych według cech i potrafią pracować z danymi bez jasno określonej struktury. W praktyce oznacza to, że algorytm AI może nauczyć się rozpoznawać na zdjęciach koty, analizując jedynie zdjęcia kotów, bez przedstawiania innych, dodatkowych pojęć opisujących, takich jak twarz, wąsy bądź uszy (Stephenson, 2020).

Systemy sztucznej inteligencji przez wpływ na dane źródłowe i przetwarzanie danych w ramach organizacji przyczyniają się do doskonalenia modelu biznesowego przedsiębiorstwa. Temat poprawy jakości danych z wykorzystaniem sztucznej inteligencji jest przedmiotem badań. Ekspertki z dziedziny AI uważają, że ocena i poprawa danych zaczyna się od zrozumienia, iż jakość danych jest wielowymiarowa. Nie jest możliwe ulepszenie jednego z wymiarów, a następnie oczekiwanie rezultatów w zaawansowanych modelach AI. Dlatego, aby rozwiązać problem z jakością danych, należy sprawdzić, czy dane treningowe, a także repozytorium danych roboczych mają wystarczającą jakość do wykorzystania w zaawansowanych modelach sztucznej inteligencji i uczenia maszynowego (AI@Enterprise Summit, 2021). W raporcie specjalnym *AI@Enterprise 2021* dotyczącym praktycznego zastosowania sztucznej inteligencji w biznesie przedstawiono nowe podejście do jakości danych skorelowane z AI, które niesie wiele interesujących korzyści, takich jak:

- brak potrzeby utrzymywania reguł – oznacza brak problemu ze skalowaniem, ponieważ procesy biznesowe stają się coraz bardziej złożone, a dane są bardziej zróżnicowane;
- algorytm Artificial Intelligence – może wykrywać i identyfikować nieznane jeszcze problemy z jakością danych;

- algorytm sztucznej inteligencji – może sam się uczyć, więc nie trzeba go programować, aby zrozumieć dane lub proces biznesowy, co w praktyce oznacza, że należy jedynie wprowadzić do niego rzeczywiste dane;
- algorytm dostosowuje się także samoczynnie, nadążając dzięki temu zarówno za wszystkimi zmianami w procesach biznesowych, jak i w towarzyszącymi im danymi;
- algorytm dzięki powyższym właściwościom może działać w trybie: wdróż oraz zapomnij, a także może nie tylko znaleźć problem, lecz również zasugerować określone rozwiązanie dla każdego odszukanego nieprawidłowego rekordu;
- algorytm jest w stanie zastąpić większość reguł w dowolnym istniejącym systemie zapewniania jakości danych.

Algorytmy mogą także stworzyć w pełni zautomatyzowany system zapewniania jakości danych w zamkniętej pętli, a problemy z danymi są naprawiane jeszcze przed identyfikacją problemu (AI@Enterprise Summit, 2021).

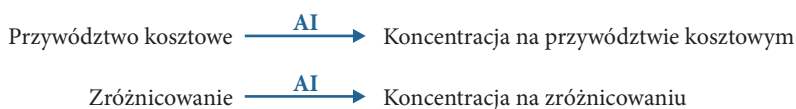
5. Zagrożenia i szanse realizacji usług w cyberprzestrzeni z wykorzystaniem AI

Jednym z głównych zagrożeń związanych z wykorzystaniem AI jest ryzyko nieporządku i braku spójności prawnej w związku z odpowiedzialnością za algorytmy, w tym systemy sztucznej inteligencji. Literatura przedmiotu z zakresu prawa i zarządzania wskazuje, że konieczne jest bezpieczeństwo oraz kontrola nie tylko algorytmu Artificial Intelligence, lecz również usług łączności z Internetem, narzędzi końcowych Internet of Things (takich jak czujniki gromadzące i przesyłające dane zasilające AI), „czystość” i przejrzystość pozyskanych i wykorzystywanych danych, bezpieczeństwo wykorzystywanej usługi *cloud computing*, a także bezpieczeństwo oraz podatność na zmiany wykorzystywanych algorytmów. Konsekwencją tego mogą być różne regulacje prawne poszczególnych podmiotów. Dlatego też problemem jest w tym przypadku złożoność systemu sztucznej inteligencji, która może uniemożliwiać jednolitą odpowiedzialność prawną (Fischer, Pązik, Świerczyński, 2023). Zagrożenie wynikające z braku jednolitych regulacji prawnych może stać się przyczyną braku chęci inwestowania w AI do momentu określania odpowiedzialności prawnej. Wyzwania związane ze sztuczną inteligencją mogą stwarzać ryzyko, jeśli nie będą właściwie zarządzane. Kluczowe jest świadome, odpowiedzialne podejście do jej rozwoju, wdrażania oraz regulacji. Coraz większe uzależnienie od zaawansowanych systemów AI może utrudnić ich zarządzanie, zwłaszcza w przypadku awarii lub sytuacji kryzysowych. Brak odpowiednich norm etycznych i regulacji może skutkować niewłaściwym wykorzystaniem AI, co prowadzi do pytań o odpowiedzialność za decyzje podejmowane przez autonomiczne systemy (tzw. „czarne

skrzynki” zastępujące człowieka w roli decydenta). Sztuczna inteligencja oferuje wiele korzyści dla organizacji oraz całego społeczeństwa (np. automatyzacja procesów, personalizacja produktów lub optymalizacja obsługi klienta), dlatego też istotne jest opracowanie i wdrożenie odpowiednich regulacji, standardów etycznych oraz edukacja społeczeństwa w zakresie AI. Współpraca międzynarodowa i zaangażowanie różnych interesariuszy są niezbędne do zminimalizowania ryzyka i maksymalizacji korzyści wynikających z rozwoju sztucznej inteligencji (DeepTechnology.ai, 2024). Ponadto AI stawia przed współczesnymi organizacjami wiele szans do ich rozwoju, a także szeroko pojętego ulepszania i wywierania przede wszystkim znaczącego wpływu na obraz rynku. Z badań przeprowadzonych przez P. Sliżę oraz E. Dobrowolską w 2019 roku wynika, że w Europie Środkowo-Wschodniej przede wszystkim Polska, a następnie Bułgaria i Rumunia to największe lokalizacje firm sklasyfikowanych jako AI Company (AIC), czyli firm deklarujących wykorzystywanie AI, zweryfikowane na podstawie ofert biznesowych (Sliż, Dobrowolska, 2022).

Sztuczna inteligencja w swoich ramach zawiera uczenie maszynowe, przetwarzanie języków naturalnych, robotykę i inne. Ze względu na skalę działania algorytmy uczenia maszynowego są w stanie optymalizować procesy biznesowe przez ich automatyzację, co niekiedy daje przestrzeń do kreowania nowych produktów bądź usług. Szansą dla firm na skorzystanie z AI stało się obniżenie kosztów mocy obliczeniowych, a także przestrzeni do przechowywania danych, co skłoniło przedsiębiorstwa do zainwestowania w technologię sztucznej inteligencji. Dodatkowo wzrosły także możliwości dostępu do danych, które są kluczowym komponentem dla algorytmów AI. Postępująca globalizacja powoduje, że firmy konkurują w bardziej globalnym oraz dynamicznym otoczeniu, co sprawia, że AI staje się szansą na uzyskanie przewagi konkurencyjnej (Przegalińska, Jemielniak, 2023a). Problematyka implementacji technologii, między innymi AI była przedmiotem badania B. Jackowskiej, P. Sliży oraz J. Sicińskiego (2023). Autorzy na nielosowo dobranej próbie dużych firm usługowych zidentyfikowali, że udział organizacji, w których została wdrożona co najmniej jedna technologia, typu: AI, *data mining*, IoT, *cloud computing*, *augmented reality*, *blockchain*, *big data*, BI, RPA lub *cybersecurity*, wynosiła 52% (w 2,6% przypadkach zaimplementowane zostały wszystkie technologie). Kluczową z perspektywy przyszłości informacją jest fakt, że jedynie w 2% organizacji nie planuje wdrożyć żadnej z wymienionych technologii (Jackowska, Sliż, Siciński, 2023). Chęć implementacji sztucznej inteligencji przez nowoczesne organizacje wiąże się z redefinicją dwóch klasycznych strategii biznesowych. Pierwsza strategia przywództwa kosztowego przez wdrożenie AI może przeobrazić się dzięki automatyzacji zadań, optymalizacji dostępnych zasobów, przy jednoczesnym zwiększeniu efektywności. Kluczowe w tym przypadku staje się tworzenie spersonalizowanych, a nawet hiperspersonalizowanych produktów lub usług dzięki segmentacji rynku oraz specjalnym kampaniom marketingowym, które oparte są na uczeniu maszynowym.

Wspomniane uczenie maszynowe, a w szczególności analiza skupień lub redukcja wymiaru może sprawić, że koncentracja może stać się strategią dominującą, która łączyć będzie w sobie zarówno przywództwo kosztowe, jak i zróżnicowanie. Techniki *machine learning* pozwalają na dokonanie szczegółowej analizy decyzji oraz preferencji zakupowych klientów, tak aby produkty lub usługi zostały jak najlepiej spersonalizowane. Doprowadzi to wówczas do możliwości obniżania marży przedsiębiorstwa, przy jednoczesnej wysokiej dostępności. Redefinicja dwóch głównych strategii biznesowych będzie oznaczać „przywództwo kosztowe zorientowane na koncentrację”, a także „zróżnicowanie oparte na koncentracji” (Przegalińska, Jemieliński, 2023a) (zob. rys. 5).



Rys. 5. Redefinicja klasycznych strategii biznesowych

Źródło: opracowanie własne na podstawie: Przegalińska, Jemieliński, 2023a

Wspomniane działania w ramach strategii i implementacji technologii sztucznej inteligencji można dostrzec w największych światowych organizacjach. Analizy zachowań zakupowych swoich klientów oparte na AI przeprowadza firma Amazon, która dzięki temu przewiduje, które produkty mogą zainteresować konsumentów w przyszłości, przygotowując się w ten sposób na kolejne miesiące pod kątem stanów magazynowych oraz planowania oferty. Podobne działania wykonuje firma Netflix, która przez analizowanie preferencji filmowych użytkowników przygotowuje dla nich spersonalizowane sugestie kolejnych produkcji filmowych i seriali. Kluczowym elementem jest również obszar posprzedażny, w którym na przykład firma Google używa chatbotów odpowiadających na zapytania klientów, redukując tym samym czas oczekiwania na odpowiedź. Są to obszary związane bezpośrednio z relacją na linii firma – klient, oprócz tego skala zastosowania AI jest dużo większa i sięga między innymi procesów produkcyjnych i logistycznych (Przegalińska, Jemieliński, 2023b).

Podsumowanie

Zasoby informacyjne stały się kluczowym elementem współczesnych organizacji biznesowych, wpływając na ich zdolność do skutecznego działania i budowania przewagi konkurencyjnej. Eksploracja danych w cyberprzestrzeni, wspierana przez rozwój technologii sztucznej inteligencji, umożliwia firmom nie tylko optymalizację procesów biznesowych, lecz również wprowadzanie innowacyjnych modeli operacyjnych.

AI oraz zaawansowane narzędzia analityczne stają się fundamentalnym elementem w zarządzaniu wielopostaciowymi danymi, co znacząco wpływa na poprawę efektywności organizacyjnej.

W artykule zaakcentowano także potrzebę ochrony zasobów informacyjnych, podkreślając wagę cyberbezpieczeństwa w kontekście materializacji zagrożeń wynikających z działalności w przestrzeni cyfrowej. Organizacje muszą zatem inwestować nie tylko w narzędzia analityczne, lecz również w rozwiązania zabezpieczające dane, aby skutecznie przeciwdziałać potencjalnym ryzykom. Z perspektywy przyszłości wykorzystanie narzędzi AI w analityce biznesowej będzie odgrywać coraz większą rolę w kształtowaniu modeli biznesowych, umożliwiając lepsze zrozumienie rynku, przewidywanie trendów oraz szybsze podejmowanie decyzji. Jednakże, jak wykazano, wykorzystanie tych technologii wiąże się z pewnymi zagrożeniami, które wymagają uważnego zarządzania, szczególnie w zakresie etyki i transparentności. Tak więc, aby maksymalizować potencjał biznesowy organizacji w erze cyfrowej, niezbędne jest strategiczne podejście do zarządzania zasobami informacyjnymi, a w tym integracja zaawansowanych narzędzi analitycznych oraz troska o cyberbezpieczeństwo. Wykorzystanie technologii AI stanowi nie tylko szansę na rozwój, lecz także wyzwanie, które wymaga odpowiedzialnego i zrównoważonego podejścia do wdrażania nowych technologii w praktyce biznesowej.

BIBLIOGRAFIA

- [1] ADAMCZEWSKI, P., 2018. Organizacje data-driven w ewolucji transformacji cyfrowej, *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu*, nr 527.
- [2] ADAMIK, A., 2019. *Nauka o organizacji. Ujęcie dynamiczne*, Łódź: Wydawnictwo Nieoczywiste.
- [3] AI@ENTERPRISE SUMMIT, 2021. *Raport specjalny AI@Enterprise 2021. Praktyczne zastosowania sztucznej inteligencji w biznesie*, https://aisummit.today/wp-content/uploads/2021/05/Raport_AI_2021.pdf (dostęp: 14.02.2025).
- [4] ANTCHAK, J., 2020. *Zarządzanie przedsiębiorstwem w cyberprzestrzeni*, Warszawa: Akademia Sztuki Wojennej.
- [5] CADD, K., 2020. *Avast Blog History of Cyber Security*, <https://blog.avast.com/history-of-cyber-security-avast> (dostęp: 15.02.2025).
- [6] DEEPTechnology.AI, 2024. *Sztuczna inteligencja – jakie niesie zagrożenia?*, <https://www.deep-technology.ai/sztuczna-inteligencja-jakie-niesie-zagrozenia/> (dostęp: 14.02.2025).
- [7] FISCHER, B., PĄZIK, A., ŚWIERCZYŃSKI, M. (red.), 2023. *Prawo sztucznej inteligencji i nowych technologii 2*, Warszawa: Wolter Kluwer.
- [8] GREGOR, B., KACZOROWSKA-SPYCHAŁSKA, D., 2020. *Technologie cyfrowe w biznesie. Przedsiębiorstwa 4.0 a sztuczna inteligencja*, Warszawa: PWN.
- [9] JACKOWSKA, B., SŁIŻ, P., ŚCIŃSKI, J., 2023. Identyfikacja stopnia dojrzałości implementacji technologii ICT w polskich przedsiębiorstwach usługowych, *Przedsiębiorstwo Przyszłości*, vol. 56, nr 3.
- [10] KISIELNICKI, J., 2013. *Systemy informatyczne zarządzania*, Warszawa: Placet.

-
- [11] KPMG, 2024. *Barometr cyberbezpieczeństwa. Na fali czy w labiryncie regulacji?*, <https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf> (dostęp: 13.02.2025).
- [12] KRYSZTOF, M., ZASKÓRSKI, P., 2023. Sztuczna inteligencja w usprawnianiu procesów biznesowych, *Nowoczesne Systemy Zarządzania*, vol. 18, nr 4.
- [13] PAWEŁOSZEK, I., 2018. Rola kreatywności w analityce biznesowej w kontekście analizy danych marketingowych, *Studia i Prace Kolegium Zarządzania i Finansów*, nr 162.
- [14] POLAK, K., 2018. *W jaki sposób działy marketingu i sprzedaży mogą wykorzystać sztuczną inteligencję do wydobycia wartości z posiadanych danych?*, <https://www.internetstandard.pl/w-jaki-sposob-dzialy-marketingu-i-sprzedazy-moga-wykorzystac-sztuczna-inteligencje-do-wydobycia-wartosci-z-posiadanych-danych/> (dostęp: 12.02.2025).
- [15] PRZEGALIŃSKA, A., JEMIELNIAK, D., 2023a. *AI w strategii. Rewolucja sztucznej inteligencji w zarządzaniu*, Warszawa: MT Biznes.
- [16] PRZEGALIŃSKA, A., JEMIELNIAK, D., 2023b. *Współpracująca sztuczna inteligencja w zastosowaniach biznesowych*, [w:] Ciszewska-Mlinarić, M. (red.), *Przyszłość jest dziś. Trendy kształtujące biznes, społeczeństwo i przywództwo*, Warszawa: Akademia Leona Koźmińskiego.
- [17] PYLE, D., 1999. *Data preparation for data mining*, San Francisco: Morgan Kaufmann.
- [18] SŁIŻ, P., DOBROWOLSKA, E., 2022. Rynek usług generowanych z wykorzystaniem technologii sztucznej inteligencji – przegląd organizacji w Europie Środkowo-Wschodniej, [w:] Wróbel, P. (red.), *Organizacje w warunkach gospodarki cyfrowej*, Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego.
- [19] STEPHENSON, D., 2020. *Big Data, Nauka o danych i AI bez tajemnic. Podejmij lepsze decyzje i rozwijaj swój biznes*, Gliwice: Wydawnictwo Helion.
- [20] WODECKI, A., 2018. *Sztuczna inteligencja w kreowaniu wartości organizacji*, Kraków: edu-Libri.
- [21] WOLNIAK, R., 2023. Deskryptywna analiza danych, *Zarządzanie i Jakość*, vol. 5, nr 2.
- [22] ZASKÓRSKI, P., 2012. *Asymetria informacyjna w zarządzaniu procesami*, Warszawa: Wojskowa Akademia Techniczna.
- [23] ZASKÓRSKI, P., ZASKÓRSKI, W., WOŹNIAK, J., 2021. *Świadomość sytuacyjna a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych*, Warszawa: CeDeWu.

