Zagrożenia dla przedsiębiorstw

2024

sektora MŚP i interesu narodowego
w erze cyfryzacji

Rekomendacje i dobre praktyki

Platforma
Przemysłu
Przyszłości

2024

Zagrożenia dla przedsiębiorstw sektora MŚP i interesu narodowego w erze cyfryzacji
Rekomendacje i dobre praktyki

Warszawa, styczeń 2024

Platforma Przemysłu Przyszłości

Materiał przygotowany w ramach prac grupy ds. Identyfikacji zagrożeń związanych z cyfryzacją Fundacji Platforma Przemysłu Przyszłości

Opracowali:
prof. dr hab. Marian Gorynia
dr hab. Joanna Kuczewska
gen. broni (w st. spocz.) dr Andrzej Fałkowski
dr hab. inż. Krzysztof Pietrusewicz, prof. ZUT

Redakcja:
dr Piotr Kryjom
Zastępca Dyrektora
Dział Zarządzania Wiedzą

Fundacja Platforma Przemysłu Przyszłości
ul. Malczewskiego 24
26-609 Radom

Platforma Przemysłu Przyszłości

Przedmowa

Oddajemy w Państwa ręce raport dotyczący zagrożeń dla przedsiębiorstw sektora MŚP i interesu narodowego w erze cyfryzacji. Niniejsza publikacja jest kolejnym opracowaniem powstałym w ramach prac think tanku powołanego przez Platformę Przemysłu Przyszłości. Tym razem skoncentrowaliśmy się na opracowaniu rekomendacji i praktycznych zaleceń dla przedsiębiorstw dotyczących zagrożeń związanych z wprowadzeniem nowych technologii. W tym przypadku zagrożenia dotyczące pojedynczych podmiotów są także rozpatrywane z punktu widzenia całej gospodarki i bezpieczeństwa narodowego.

Wybór tego tematu nie był przypadkowy. Od kilku lat obserwujemy proces przyspieszonej transformacji cyfrowej polskiej gospodarki. Odbywa się on pod wpływem naturalnego trendu wykorzystania nowych technologii cyfrowych i włączania polskich przedsiębiorstw do globalnych łańcuchów wartości. Na ten proces nakładają się także skutki kryzysu pandemicznego COVID-19 oraz rozwój zagrożeń wynikających z wojny w Ukrainie. W tej sytuacji kluczowe wydaje się pogłębienie refleksji na temat przemyślanego wprowadzania nowych rozwiązań do przedsiębiorstw uwzględniającego nie tylko krótkoterminowe cele związane z podnoszeniem efektywności, ale również zagrożenia związane z interesem publicznym i bezpieczeństwem narodowym.

Niniejsze opracowanie jest jednym z dwóch raportów dotyczących zagrożeń wprowadzania technologii cyfrowych do przedsiębiorstw. Pierwszy raport dotyczy identyfikacji luki cyfrowej oraz zagrożeń wynikających z wprowadzania technologii cyfrowych do przedsiębiorstw, natomiast drugi raport zawiera rekomendacje i praktyczne zalecenia. Pierwszy raport ma charakter teoretyczny i definiuje podstawowe koncepcje oraz pojęcia, natomiast raport drugi odnosi się do praktycznych aspektów działania przedsiębiorstwa i wskazuje najważniejsze zagrożenia zarówno w odniesieniu do poszczególnych technologii cyfrowych jak i procesów biznesowych. Na szczególną uwagę zasługują rekomendacje, które odnoszą się zarówno do polityki gospodarczej oraz działania samorządu gospodarczego jak i praktyki działania poszczególnych przedsiębiorstw. Chciałbym bardzo podziękować autorom, Panu prof. Marianowi Goryni, Pani dr hab. Joannie Kuczewskiej, Panu gen. broni (w st. spocz.) dr Andrzejowi Fałkowskiemu oraz Panu dr hab. Krzysztofowi Pietrusewiczowi, za przekazaną wiedzę, otwartość i zaangażowanie. Mam nadzieję, że publikacja spotka się z Państwa życzliwym zainteresowaniem i pozytywnym odbiorem.

dr Piotr Kryjom
Zastępca Dyrektora
Działu Zarządzania Wiedzą

Spis treści

Streszczenie 6
Summary 7

Wprowadzenie 8

1. Macierz ryzyka 10
   - 1.1. Internet Rzeczy (Internet of Things) – monitorowanie i zbieranie danych z urządzeń 10
   - 1.2. Łańcuch bloków (Blockchain) – rejestr zdecentralizowanych danych, bezpiecznie współużytkowanych 14
   - 1.3. Internet nowej generacji (5G) 17
   - 1.4. Chmura obliczeniowa (Cloud computing) 20
   - 1.5. Sztuczna inteligencja (Artificial Intelligence) i uczenie maszynowe (Machine Learning) 23
   - 1.6. Analiza danych i analiza dużych zbiorów danych (Big Data) 26
   - 1.7. Cyberbezpieczeństwo 29
   - 1.8. Superkomputery i komputery kwantowe 33
   - 1.9. Cyfrowe modelowanie i produkcja (Digital modeling and fabrication) 38
   - 1.10. Systemy autonomiczne i robotyzacja 45
2. Zalecenia i rekomendacje – podejście dedukcyjne 45
   - 2.1. Rekomendacje dla strategii przedsiębiorstw 46
     - 2.1.1. Pozycja cyfrowa 47
     - 2.1.2. Potencjał cyfryzacyjny 49
     - 2.1.3. Strategia cyfrowa 54
   - 2.2. Implikacje dla polityki gospodarczej 59
   - 2.3. Zalecenia dla samorządu gospodarczego 61
3. Zalecenia i rekomendacje – podejście indukcyjne bazujące na studiach przypadków 63

Zakończenie 70

Bibliografi 71

Spis rysunków, tabel 78

Streszczenie

W drugiej części raportu skupiającej się na rekomendacjach mających na celu przeciwdziałanie zagrożeniom związanym z wdrażaniem technologii cyfrowych w MŚP, autorzy dokonują starannej analizy problemu. Celem opracowania jest nie tylko identyfikacja zagrożeń, lecz także dostarczenie praktycznych, zrównoważonych rozwiązań, które mogą wspierać przedsiębiorstwa w skutecznym zarządzaniu ryzykiem cyfrowym, a jednocześnie chronić interesy państwa.

Niniejsze opracowanie obejmuje w pierwszej kolejności kontekst zagrożeń wynikających z dynamicznego postępu technologicznego, zwracając szczególną uwagę na ich potencjalny wpływ na stan ekonomiczny, organizacyjny przedsiębiorstw, a nawet szerzej na stan bezpieczeństwa państwa. W kolejnym etapie, prezentowana jest macierz ryzyka, która służy identyfikacji potencjalnych zagrożeń oraz ocenie ich skali i wpływu na funkcjonowanie MŚP. W ramach podejścia dedukcyjnego, raport proponuje szeroko zakrojone strategie przeciwdziałania zagrożeniom. Podkreśla się konieczność określenia i wzmocnienia pozycji cyfrowej jednostek organizacyjnych, wykorzystania potencjału cyfryzacyjnego oraz stworzenia spójnej strategii cyfrowej, w której bezpieczeństwo odgrywa kluczową rolę. Rekomendacje obejmują zarówno postępowanie ogólne, jak i podejścia bazujące na studiach przypadków. W kontekście strategii przedsiębiorstw, zaleca się określenie i wzmocnienie pozycji cyfrowej, wykorzystanie potencjału cyfryzacyjnego oraz opracowanie spójnej strategii cyfrowej, uwzględniającej różnorodne aspekty. Dodatkowo, w tej części raportu analizowane są implikacje dla polityki gospodarczej, sugerując konieczność integracji strategii cyfrowych przedsiębiorstw z ogólną polityką gospodarczą państwa.

W zakresie samorządu gospodarczego, zaleca się promowanie współpracy mię-dzy przedsiębiorstwami w celu zwiększenia ogólnego poziomu bezpieczeństwa cyfro-wego. Wreszcie, podejście oparte na studiach przypadków stanowi praktyczne narzę-dzie, umożliwiające dostosowanie rekomendacji do różnych kontekstów i sytuacji oraz wyciąganie wniosków na bazie realnych doświadczeń. W ten sposób, raport oferuje wszechstronne podejście do przeciwdziałania zagrożeniom związanym z wprowadzaniem nowych technologii cyfrowych, uwzględniając zarówno aspekty teoretyczne, jak i praktyczne.

Opracowanie zatem opiera się na kompleksowym podejściu metodologicznym, mającym na celu skuteczną analizę i rekomendacje związane z zagrożeniami wprowadzania nowych technologii cyfrowych w przedsiębiorstwach.

Summary

In the second part of the report focusing on recommendations to counter threats associated with the implementation of digital technologies in SMEs, the authors conduct a thorough analysis of the issue. The aim of the study is not only to identify threats but also to provide practical, sustainable solutions that can support businesses in effective digital risk management while safeguarding national interests.

This section encompasses the context of threats arising from dynamic technological advancements, paying particular attention to their potential impact on the economic and organizational issues of businesses, as well as broader implications for national security.

Subsequently, a risk matrix is presented to identify potential threats and assess their scale and impact on the functioning of SMEs. The deductive approach proposed in the report suggests comprehensive strategies to counter threats, emphasizing the need to define and strengthen the digital position of organizational units, harness digitalization potential, and create a coherent digital strategy where security plays a crucial role.

Recommendations include both general guidelines and case study-based approaches. Concerning corporate strategies, it is advised to define and reinforce the digital position, utilize digitalization potential, and develop a coherent digital strategy considering diverse aspects.

Furthermore, the report analyzes implications for economic policy, suggesting the necessity of integrating corporate digital strategies with the overall economic policy of the country. In terms of economic self-government, promoting collaboration between businesses to enhance overall digital security is recommended.

Lastly, the case study-based approach serves as a practical tool, allowing for the adaptation of recommendations to different contexts and situations, drawing conclusions based on real experiences.

The report provides a holistic perspective on mitigating threats linked to the introduction of new digital technologies, considering both theoretical and practical aspects. This study is grounded in a thorough methodological framework designed for effective analysis and recommendations concerning the challenges of implementing new digital technologies in businesses.

Wprowadzenie

Rozważania w części II raportu kontynuują tematykę rozpoczętą w części I, skupiając się na wyzwaniach związanych z cyfryzacją, zwłaszcza małych i średnich firm (MŚP). Kontekstualne tło podkreśla zagrożenia wynikające z dynamicznego postępu technologii, ze szczególnym uwzględnieniem potencjalnego wpływu na aspekty ekonomiczne i organizacyjne przedsiębiorstw, oraz implikacje dla bezpieczeństwa narodowego.

Celem tej części nie jest jedynie zrozumienie i analiza problemów, lecz także opracowanie praktycznych i zrównoważonych rozwiązań. Te rozwiązania mają identyfikować potencjalne zagrożenia oraz proponować skuteczne środki zaradcze. Ich głównym celem jest umożliwienie przedsiębiorstwom skutecznego zarządzania ryzykiem cyfrowym, jednocześnie chroniąc ich interesy ekonomiczne oraz szerzej – interesy narodowe.

W obliczu dynamicznego postępu technologicznego, choć pojawiają się liczne możliwości, to równocześnie rodzą się ryzyka związane z procesem cyfryzacji przedsiębiorstw. Raport ten prezentuje narzędzia analizy ryzyka, takie jak macierz, umożliwiając identyfikację potencjalnych zagrożeń cyfrowych oraz ocenę ich wpływu na funkcjonowanie MŚP. Następnie, przyjmując dedukcyjne podejście, proponowane są spójne strategie przeciwdziałania tym zagrożeniom.

Podkreślono również konieczność wyznaczania i wzmacniania pozycji cyfrowej jednostek organizacyjnych, efektywnego wykorzystywania potencjału cyfryzacji oraz formułowania spójnych strategii, w których bezpieczeństwo odgrywa kluczową rolę. W kontekście strategii przedsiębiorstw, kładzie się nacisk na precyzyjne określanie i wzmacnianie pozycji cyfrowej, efektywne wykorzystywanie potencjału cyfryzacji oraz tworzenie spójnych strategii, uwzględniających różnorodne aspekty.

Dodatkowo, analizowane są implikacje dla polityki gospodarczej, nawołując do integracji korporacyjnych strategii cyfrowych z ogólną polityką gospodarczą państwa. Poprzez zastosowanie różnorodnych narzędzi badawczych, od przeglądu literatury po analizę studiów przypadków, raport ten aspiruje do roli kompleksowego przewodnika, wspierając przedsiębiorstwa w skutecznym zarządzaniu ryzykiem cyfrowym, a jednocześnie chroniąc fundamenty bezpieczeństwa państwa w obliczu dynamicznego rozwoju technologii cyfrowych.

Rekomendacje zawarte w tej części obejmują zarówno ogólne zasady, jak i podejścia oparte na studiach przypadków. Taki sposób pozwala dostosować rekomendacje do różnych kontekstów i sytuacji, jednocześnie czerpiąc wnioski z praktycznych doświadczeń. Wśród rekomendacji dotyczących samorządu gospodarczego znajduje się wspieranie współpracy między przedsiębiorstwami w celu podniesienia ogólnego poziomu bezpieczeństwa cyfrowego.

Do rozważań szczegółowych przyjęto szereg znanych technologii, takich jak: internet rzeczy (Internet of Things) - monitorowanie i zbieranie danych z urządzeń, łańcuch bloków (Blockchain) - rejestr zdecentralizowanych danych, bezpieczne współużytkowanie, internet nowej generacji (5G), chmura obliczeniowa (Cloud computing), sztuczna inteligencja (Artificial Intelligence) i uczenie maszynowe (Machine Learning), analiza danych i analiza dużych zbiorów danych (Big Data), cyberbezpieczeństwo, superkomputery, komputery kwantowe, bezpieczna komunikacja kwantowa, cyfrowe modelowanie i produkcja (Digital modeling and fabrication), systemy autonomiczne i robotyzacja, obliczenia dużych wydajności (HPC).

Katalog powyższy nie jest jednak zamknięty. Postęp w dziedzinie cyfryzacji powoduje, że w szybkim tempie pojawiają się kolejne technologie wraz ze swoimi dobrodziejstwami, jak i wadami.

Przygotowanie się na już istniejące, przy pomocy m.in. części I i II Raportu, pomoże przynajmniej metodologicznie, np. w postaci procedur standardowych opracowanych w MŚP, przygotować się na sytuacje potencjalnych, negatywnych skutków wprowadzenia technologii cyfrowych w przyszłości.

1 Macierz ryzyka

W kolejnych podrozdziałach autorzy zaproponowali macierze ryzyk zidentyfikowanych w toku prac nad raportem wraz ze wskazaniem potencjalnego poziomu ryzyka związanego z wdrażaniem technologii przemysłu przyszłości. Im wyższy poziom ryzyka, tym więcej uwagi należy poświęcić minimalizacji wpływu jego wystąpienia w działalności firm.

1.1. Internet Rzeczy (Internet of Things) – monitorowanie i zbieranie danych z urządzeń

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego
1	2	3	4
ID	**ZE1.1**	**ZT1.1**	**ZB1.1**
Nazwa	**Koszty wdrożenia**	**Brak standaryzacji wymiany danych**	**Zagrożenia w sieci**
Ryzyko	Wysokie	Niskie	Wysokie
Opis	Implementacja infrastruktury IoT, zakup sensorów, urządzeń komunikacyjnych i innych systemów zarządzania może wymagać znacznych inwestycji. Z punktu widzenia MŚP może to stanowić bardzo duże wyzwanie. [1]	Na rynku dostępnych jest wiele rozwiązań systemów IoT/IIoT. Producenci stosują mniej lub bardziej usprawnione normatywne interfejsy komunikacyjne. Chęć wprowadzenia odróżniającego się od innego producenta rozwiązania prowadzi do sytuacji konieczności wyboru technologii ICT na bardzo wczesnym etapie wdrażania technologii. Na rynku znajdujemy kilka tzw. referencyjnych modeli architektury systemów IIoT.	Urządzenia IoT są często słabiej zabezpieczone niż tradycyjne komputery. Hakerzy mogą wykorzystać te słabe punkty, aby uzyskiwać zdalny dostęp do urządzeń IoT, kradnąc dane lub wykorzystywać je do przeprowadzenia ataków na inne systemy. [2]
Czynniki	Czynnikiem ryzyka jest tutaj świadomość kadry zarządzającej dotycząca sposobów finansowania takiej inwestycji.	Kluczowym czynnikiem ryzyka jest tutaj – bardziej aniżeli wybór konkretnego dostawcy rozwiązania – wybór określonej architektury systemu (dostępne architektury to m.in. IIRA, BdvaSira, FIWARE)	Dla bezpieczeństwa narodowego, głównym czynnikiem ryzyka jest rozwijająca się i ewoluująca cyberprzestrzeń, co umożliwia ataki cybernetyczne państw, na infrastrukturę krytyczną, kradzież informacji wrażliwych etc.

1	2	3	4
ID	**ZE1.2**	**ZT1.2**	**ZB1.2**
Nazwa	**Bezpieczeństwo danych strategicznych i zagrożenia dla prywatności [3], [4]**	**Uzależnienie od jednego dostawcy technologii**	**Zbieranie danych wywiadowczych**
Ryzyko	Wysokie	Wysokie	Wysokie
Opis	Zwiększona ilość danych generowanych przez urządzenia IoT zwiększa ryzyko związane z bezpieczeństwem danych. Ryzyko związane z nieprawidłowym zabezpieczeniem danych oraz ataki hakerskie mogą prowadzić do utraty poufnych informacji, co może negatywnie wpłynąć na reputację firmy i spowodować straty ekonomiczne. [5]	Brak wysokich kompetencji związanych z wdrażaniem technologii Internetu Rzeczy oraz jego przemysłowej odmiany sprawia, że MŚP chcąc skrócić sobie drogę do wdrożenia zamiast opracować strategię cyfryzacji zdają się na niekiedy mało profesjonalne doradztwo, w którym jedynym kryterium jest monolityczne podejście do rozwiązania problemu monitorowania i zbierania danych – od tego samego dostawcy, co systemów sterowania oraz wizualizacji.	Państwa lub aktorzy niepaństwowi mogą wykorzystywać urządzenia IoT do zbierania danych wywiadowczych. To może obejmować dane o ruchu ulicznym, lokalizację urządzeń, monitorowanie zachowań ludzi i inne informacje, które mogą być wykorzystane w celach wywiadowczych. [6]
Czynniki	Czynnikiem ryzyka jest tutaj poziom świadomości osób zarządzających w zakresie wdrożenia odpowiednio skutecznych systemów zabezpieczeń i wykorzystania dostępnych danych.	Kluczowym czynnikiem wpływającym tutaj na zwiększenie ryzyka jest chęć skrócenia czasu wdrożenia za wszelką cenę.	Jeden z najważniejszych czynników ryzyka to utrata tajności informacji.
ID	**ZE1.3**	**ZT1.3**	**ZB1.3**
Nazwa	**Zależność od dostawców**	**Starzejąca się technologia. Nowości na rynku**	**Sabotaż i cyberataki na infrastrukturę krytyczną**
Ryzyko	Wysokie	Niskie	Wysokie
Opis	Wdrażanie IoT często wiąże się z korzystaniem z różnych dostawców technologii. Zbyt duża zależność od pojedynczych dostawców, która jest często wynikiem braku strategii transformacji cyfrowej i podatności na zachęty marketingowe może stworzyć ryzyko związanego z ewentualnymi problemami dostaw, zmianami cen czy zmianami w polityce dostawcy.	Na rynku pojawia się wiele rozwiązań technologicznych z obszaru IoT/IIoT. Poza drobnymi graczami i startup-ami szukającymi nowych modeli biznesowych, rynek ten zaczynają zagospodarowywać również duże firmy technologiczne z obszaru systemów sterowania: Siemens, ABB, Fanuc, Beckhoff, ifm electronic i kilka innych. Jest to swego rodzaju ewolucyjny rozwój już posiadanych systemów. Zupełnie inaczej jest w przypadku IoT użytkowego, gdzie firmy przebijają się innowacyjnymi pomysłami, które w niektórych przypadkach mogą być jedynie chęcią monetyzacji nietrafionych pomysłó .	Jeśli urządzenia IoT są używane w infrastrukturze krytycznej, takiej jak elektrownie, sieci energetyczne lub systemy transportu, potencjalnie stanowią one cel dla cyberataków. Ataki na te systemy mogą mieć poważne konsekwencje dla bezpieczeństwa narodowego.[7]

1	2	3	4
Czynniki	Czynnikiem, który wpływa tutaj na zwiększenie ryzyka jest chęć szybkiego wprowadzenia technologii cyfrowych bez odpowiedniego poziomu wiedzy na ich temat.	Kluczowym czynnikiem ryzyka jest bardzo duża liczba nowych rozwiązań na rynku.	Jeden z najważniejszych czynników ryzyka to możliwość przerwania dostępu do kluczowych zasobów energetycznych, komunikacyjnych czy innych niezbędnych dla funkcjonowania państwa.
ID	**ZE1.4**	**ZT1.4**	**ZB1.4**
Nazwa	**Zagrożenia związane z konkurencją**	**Utrata lub nieuprawniony dostęp do strategicznych danych operacyjnych**	**Zakłócenie usług i komunikacji**
Ryzyko	Średnie	Wysokie	Wysokie
Opis	Firmy, które nie dostosowują się do nowych trendów technologicznych, mogą znaleźć się w niekorzystnej sytuacji wpływającej na pogorszenie pozycji konkurencyjnej. Jednocześnie, zbyt szybkie wdrożenie technologii cyfrowych bez odpowiedniej strategii może prowadzić do marnowania zasobów na technologie, które nie przynoszą wartości dodanej. [8]	Każdy system cyfrowy, w tym IIoT narażony jest na zdarzenie nieuprawnionego dostępu. O ile monitorowanie i zbieranie danych z systemów produkcyjnych stanowi jedynie zagrożenie udostępnienia informacji, o tyle nieuprawniony dostęp do modyfikowanych w systemie parametrów może doprowadzić do realnego zagrożenia.	Ataki na urządzenia IoT mogą prowadzić do zakłócenia usług publicznych, komunikacji i operacji rządowych, co może wpłynąć na zdolność państwa do reagowania na kryzysy lub utrzymania normalnego funkcjonowania. [9]
Czynniki	Czynnikiem, który wpływa tutaj na zwiększenie ryzyka jest presja walki konkurencyjnej i chęć wyprzedzenia konkurentów.	Kluczowym czynnikiem ryzyka jest tutaj poziom realnego zagrożenia dla życia ludzkiego, jakim może skutkować nieuprawniony dostęp do parametrów monitorowanego systemu. Stąd typową praktyką jest integracja systemów IIoT w sieciach wewnętrznych, zaś udostępnianie danych realizować należy raczej w trybie Business Intelligence aniżeli wystawiania poza systemy ICT firmy danych surowych.	Jeden z najważniejszych czynników ryzyka to utrata dostępności, która prowadzi do zakłóceń, przerw lub utraty dostępności kluczowych usług i środków komunikacji w skali masowej np. utrzymania porządku publicznego, zarządzania kryzysowego czy nawet świadczenia usług medycznych i ratunkowych.

1	2	3	4
ID			**ZB1.5**
Nazwa			**Zapewnienie dostępu do danych poufnych**
Ryzyko			Wysokie
Opis			Jeśli urządzenia IoT są wykorzystywane w sektorach, które przechowują dane poufne, takie jak służba zdrowia lub finanse, ich skompromitowanie może prowadzić do wycieku danych i naruszenia prywatności. [10]
Czynniki			Jeden z najważniejszych czynników ryzyka to możliwość nieuprawnionego dostępu, przecieku lub utraty poufnych danych, które mogą zawierać informacje o bezpieczeństwie narodowym, strategiach obronnych, działaniach wywiadowczych, czy danych osobowych kluczowych osób.

Źródło: opracowanie własne

1.2. Łańcuch bloków (Blockchain) – rejestr zdecentralizowanych danych, bezpiecznie współużytkowanych

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE2.1	ZT2.1	ZB2.1
Nazwa	Koszty wdrożenia i integracji	Brak demonstratora technologii	Anonimowość i przestępczość
Ryzyko	Wysokie	Wysokie	Średnie
Opis	MŚP mogą znaleźć się w trudnej sytuacji związanej z dostosowaniem i integracją istniejących systemów do korzystania z Blockchaina. Te firm , które maja już rozbudowane systemy informatyczne mogą zmagać się z czasochłonnym i skomplikowanym procesem integracji Blockchaina. Dodatkowo muszą ponieść koszty szkoleń dla personelu oraz dostosować swoje procesy operacyjne. [11], [12]	Brak zrozumiałego dla MŚP demonstratora technologii. Wiele mówi się o potencjalnych zastosowaniach technologii Blockchain w energetyce, w bankowości, w logistyce i transporcie, w zapewnieniu jakości żywności, jednakże to opracowania i koncepcje. Interesującą inicjatywą w Polsce jest praca zespołu z Politechniki Łódzkiej, wskazująca na zastosowania technologii blockchain w systemach IoT.	Blockchain może być wykorzystywany do przeprowadzania nielegalnych działań, takich jak handel narkotykami, pranie pieniędzy i unikanie opodatkowania, ze względu na swoją względną anonimowość. [13]
Czynniki	Czynnikiem, który wpływa na zwiększenie ryzyka jest organiczny dostęp MŚP do demonstratorów Blockchain i w związku z tym podejmowaniem niewłaściwych decyzji inwestycyjnych.	Kluczowym czynnikiem ryzyka wydaje się brak centralnych rządowych inwestycji, dzięki którym demonstrator mógłby zostać szybko przygotowany.	Jeden z najważniejszych czynników ryzyka utrata kontroli nad przepływem finansó , umożliwiając przestępcom ukrywanie źródeł środków oraz utrudniając organom ścigania śledzenie nielegalnych działań
ID	ZE2.2	ZT2.2	ZB2.2
Nazwa	Zagrożenia związane z bezpieczeństwem	Nieetyczne użycie technologii	Zastosowania militarno-strategiczne
Ryzyko	Niskie	Niskie	Średnie
Opis	Mimo, że blockchain jest technologią znaną z bezpieczeństwa, to nadal istnieją potencjalne zagrożenia, takie jak ataki na algorytmy kryptograficzne, a także ryzyko związane z nieprawidłowym wdrożeniem smart kontraktów. [14]–[16]	Technologia blockchain, jak żadna inna współczesna technologia informatyczna sprawia, że w systemie ICT przechowywane są dane strategiczne, dla celów usprawnienia i przyspieszenia podejmowania strategicznych decyzji. Tego typu technologia, w powiązaniu ze sztuczną inteligencją, w nieetycznym użyciu może stać się potężnym narzędziem manipulacji.	Niektóre zastosowania blockchain, takie jak kryptowaluty, mogą być używane do finansowania działań militarnych, terroryzmu lub przemytu broni. [17]

1	2	3	4
Czynniki	Czynnikiem ryzyka jest tutaj za niski poziom świadomości osób zarządzających w zakresie wdrożenia odpowiednio skutecznych systemów zabezpieczeń.	Kluczowym czynnikiem ryzyka jest wysoki poziom zaufania do osób i instytucji, które wdrażają tą technologię.	Jeden z najważniejszych czynników ryzyka to utrata integralności i wiarygodności danych strategicznych, która może prowadzić do dezinformacji, błędnych decyzji strategicznych, a nawet wprowadzenia w błąd co do rzeczywistych zdolności obronnych państwa.
ID		**ZT2.3**	**ZB2.3**
Nazwa		**Energochłonność technologii**	**Ryzyko kryptowalut**
Ryzyko		Wysokie	Średnie
Opis		Z uwagi na olbrzymią ilość obliczeń numerycznych, technologia blockchain jest jedną z tych, która potrzebuje dużych zasobów energii elektrycznej. Dla porównania, scentralizowane systemy zarządzania finansami są mniej energochłonne przy tych samych operacjach i zadaniach.	Instytucje finansowe i gospodarki narodowe mogą być narażone na ryzyko wynikające z niestabilności kryptowalut, co może wpłynąć na stabilność systemu finansowego. [18]
Czynniki		Kluczowym czynnikiem ryzyka w tym obszarze jest opracowanie w przyszłości stosownych do celu algorytmów wykorzystujących technologię blockchain.	Jeden z najważniejszych czynników ryzyka to anonimowość transakcji umożliwiająca nieuczciwym podmiotom finansowania nielegalnych działań, takich jak przestępstwa zorganizowane, handel narkotykami, terroryzm czy cyberataki oraz trudności w ściganiu przestępców, śledzeniu przepływów finansowych oraz utraty kontroli nad przepływem środków w obszarze finansowania działań nielegalnych.

1	2	3	4
ID			**ZB2.4**
Nazwa			**Wykorzystanie w atakach DDoS**
Ryzyko			Średnie
Opis			Zdecentralizowane aplikacje i usługi oparte na blockchain mogą stać się celem ataków typu DDoS (Distributed Denial of Service), co można przetłumaczyć na język polski jako Rozproszony Atak Odmowy Usługi, które mają na celu zakłócenie działania systemów.
Czynniki			Jeden z najważniejszych czynników ryzyka to zakłócenia funkcjonowania przez przeładowanie sieci dużą ilością żądań lub transakcji, co może prowadzić do utraty dostępności i obniżenia wydajności systemu.

Źródło: opracowanie własne

1.3. Internet nowej generacji (5G)

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE3.1	ZT3.1	ZB3.1
Nazwa	Zagrożenie związane z bezpieczeństwem danych strategicznych	Zbytnia ufność w bezpieczeństwo przesyłu danych	Cyberbezpieczeństwo
Ryzyko	Wysokie	Wysokie	Wysokie
Opis	Wprowadzenie technologii 5G na szeroką skalę wiąże się ze zdecydowanie wyższym i dynamicznym przepływem informacji. Przepływ danych strategicznych dotyczących operacji biznesowych, infrastruktury firmy oraz kluczowych danych klientów i dostawców firmy może być zagrożony możliwością ich przejęcia. [19]	W czasie, kiedy do dyspozycji mieliśmy Internet pakietowy (GPRS), zaś przesyłanie MMSów było pieśnią przyszłości, inżynierowie projektujący np. systemy monitorowania sieci ciepłowniczych czy wytwarzania energii elektrycznej, więcej uwagi przywiązywali do stosowania środków technicznych zabezpieczających dane aniżeli współcześnie w epoce Internetu LTE, czy wreszcie 5G. Zakres informacji jaką możemy przesyłać dzięki sieci 5G to już nie tylko proste informacje o stanie monitorowanych urządzeń, ale realne umożliwienie pełnej diagnostyki w czasie rzeczywistym, również w oparciu o sygnały szybkozmienne, jak drgania czy sygnały emisji akustycznej.	5G to nie tylko szybszy internet, ale także infrastruktura, która łączy ogromną liczbę urządzeń IoT (Internet of Things). To tworzy potencjalnie większą powierzchnię ataku dla cyberprzestępców, którzy mogą wykorzystać 5G do przeprowadzania zaawansowanych ataków. [20]
Czynniki	Kluczowym czynnikiem wpływającym na to ryzyko jest świadomość kadry zarządzającej o konieczności inwestycji w systemy ochrony danych.	Wszystkie te atrakcyjne cechy technologii Internetu nowej generacji przesłaniają użytkownikom realne zagrożenia wynikające z możliwego przejęcia tych danych – jak np. o stanie technicznym urządzeń w przemyśle przetwórczym.	Wprowadzenie technologii 5G zwiększa zakres i pojemność sieci, co jednocześnie zwiększa potencjalny obszar ataku na kluczową infrastrukturę, taką jak energetyka, transport, zdrowie czy systemy komunikacji.

1	2	3	4
ID	**ZE3.2**	**ZT3.2**	**ZB3.2**
Nazwa	**Koszty infrastrukturalne**	**Zbyt wolny rozwój infrastruktury i brak gotowości użytkowników końcowych**	**Zależność od dostawców zagranicznych**
Ryzyko	Niskie	Niskie	Wysokie
Opis	Wdrożenie nowej technologii sieciowej 5G wymaga znacznych inwestycji w nową infrastrukturę, taką jak stacje bazowe, anteny i urządzenia. To może generować koszty. [21], [22]	Technologia 5G w przypadku urządzeń mobilnych to technologia bardziej energochłonna. „W porównaniu z siecią LTE sieć 5G pozwala przesyłać więcej danych na jednostkę czasu, a to oznacza większe zużycie energii" (https://consumer.huawei.com/pl/support/content/pl-pl00733968/). Producenci urządzeń mobilnych sugerują w tym trybie włączanie opcji oszczędzania energii elektrycznej.	Wiele krajów opiera się na zagranicznych dostawcach technologii 5G, co może stwarzać ryzyko, jeśli dostawcy nie gwarantują bezpieczeństwa sieci. Wybór dostawców związanych z państwami, które mogą dążyć do wykorzystania tej infrastruktury w celach szpiegowskich lub sabotażu, stanowi potencjalne zagrożenie. [23]
Czynniki	Kluczowym czynnikiem zwiększającym to ryzyko jest brak świadomości kadry zarządzającej związanej z planowaniem wydatków inwestycyjnych oraz chęć szybkiej realizacji inwestycji aby być w czołówce firm wykorzystujących technologię 5G.	Kluczowym czynnikiem ryzyka w aplikacjach przemysłowych wydaje się zatem być pojawienie się na rynku nowych technologii związanych z ogniwami energetycznymi dla urządzeń mobilnych.	Zależność od zagranicznych dostawców technologii 5G, zwłaszcza tych kontrolowanych lub wspieranych przez państwa obce, może stwarzać ryzyko wprowadzenia „tylnych drzwi", szpiegostwa przemysłowego czy celowych zakłóceń w funkcjonowaniu sieci. Ingerencja ze strony dostawców zagranicznych może prowadzić do utraty kontroli nad kluczową infrastrukturą telekomunikacyjną, utraty poufności informacji.
ID			**ZB3.3**
Nazwa			**Naruszenia prywatności**
Ryzyko			Wysokie
Opis			W związku z rozległą siecią urządzeń IoT i przetwarzaniem dużych ilości danych, może istnieć ryzyko naruszeń prywatności obywateli. Nieprawidłowe wykorzystanie danych lub dostęp osób niepowołanych może stanowić zagrożenie dla bezpieczeństwa narodowego. [24]

1	2	3	4
Czynniki			5G umożliwia zbieranie i przetwarzanie znacznie większej ilości danych związanych z użytkownikami, w tym ich lokalizacją, nawykami korzystania z usług oraz innymi danymi osobowymi może prowadzić do wycieku ogromnych ilości danych osobowych. Naruszenia prywatności mogą prowadzić do nadużywania zebranych danych, a także umożliwiać śledzenie obywateli bez ich świadomej zgody, co stwarza potencjalne ryzyko nadużycia władzy.
ID			**ZB3.4**
Nazwa			**Zastosowania militarne**
Ryzyko			Wysokie
Opis			5G ma potencjał do zastosowań w dziedzinie wojskowości, takie jak zdalne operacje, komunikacja w czasie rzeczywistym i autonomia pojazdów. Jednak to również oznacza, że potencjalne ataki na infrastrukturę 5G mogą mieć wpływ na zdolności obronne kraju. [25]
Czynniki			
ID			**ZB3.5**
Nazwa			**Ataki na infrastrukturę krytyczną**
Ryzyko			Wysokie
Opis			Infrastruktura krytyczna, takie jak energetyka, transport czy opieka zdrowotna, może być bardziej podatna na ataki cybernetyczne z wykorzystaniem technologii 5G. Przerwanie dostępu do tych usług może stanowić zagrożenie dla bezpieczeństwa narodowego. [26]
Czynniki			5G zwiększa powierzchnię ataku dla potencjalnych zagrożeń cybernetycznych, co może prowadzić do ataków na infrastrukturę wojskową, systemy komunikacji, czy też szpiegostwa elektronicznego.

Źródło: opracowanie własne

1.4. Chmura obliczeniowa (Cloud computing)

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE4.1	ZT4.1	ZB4.1
Nazwa	Koszty migracji, wdrożenia i integracji systemów	Integracja z istniejącymi systemami	Ochrona danych
Ryzyko	Wysokie	Wysokie	Średnie
Opis	Przejście na chmurę obliczeniową może generować koszty związane z migracją danych, dostosowaniem aplikacji do nowego środowiska oraz szkoleniem pracowników. Ponadto integracja systemów w chmurze z istniejącymi aplikacjami może wymagać dodatkowych nakładów finansowych. [27	Wdrażanie technologii „chmurowych" nigdy nie oznacza nagłej, bezpiecznej, nie wymagającej nakładów i wysiłku zmiany w modelu pracy, zarządzania danymi. Zwykle jest tak, że MŚP transformuje się stopniowo. Przechodzenie na model chmurowy, niezależnie od tego czy subskrypcyjny czy też z zastosowaniem własnych zasobów (infrastruktury) to proces. Wymaga konsekwentnego przełączania interfejsów wymiany danych pomiędzy lokalnymi systemami IT a rozwiązaniami integrującymi dane całego przedsiębiorstwa.	Przechowywanie danych w chmurze obliczeniowej może podnosić pytania dotyczące ochrony prywatności i bezpieczeństwa informacji. Dostawcy usług chmurowych muszą podejmować odpowiednie środki bezpieczeństwa, aby chronić dane użytkowników przed atakami lub dostępem osób niepowołanych. [28]
Czynniki	Czynnikiem, który wpływa tutaj na zwiększenie ryzyka jest przemyślany wybór dostawcy usług chmurowych oraz presja związana z chęcią jak najszybszego wdrożenia nowego rozwiązania.	Strategia to jedno, a technologie, głównie wymiany danych pomiędzy systemami, to drugie. Kluczowym czynnikiem zagrożenia jest w tym przypadku liczba „silosów" IT przedsiębiorstwa, które trzeba z sobą integrować. Może się bowiem okazać, że najlepiej wszystkie zamknąć i zastąpić nowym systemem, ponieważ koszt integracji może przewyższać całościowe wdrożenie.	Czynnik ryzyka to zagrożenie związane z prywatnością danych. Przenoszenie danych państwowych do chmury oznacza, że te informacje są przechowywane i przetwarzane na zewnętrznych serwerach, często zarządzanych przez prywatne firmy lub dostawców usług chmurowych. Może to być naruszenie dostępu, brak kontroli nad danymi, zakres terytorialny i uzależnienie od dostawców usług.

1	2	3	4
ID	**ZE4.2**		**ZB4.2**
Nazwa	**Zależność od dostawcy chmury, awarie i dostępność**		**Zakłócenia usług chmurowych**
Ryzyko	Wysokie		Średnie
Opis	Przedsiębiorstwa korzystające z chmury obliczeniowej uzależnione są od dostawcy usług chmurowych. Zmiany w warunkach umowy, awarie usług lub zmiana cen mogą wpłynąć na koszty w przedsiębiorstwie. [29]		Zawodność lub awarie usług chmurowych mogą zakłócić działanie systemów krytycznych i usług publicznych, co stanowi potencjalne zagrożenie dla bezpieczeństwa narodowego. [30]
Czynniki	Czynnikiem, który wpływa tutaj na zwiększenie ryzyka jest chęć szybkiego wprowadzenia chmury obliczeniowej bez odpowiedniego poziomu wiedzy na jej temat.		Jeden z kluczowych czynników ryzyka to zawodność dostawcy chmury obliczeniowej. Zakłócenia mogą wystąpić z różnych powodów, takich jak awarie sprzętu, ataki cybernetyczne, czy też problemy z zarządzaniem danymi.
ID	**ZE4.3**		**ZB4.3**
Nazwa	**Nadużycia i nieuczciwe korzystanie z usług chmurowych [31]**		**Zależność od dostawców zagranicznych**
Ryzyko	Wysokie		Średnie
Opis	Łatwość wykorzystania zasobów chmurowych sprawia, że stają się one celem organizacji cyberprzestępczych. Istnieje zatem ryzyko ataków mających na celu uzyskanie dostępu do zasobów chmury dzięki włamaniu na konta administracyjne organizacji korzystających z usług chmurowych. [32]		Wiele krajów korzysta z usług chmurowych oferowanych przez dostawców zagranicznych. To może rodzić ryzyko w przypadku, gdy dostawcy ci nie gwarantują bezpieczeństwa lub przestrzegania przepisów dotyczących prywatności. [23]
Czynniki	Czynnikiem ryzyka jest tutaj poziom świadomości kadry menedżerskiej i zakres wdrażania systemów ochrony danych.		Jeden z kluczowych czynników to ryzyko utraty kontroli nad danymi i infrastrukturą, co może skutkować utratą pełnej kontroli nad tymi danymi. Państwo może napotkać trudności w monitorowaniu, audytowaniu czy egzekwowaniu polityki bezpieczeństwa danych zgodnie z krajowymi przepisami, gdyż dostawcy chmurowi często operują w różnych jurysdykcjach.

1	2	3	4
ID			**ZB4.4**
Nazwa			**Cyberataki**
Ryzyko			Średnie
Opis			Chmura obliczeniowa może stać się celem zaawansowanych cyberataków. Atak na dostawcę usług chmurowych może prowadzić do wycieku danych, a w konsekwencji do kompromitacji danych krytycznych dla bezpieczeństwa narodowego. [33]
Czynniki			Chmura obliczeniowa umożliwia przechowywanie ogromnych ilości danych i zasobów w jednym miejscu. Atakujący, jeśli uzyska dostęp do jednego punktu w chmurze, może potencjalnie narazić na ryzyko duże ilości danych lub zasobów. W przypadku dzielenia zasobów i nieodpowiedniego ich izolowania, istnieje ryzyko, że atakujący może wykorzystać lukę w zabezpieczeniach, aby uzyskać dostęp do danych innych podmiotów.
ID			**ZB4.5**
Nazwa			**Zakłócenia operacji wojskowych**
Ryzyko			Średnie
Opis			W kontekście obronności i operacji wojskowych, awarie lub zakłócenia w usługach chmurowych mogą wpłynąć na zdolność do wykonywania operacji i komunikacji. [34]
Czynniki			Jeśli państwo jest silnie zależne od chmury obliczeniowej, to awaria tego środowiska może znacząco utrudnić lub nawet uniemożliwić realizację planowanych operacji wojskowych.

Źródło: opracowanie własne

1.5. Sztuczna inteligencja (Artificial Intelligence) i uczenie maszynowe (Machine Learning)

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID ryzyka (unikalne)	**ZE5.1**	**ZT5.1**	**ZB5.1**
Nazwa ryzyka	**Koszty wdrożenia**	**Ignorancja ludzka i przypisywanie AI cech mitycznych**	**Cyberatakcyjne potencjały**
Poziom ryzyka	Wysokie	Wysokie	Średnie
Opis ryzyka	Wdrożenie systemów AI i ML w przedsiębiorstwach może generować wysokie koszty, zarówno związane z zakupem i dostosowaniem odpowiednich technologii, jak i szkoleniem personelu. [8], [35], [36]	Uchwałą Nr 196 Rady Ministrów z dnia 28 grudnia 2020 roku ustanowiono w Polsce „Politykę dla rozwoju sztucznej inteligencji w Polsce od roku 2020" [37]. Zdefiniowano w tym dokumencie punkty styku AI i społeczeństwa, AI i innowacyjnych firm, AI i nauki, AI i edukacji, AI i współpracy międzynarodowej czy wreszcie AI i sektora publicznego. Z punktu widzenia technologicznego sztuczna inteligencja jest analogiem zamkniętego układu regulacji z tzw. sprzężeniem zwrotnym. Nie są mityczne a czysto technologiczne: niezbędna jest odpowiednia moc obliczeniowa oraz specjalistyczna wiedza techniczna nt. konkretnego zastosowania wybranego rodzaju algorytmu uczenia maszynowego/ ogólnie metod sztucznej inteligencji do zastosowania (rozpoznawanie obrazu, podejmowanie decyzji, sterowanie wielowymiarowymi obiektami fizycznymi, diagnozowanie stanu maszyn i urządzeń lub budynków).	AI i ML mogą być wykorzystywane do przeprowadzania bardziej zaawansowanych i skutecznych cyberataków. Algorytmy ML mogą pomóc hakerom w identyfikowaniu luk w zabezpieczeniach, a także w automatyzacji ataków. [38]
Czynniki ryzyka	Kluczowym czynnikiem ryzyka może być tutaj świadomość kadry zarządzającej i dostosowania strategii wdrażania rozwiązań AI i ML do realnych potrzeb przedsiębiorstwa zgodnych z obranymi celami strategicznymi.	Systemy sztucznej inteligencji są zarówno zasobochłonne jak i energochłonne. Dodatkowo, czas potrzebny na dostrojenie/nauczenie algorytmu jest duży. Algorytmy sztucznej inteligencji, w tym uczenia maszynowego, jak sama nazwa wskazuje, wymagają czasu i danych by się po prostu nauczyć.	Kluczowym czynnikiem ryzyka może być stworzenie zautomatyzowanych ataków, które szybko analizują, identyfikują i wykorzystują podatności w systemach bez potrzeby ciągłej interwencji człowieka.

1	2	3	4
ID	**ZE5.2**		**ZB5.2**
Nazwa	**Zmiany zatrudnienia i deficyty związane z brakiem wyspecjalizowanej kadry**		**Dezinformacja i deepfake**
Ryzyko	Wysokie		Średnie
Opis	Wdrożenie systemów AI i ML mogą prowadzić do redukcji niektórych tradycyjnych stanowisk i jednocześnie mogą kreować nowe stanowiska wymagające umiejętności z zakresu analizy danych i obsługi tych technologii. [39], [40]		Za pomocą technologii AI można tworzyć deepfake - realistyczne fałszywe treści wideo i audio, które mogą być wykorzystywane do rozpowszechniania dezinformacji i siania zamętu w społeczeństwach. [41]
Czynniki	Kluczowym czynnikiem ryzyka jest błędna analiza potrzeb oraz presja wdrożenia systemów AI i ML w celu jak najszybszej redukcji kosztów i wzrostu zysku.		Czynnikiem ryzyka będzie odróżnienie bardzo wiernych manipulacji, jak fałszywe film , dźwięki lub obrazy, które trudno odróżnić od prawdziwych, co może wpływać na opinię publiczną, destabilizować społeczeństwo i wprowadzać zamieszanie w sytuacjach kryzysowych.
ID	**ZE5.3**		**ZB5.3**
Nazwa	**Ryzyko związane z jakością danych i podejmowaniem błędnych decyzji**		**Autonomiczne systemy wojskowe**
Ryzyko	Wysokie		Średnie
Opis	Brak dokładnych i reprezentatywnych danych wykorzystywanych przez AI i ML może prowadzić do błędnych wniosków, co z kolei zwiększa zagrożenie stabilności ekonomicznej przedsiębiorstwa. [42], [43]		AI może być wykorzystywane do sterowania autonomicznymi systemami wojskowymi, co rodzi pytania o kontrolę i etykę wojny. [44]
Czynniki	Kluczowym czynnikiem ryzyka jest tutaj rzetelność danych wykorzystywanych przez systemy AI i ML, kwestia poziomu zaufania do rozwiązań generowanych przez te systemy oraz odpowiedzialność za decyzje maszynowe.		Jeden z istotnych czynników ryzyka to fakt, że decyzje autonomiczne w kontekście użycia siły mogą prowadzić do sytuacji, gdzie ludzka interwencja staje się utrudniona lub niemożliwa w czasie rzeczywistym, co może prowadzić do poważnych konsekwencji, takich jak niekontrolowane ataki, błędy identyfikacyjne, lub użycie siły w sposób, który nie jest zgodny z zasadami międzynarodowego prawa humanitarnego.

1	2	3	4
ID			**ZB5.4**
Nazwa			**Naruszenia prywatności**
Ryzyko			Średnie
Opis			Uczenie maszynowe i analiza danych mogą być używane do śledzenia i monitorowania obywateli, co stanowi potencjalne zagrożenie dla prywatności i wolności jednostek. [45]
Czynniki			Jeden z najważniejszych czynników ryzyka to zbieranie ogromnych ilości danych, co niesie ze sobą śledzenie działań, preferencji, nieautoryzowane monitorowanie jednostek etc.
ID			**ZB5.5**
Nazwa			**Zatrudnienie i ekonomia**
Ryzyko			Średnie
Opis			Automatyzacja prac przy użyciu AI i ML może prowadzić do utraty miejsc pracy i destabilizacji ekonomii, co może wpłynąć na bezpieczeństwo socjalne. [46]
Czynniki			Czynnikiem ryzyka jest ryzyko bezrobocia strukturalnego, a wiec utrata miejsc pracy w niektórych sektorach, co wpływać będzie na struktury i modele biznesowe oraz generować trudności w gospodarce kraju

Źródło: opracowanie własne

1.6. Analiza danych i analiza dużych zbiorów danych (Big Data)

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE6.1	ZT6.1	ZB6.1
Nazwa	Koszty wdrożenia	Wybór technologii, definicja wyzwania interfejsów	Naruszenia prywatności
Ryzyko	Wysokie	Niskie	Wysokie
Opis	Wdrożenie systemów analizy dużych zbiorów danych (Big Data), w tym zakup odpowiedniego oprogramowania, pozyskanie wykwalifikowanego personelu i szkolenie pracowników, może generować wysokie koszty. Firmy muszą także inwestować w odpowiednie narzędzia analityczne oraz pozyskiwać pracowników z umiejętnościami z zakresu analizy danych. [47]	Zanim przygotujemy dane do analiz, należy zadbać o ich jakość podczas gromadzenia. Do dużych zbiorów danych zaliczamy zarówno dane pochodzące z pracujących każdego dnia maszyn, systemów zasilania oraz zużycia mediów, czy wreszcie dane związane z procesami zarządczymi w firmie. Jeżeli nie dopilnujemy, by gromadzone dane były wysokiej jakości, wtedy analizy będą obarczone dużymi błędami. Dodatkowo do danych stanowiących duże zbiory zaliczamy nie tylko dane dostępne cyfrowo, ale również sygnały, takie jak dźwięk czy obraz zeskanowanych dokumentów. Na porządku dziennym jest również zastosowanie algorytmów rozpoznawania języka naturalnego, obszarowo przypisywane metodom sztucznej inteligencji i uczenia maszynowego.	W miarę zbierania, przetwarzania i analizowania ogromnych ilości danych, istnieje ryzyko naruszenia prywatności obywateli. Zbyt szerokie lub niekontrolowane wykorzystanie danych osobowych może stanowić zagrożenie. [45]
Czynniki	Kluczowym czynnikiem ryzyka jest pozyskanie wykwalifikowanych pracowników rekompensujących poniesione nakłady inwestycyjne.	Zagrożenia związane z zastosowaniem AI do analizy danych oraz metod uczenia maszynowego w aplikacjach do dużych zbiorów danych wnoszą wszystkie ryzyka z nimi związane do obszaru BigData.	Jeden z czynników ryzyka to nadmierna inwigilacja, profilowanie lub nielegalne udostępnianie danych.

1	2	3	4
ID	**ZE6.2**	**ZT6.2**	**ZB6.2**
Nazwa	**Zarządzanie danymi**	**Dużo danych, dużo przestrzeni, dużo energii**	**Wywiad gospodarczy**
Ryzyko	Wysokie	Średnie	Wysokie
Opis	Nieumiejętność opracowania skutecznego planu zarządzania danymi może prowadzić do nadmiernego gromadzenia niepotrzebnych informacji. To wpływa na zwiększenie kosztów związanych z ich przechowywaniem i przetwarzaniem. [48]	Podobnie jak w przypadku technologii Internetu nowej generacji (5G) jednakże na znacznie większą skalę pojawia się problem zasobów energetycznych dla systemów opartych o analizę dużych zbiorów danych.	Firmy lub państwa mogą wykorzystywać analizę Big Data do pozyskiwania konkurencyjnych informacji gospodarczych lub technologicznych, co może wpłynąć na interesy narodowe. [49]
Czynniki	Kluczowym czynnikiem ryzyka jest pozyskanie wykwalifikowanych pracowników w zakresie analizy Big Data.	Konieczność zabezpieczenia danych przed utratą, konieczność zabezpieczenia zasilania systemów w trakcie pracy, duże zużycie energii – wszystko to wyzwania i de facto czynniki kształtujące ryzyko operacyjne MŚP podczas wdrażania tej technologii.	Jeden z czynników ryzyka to nielegalne pozyskiwanie poufnych informacji dotyczących strategii, planów inwestycyjnych, nowych produktów czy tajemnic handlowych konkurencyjnych firm.
ID	**ZE6.3**		**ZB6.3**
Nazwa	**Brak umiejętności analitycznych i ryzyko błędnych decyzji**		**Zagrożenia w sieci**
Ryzyko	Wysokie		Wysokie
Opis	Przedsiębiorstwa mogą napotkać trudności w pozyskaniu odpowiednich pracowników posiadających umiejętności analityczne gwarantujące podejmowanie słusznych decyzji strategicznych na podstawie analizy Big Data. Istnieje ryzyko błędnych wniosków, zwłaszcza jeśli dane są nieprawidłowe lub analizowane niewłaściwie. [50]		Big Data może być celem ataków cybernetycznych, ze względu na duże ilości cennych informacji, które przechowuje. Atak na bazę danych Big Data może prowadzić do wycieku informacji lub sabotowania działalności. [51]
Czynniki	Kluczowym czynnikiem ryzyka jest tutaj możliwość pozyskania wyspecjalizowanych pracowników.		Czynnikiem ryzyka jest potencjał wykorzystania Big Data do ulepszania i zwiększania skuteczności ataków cybernetycznych.

1	2	3	4
ID			**ZB6.4**
Nazwa			**Ukierunkowane dezinformacje**
Ryzyko			**Wysokie**
Opis			Analiza danych może być używana do tworzenia bardziej wyrafinowanych i ukierunkowanych kampanii dezinformacyjnych, które wpłyną na opinię publiczną i procesy polityczne. [52]
Czynniki			Czynnikiem ryzyka jest możliwość manipulacji ogromnymi ilościami informacji w celu celowego wprowadzania w błąd opinii publicznej. Wykorzystując Big Data, ktoś może precyzyjnie dostosowywać treści dezinformacyjne do konkretnej grupy odbiorców, co zwiększa skuteczność kampanii dezinformacyjnych.

Źródło: opracowanie własne

1.7. Cyberbezpieczeństwo

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE7.1	ZT7.1	ZB7.1
Nazwa	Ryzyko wdrożenia niewłaściwych rozwiązań technologicznych	Konieczność stosowania najnowszych osiągnięć techniki (zagrożenie)	Ataki cybernetyczne
Ryzyko	Wysokie	Wysokie	Wysokie
Opis	Duże ryzyko wiąże się z zastosowaniem nieodpowiednich systemów i narzędzi ochrony danych tworzących nieskuteczną zaporę przed atakami hakerskimi. [53], [54]	Wojna w Ukrainie i inne kryzysy związane ze zwiększoną aktywnością służb specjalnych, firm i instytucji pokazują jak ważne jest stosowanie systemów typu SIEM (ang. Security Information and Event Management). Systemy tego typu dostarczają raportów i generują ostrzeżenia dotyczące podejrzanego ruchu w sieci komputerowej. Na koniec dnia jednakże wszystko, poza kosztem inwestycji w sam sprzęt i oprogramowanie zwiększające poziom bezpieczeństwa cyfrowego, poza zasilaniem (dostarczeniem odpowiedniej ilości energii elektrycznej) wymaga odprowadzenia niekiedy olbrzymiej ilości ciepła.	Hakerzy, cyberprzestępcy lub państwa-narodowe mogą próbować włamać się do systemów komputerowych, sieci, instytucji rządowych lub innych kluczowych organizacji w celu kradzieży informacji, sabotażu lub zakłócenia operacji krytycznych. [55]
Czynniki	Kluczowe czynniki ryzyka zmniejszające szansę jego wystąpienia to zakup wyłącznie nowych rozwiązań technologicznych, o wysokiej skuteczności.	Rozwój technologiczny jest w tym obszarze bardzo dynamiczny, zastosowanie metod sztucznej inteligencji coraz powszechniejsze. MŚP nie mogą tutaj oszczędzać, ponieważ skutki złamania bezpieczeństwa cyfrowego MŚP np. w zakresie danych z produkcji czy danych o klientach w obszarze innowacyjnych technologii mogą być znacznie kosztowniejsze od potencjalnej inwestycji.	Czynnikiem ryzyka jest rosnąca złożoność i zaawansowanie technik używanych przez cyberprzestępców. Atakujący stale doskonalą swoje metody, co może sprawić, że tradycyjne środki obrony staną się mniej skuteczne.

1	2	3	4
ID	**ZE7.2**		**ZB7.2**
Nazwa	**Wysokie koszty wdrożenia kompleksowych rozwiązań cyberbezpieczeństwa**		**Infrastruktura krytyczna**
Ryzyko	Wysokie		Wysokie
Opis	Wdrożenie zaawansowanego, nowoczesnego, ale jednocześnie skutecznego oprogramowania antywirusowego, systemów wykrywania ataków hakerskich czy zabezpieczenia sieciowe, mogą generować wysokie koszty. Firmy muszą inwestować w odpowiednie technologie, szkolenie personelu i regularne aktualizacje. [56]		Ataki na infrastrukturę krytyczną, taką jak elektrownie, sieci energetyczne, systemy transportu i telekomunikacji, mogą prowadzić do poważnych zakłóceń w dostawach energii, usługach publicznych lub innych kluczowych obszarach, co ma wpływ na zdolność państwa do działania. [57]
Czynniki	Kluczowym czynnikiem ryzyka jest tutaj świadomość kadry zarządzającej w zakresie znaczenia wyboru wyłącznie nowoczesnych technologii, które mogą okazać się znacznie mniej kosztowne w stosunku do poniesionych strat w przypadku złamania zabezpieczeń.		Czynnikiem ryzyka jest rosnące zagrożenie ataków cybernetycznych na kluczowe sektory, takie jak energetyka, transport, czy komunikacja, co może prowadzić do poważnych zakłóceń lub zniszczeń w funkcjonowaniu kraju.
ID	**ZE7.3**		**ZB7.3**
Nazwa	**Ograniczenie dostępności do danych i zmniejszenie wydajności sieci**		**Naruszenia prywatności i wycieki danych**
Ryzyko	Niskie		Wysokie
Opis	Wdrażanie środków bezpieczeństwa, takich jak zabezpieczenia sieciowe czy kontrole dostępu, może skutkować ograniczeniem dostępności do danych dla niepowołanych użytkowników oraz wpływać na ograniczenie wydajność sieci. Jeśli nie są dobrze dostosowane, mogą generować opóźnienia w przesyłaniu danych i wpływać na działanie aplikacji, a tym samym zmniejszać efektywność operacji i procesów biznesowych. [58]		Ataki na bazy danych i naruszenia prywatności mogą prowadzić do kradzieży wrażliwych informacji, wycieku poufnych dokumentów lub naruszenia prywatności obywateli, co może mieć wpływ na bezpieczeństwo narodowe. [59]

1	2	3	4
Czynniki	Kluczowym czynnikiem ryzyka jest tutaj świadomość kadry zarządzającej w zakresie znaczenia wyboru wyłącznie nowoczesnych technologii.		Ataki cybernetyczne mogą doprowadzić do nieautoryzowanego dostępu do baz danych zawierających poufne informacje, co stanowi poważne zagrożenie dla prywatności jednostek i bezpieczeństwa państwa.
ID			**ZB7.4**
Nazwa			**Sabotaż operacji rządowych**
Ryzyko			Wysokie
Opis			Ataki na systemy rządowe mogą zakłócić działalność rządową, łączność, zdolność do reagowania na kryzysy i obronność narodową. [60]
Czynniki			Czynnikiem ryzyka jest możliwość zakłócania, dezorganizacji lub zniszczenia systemów informatycznych odpowiedzialnych za kluczowe funkcje państwa. Ataki cybernetyczne, skierowane na operacje rządowe, mogą prowadzić do utraty integralności danych, zakłóceń w komunikacji, a także paraliżu systemów zarządzania.

1	2	3	4
ID			**ZB7.5**
Nazwa			**Dezinformacja i propaganda online**
Ryzyko			Wysokie
Opis			Manipulacja informacjami i dezinformacja rozpowszechniane za pomocą Internetu mogą wpłynąć na opinię publiczną, destabilizować społeczeństwo i wpłynąć na procesy polityczne oraz stabilność państwa. [61]
Czynniki			Czynnikiem ryzyka jest możliwość geoprzestrzennego wpływu na opinię publiczną oraz demokratyczne procesy decyzyjne poprzez fałszywe informacje rozprzestrzeniane w Internecie, szerzenie dezinformacji, tworzenie fałszywych narracji czy nawet manipulacji społeczeństwem za pomocą propagandy online.
ID			**ZB7.6**
Nazwa			**Ataki na sektor zdrowia**
Ryzyko			Wysokie
Opis			W trakcie kryzysów, takich jak pandemia, ataki cybernetyczne na sektor zdrowia mogą zakłócić dostęp do opieki zdrowotnej, dostaw lekarstw i informacji zdrowotnych. [62]
Czynniki			Czynnikiem ryzyka dla sektora zdrowia jest możliwość zakłócenia, zablokowania lub nawet zniszczenia systemów informatycznych w placówkach medycznych, co może prowadzić do poważnych zagrożeń dla pacjentów, zakłóceń w świadczeniu opieki zdrowotnej oraz naruszenia poufności danych medycznych.

Źródło: opracowanie własne

1.8. Superkomputery i komputery kwantowe

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE8.1	ZT8.1	ZB8.1
Nazwa	Wysokie koszty inwestycji	Brak dostępności użytkowej technologii	Ataki na kryptografię
Ryzyko	Wysokie	Wysokie	Wysokie
Opis	Przedsiębiorstwa planujące inwestycje w infrastrukturę, specjalistyczną technologię i wysoko wykwalifikowany personel muszą liczyć się z poniesieniem wysokich kosztów inwestycji. [63]	Wiele mówi się obecnie o możliwościach, jakie oferują kubity oraz o tym, jak zmienią świat. Dziedzinowość komputera kwantowego sprawia, że każde z zastosowań jest de facto opracowaniem nowego typu oraz rodzaju komputera kwantowego.	Superkomputery o dużej mocy obliczeniowej mogą być używane do łamania kryptografii, w tym algorytmów szyfrowania, co stanowi zagrożenie dla poufności danych i bezpieczeństwa komunikacji. [64]
Czynniki	Kluczowym czynnikiem ryzyka jest chęć szybkiego uczestnictwa w nowoczesnych projektach bez oszacowania zwrotu z tak kosztownej inwestycji.	Sama idea komputera kwantowego wskazuje, iż strukturalnie jest to rozwiązanie bardzo bezpieczne – wszystko będzie zależeć od obszaru zastosowań oraz tego, jakie dane i jakie ilości danych będą wymieniane pomiędzy komputerami kwantowymi a otoczeniem (w tym innymi systemami).	Czynnikiem ryzyka jest potencjalna możliwość złamania lub osłabienia algorytmów kryptograficznych, co może prowadzić do kompromitacji poufności komunikacji oraz naruszenia integralności danych przechowywanych elektronicznie.
ID		ZT8.2	ZB8.2
Nazwa		Wyzwania związane z programowaniem kwantowym	Symulacje broni jądrowej
Ryzyko		Wysokie	Wysokie
Opis		Programowanie komputerów kwantowych jest bardzo skomplikowane i wymaga specjalistycznych umiejętności i wiedzy eksperckiej. Brak wykwalifikowanych programistów kwantowych może stanowić poważne zagrożenie dla efektywnego wykorzystania zaawansowanych komputerów. [65]	Superkomputery są wykorzystywane do przeprowadzania symulacji broni jądrowej i innych zastosowań militarnych, co rodzi pytania dotyczące stabilności i kontroli broni nuklearnej. [66]

1	2	3	4
Czynniki		Kluczowym czynnikiem ryzyka jest dostępność i koszt utrzymania wyspecjalizowanych pracowników.	Czynnikiem ryzyka jest potencjalne przejęcie lub zakłócenie systemów komputerowych odpowiedzialnych za kontrolę i monitorowanie broni jądrowej, co może prowadzić do poważnych konsekwencji, w tym przypadkowego uruchomienia, dezaktywacji, lub nawet fałszywej informacji na temat potencjalnych ataków. Ataki cybernetyczne na systemy kontroli broni jądrowej stanowią szczególne zagrożenie ze względu na potencjalne katastrofalne skutki i wpływ na bezpieczeństwo globalne.
ID			**ZB8.3**
Nazwa			**Ataki na infrastrukturę krytyczną**
Ryzyko			Wysokie
Opis			Użycie superkomputerów do przeprowadzania zaawansowanych ataków na infrastrukturę krytyczną, taką jak systemy energetyczne czy telekomunikacyjne, może stanowić poważne zagrożenie dla bezpieczeństwa narodowego. [67]
Czynniki			Czynnikiem ryzyka jest potencjalna zdolność do złamania tradycyjnych szyfrów i algorytmów kryptograficznych, co mogłoby umożliwić przeprowadzenie ataków na kluczowe systemy informatyczne wspierające infrastrukturę, takie jak sieci energetyczne, systemy telekomunikacyjne czy systemy transportowe. Komputery kwantowe, gdyby stały się powszechnie dostępne i zdolne do łamania obecnych standardów kryptograficznych.

1	2	3	4
ID			**ZB8.4**
Nazwa			**Łamanie kryptografii kwantowej**
Ryzyko			Średnie
Opis			Komputery kwantowe mają potencjał do łamania kryptografii kwantowej, która jest obecnie uważana za jedno z najbardziej zaawansowanych narzędzi do ochrony danych. To może stanowić zagrożenie dla bezpieczeństwa komunikacji i przechowywanych informacji. [68]
Czynniki			Czynnikiem ryzyka jest ewentualna zdolność do skutecznego atakowania algorytmów kryptograficznych, które są obecnie uważane za odporne na ataki komputerów klasycznych.
ID			**ZB8.5**
Nazwa			**Rozkładanie algorytmów kryptograficznych**
Ryzyko			Średnie
Opis			Komputery kwantowe mogą znacznie przyspieszyć proces rozkładania algorytmów kryptograficznych, co może wpłynąć na bezpieczeństwo danych i komunikacji. [69]
Czynniki			Czynnikiem ryzyka jest potencjalna zdolność tych zaawansowanych systemów obliczeniowych do efektywnego rozkładania liczby na czynniki, co mogłoby umożliwić łamanie algorytmów opartych na trudności rozkładania dużych liczb na czynniki pierwsze i potencjalnie przyspieszyć proces rozkładania, co z kolei mogłoby zagrażać bezpieczeństwu systemów kryptograficznych

1	2	3	4
ID			**ZB8.6**
Nazwa			**Ataki na infrastrukturę komunikacji kwantowej**
Ryzyko			Wysokie
Opis			Mimo, że komunikacja kwantowa zapewnia wysoki poziom bezpieczeństwa, to także wymaga zaufanej infrastruktury kwantowej. Ataki na tę infrastrukturę mogą naruszyć bezpieczeństwo komunikacji. [70]
Czynniki			Czynnikiem ryzyka jest potencjalna zdolność złamania protokołów kwantowych, co mogłoby prowadzić do zakłóceń, przechwytywania lub manipulacji przesyłanych kwantowo informacji. Infrastruktura komunikacji kwantowej bazuje na zasadach fizyki kwantowej i jest obecnie uważana za jedno z najbezpieczniejszych rozwiązań w zakresie komunikacji. Jednak superkomputery i komputery kwantowe mogą potencjalnie wprowadzić nowe zagrożenia, umożliwiając atakującym łamanie zabezpieczeń kwantowych protokołów komunikacyjnych.

1	2	3	4
ID			**ZB8.7**
Nazwa			**Złamania protokołów kwantowych**
Ryzyko			Wysokie
Opis			Teoretycznie istnieją sposoby na złamanie protokołów komunikacji kwantowej, co może skutkować naruszeniem bezpieczeństwa komunikacji. [71]
Czynniki			Czynnikiem ryzyka jest potencjalna zdolność tych zaawansowanych systemów obliczeniowych do atakowania i przełamywania zabezpieczeń stosowanych w komunikacji kwantowej, co mogłoby prowadzić do dezintegracji podstawowych mechanizmów bezpieczeństwa opartych na zasadach kwantowych. Protokoły kwantowe, takie jak kwantowe klucze kryptograficzne, opierają się na niemożliwości skopiowania informacji kwantowej oraz na zasadach nieoznaczoności kwantowej. Ewentualny postęp umożliwić złamanie tych protokołów.

Źródło: opracowanie własne

1.9. Cyfrowe modelowanie i produkcja (Digital modeling and fabrication)

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE9.1	ZT9.1	ZB9.1
Nazwa	Wysokie koszty inwestycji	Zbyt duża różnorodność oprogramowania do cyfrowego modelowania, symulacji oraz produkcji	Produkcja broni i narzędzi
Ryzyko	Średnie	Wysokie	Wysokie
Opis	Wprowadzenie systemów cyfrowego modelowania i produkcji może wymagać inwestycji w nowe technologie, oprogramowanie, sprzęt i szkolenie pracowników, co może być przyczyną poniesienia wysokich kosztów.	Obecnie na rynku możemy spotkać szereg różnego rodzaju programów komputerowych, rozwiązujących w różny sposób elementy procesu projektowania i implementowania systemów cyberfizycznych (łączących świat cyfrowy z fizycznym, z naciskiem na współpracę systemu z użytkownikiem).	Dostęp do zaawansowanych narzędzi cyfrowego modelowania i produkcji może ułatwić produkcję broni lub narzędzi wykorzystywanych w działaniach przestępczych lub terrorystycznych, co stanowi zagrożenie dla bezpieczeństwa narodowego. [72]
Czynniki	Czynnikiem ryzyka jest tutaj świadomość kadry zarządzającej dotycząca sposobów finansowania takiej inwestycji.	Dostępne programy komputerowe, wspomagające wytwarzanie innowacyjnych produktów, charakteryzują się dużą złożonością oraz jest ich bardzo wiele na rynku. Dla MŚP dużym zagrożeniem może być stosowanie narzędzi, które nie mają przełożenia na wytwarzaną wartość.	Czynnikiem ryzyka jest potencjalna łatwość i dostępność wytwarzania zaawansowanych broni lub narzędzi przy wykorzystaniu tej technologii, co może prowadzić do niekontrolowanego rozprzestrzeniania się potencjalnie niebezpiecznych środków. Dostęp do precyzyjnych planów i schematów broni czy narzędzi może być łatwiejszy.
ID	ZE9.2	ZT9.2	ZB9.2
Nazwa	Ryzyko uzależnienia się od dostawców technologii	Ograniczenie optyki i szybkości skanerów 3D	Piractwo intelektualne
Ryzyko	Wysokie	Niskie	Wysokie
Opis	W zakresie cyfrowego modelowania i produkcji istnieje duże zróżnicowanie oferty. MŚP często podejmują niewłaściwe decyzje i tym samym uzależniają się od danego dostawcy. Relacje z nieodpowiednim dostawcą technologii mogą narażać firmę na ponoszenie dodatkowyc kosztów wynikających ze zmian w warunkach umowy, awarii usług czy problemów finansowych dostawc .	Wytwarzanie przyrostowe (druk 3D) jako technologia przyjęła się doskonale nie tylko w zastosowaniach edukacyjnych ale również w codziennej praktyce MŚP. Zdecydowanie wyzwaniem dla zastosowania jest obecnie cena oraz parametry techniczne skanerów 3D, dzięki którym możliwe jest zastosowanie podejścia tzw. inżynierii odwrotnej.	Możliwość łatwego kopiowania produktów, włącznie z produktami opatrzonymi znakami towarowymi i patentami, może prowadzić do naruszeń własności intelektualnej, co może wpłynąć na gospodarkę narodową. [73]

2	2	2	2
Czynniki	Czynnikiem, który wpływa tutaj na zwiększenie ryzyka jest szeroki dostęp MŚP do technologii DMF i wybór niewłaściwego dostawcy powodowany presją walki konkurencyjnej.	Jeszcze kilka lat temu skanowanie 3D kojarzyło się z nieuczciwymi praktykami, kopiowaniem, czy wręcz próbą kradzieży wzorów użytkowych konkurencji – współcześnie jest normalnym narzędziem codziennej pracy projektantów.	Czynnikiem ryzyka jest możliwość łatwego kopiowania i rozpowszechniania chronionych prawem wzorów, produktów czy technologii, co może prowadzić do utraty dochodów dla oryginalnych twórców, przedsiębiorstw oraz naruszenia praw własności intelektualnej. Przy użyciu cyfrowego modelowania, łatwiej jest replikować przedmioty, wyroby czy konstrukcje, co zwiększa ryzyko nieautoryzowanego kopiowania i dystrybucji.
ID		**ZT9.3**	**ZB9.3**
Nazwa		**Ograniczenie technologii prototypowania**	**Wytwarzanie substancji niebezpiecznych**
Ryzyko		Niskie	Wysokie
Opis		Cena drukarek 3D wysokiej jakości cały czas stanowi barierę dla zastosowania w MŚP. Utrudnienia w dostępności technologii hybrydowych (przyrostowych z obróbką skrawaniem w ramach pojedynczego systemu produkcyjnego) stanowią jeszcze większą barierę.	Technologie cyfrowego modelowania i produkcji mogą być wykorzystywane do produkcji niebezpiecznych substancji lub materiałów wybuchowych, co stanowi zagrożenie dla bezpieczeństwa narodowego. [74]
Czynniki		Wydaje się, że kluczowym czynnikiem zagrożenia wdrażania technologii nie jest otwartość MŚP na zmianę modelu biznesowego, w którym technologie przyrostowe odgrywają coraz istotniejszą rolę a koszty wdrażania technologii.	Czynnikiem ryzyka jest potencjalna możliwość produkcji nielegalnych substancji chemicznych lub materiałów wybuchowych, co może prowadzić do zagrożenia publicznego, terroryzmu lub przestępczości zorganizowanej.
ID		**ZT9.4**	**ZB9.4**
Nazwa		**Ograniczenie mocy obliczeniowej komputerów**	**Ulepszanie broni**
Ryzyko		Wysokie	Wysokie
Opis		Symulacje komputerowe cyfrowej re-prezentacji fizycznych systemów (ang Digital Twin, Asset Administration Shell) wymagają dużych mocy obliczeniowych. Komputery, stosowane w tym aspekcie cyfryzacji muszą posiadać dedykowane karty graficzne oraz „gamingowe” proc - sory, dyski twarde, monitory.	Możliwość modyfikowania broni i tworzenia nowych projektów za pomocą cyfrowego modelowania może zwiększyć dostępność niebezpiecznych broni na rynku, co może wpłynąć na bezpieczeństwo narodowe. [75]

2	2	2	2
Czynniki		W tym konkretnym przypadku czynnikiem kształtującym ryzyko jest zignorowanie analizy wymagań sprzętowych komputerów, stosowanych w zagadnieniach cyfrowego modelowania i symulacji produkcji.	Czynnikiem ryzyka jest potencjalna możliwość łatwego dostępu do zaawansowanych projektów broni, ich modyfikacji oraz produkcji niestandardowych komponentów, co może prowadzić do powstania bardziej zaawansowanych, trudnych do kontrolowania lub przewidzenia rodzajów broni. Technologie cyfrowego modelowania umożliwiają dokładne projektowanie i produkcję broni, co stwarza ryzyko, że potencjalni aktorzy (w tym osoby prywatne czy grupy przestępcze) mogą wykorzystać tę technologię do stworzenia broni o zwiększonej skuteczności, zasięgu lub innych parametrach.
ID		**ZT9.5**	
Nazwa		**Mała liczba rozwiązań zgodnych z Asset Administration Shell**	
Ryzyko		Wysokie	
Opis		Rozwój technologii kontrolno-pomiarowych, zgodnych z filozofi Asset Administration Shell jest powolny . Tutaj nie należy upatrywać szansy we wdrażaniu podejścia przez startupy – zrobią to raczej duże firmy – producenci systemów sterowania.	
Czynniki		Duże zagrożenie wynika z uproszczenia, w myśl którego cyfrowy bliźniak (ang. Digital Twin) stawiany jest na równi z AAS (ang. Asset Administration Shell). AAS to standardowy model informacji, podczas gdy Digital Twin jest swego rodzaju koncepcją, polegającą na tworzeniu cyfrowych reprezentacji fizycznych obiektów i/lub systemó . AAS to konkretny standard, służący do reprezentacji danych o zasobach.	

Źródło: opracowanie własne

1.10. Systemy autonomiczne i robotyzacja

	Zagrożenia ekonomiczne	Zagrożenia technologiczne	Zagrożenie dla bezpieczeństwa narodowego / Bezpieczeństwo narodowe
1	2	3	4
ID	ZE10.1	ZT10.1	ZB10.1
Nazwa	Koszty inwestycji	Kontakt robotów z otoczeniem w tym ludźmi	Zastosowania militarne
Ryzyko	Wysokie	Średnie	Wysokie
Opis	Implementacja systemów autonomicznych i robotyzacji wymaga znacznych inwestycji w zakup i instalację odpowiednich technologii, szkolenie personelu, dostosowanie infrastruktury i utrzymanie systemów. Koszty te mogą stanowić wyzwanie, zwłaszcza dla MŚP.	Olbrzymim wyzwaniem a zarazem zagrożeniem dla tempa wdrażania technologii robotycznych jest ich kontakt z otoczeniem zewnętrznym. Współcześnie robotyka skupia się na zwiększaniu produktywności przy założeniu eliminacji kontaktu z otoczeniem (co nie jest niczym złym w przypadku systemów produkcyjnych).	Autonomiczne systemy wojskowe mogą stanowić zagrożenie, jeśli są używane w celach agresywnych lub niestabilnych konfliktów, co może prowadzić do eskalacji i nieprzewidywalnych skutków. [76]
Czynniki	Czynnikiem ryzyka jest świadomość i umiejętność kadry zarządzającej związana z pozyskiwaniem zewnętrznych źródeł finansowania inwestycji oraz ich planowania.	Bardzo dużym wyzwaniem jest zwiększenie stopnia współpracy maszyn autonomicznych, które w niedalekiej przyszłości mają współpracować z człowiekiem.	Czynnikiem ryzyka jest możliwość utraty kontroli nad tymi systemami, co może prowadzić do nieprzewidywalnego zachowania, błędów w identyfikacji celów czy skutków niezamierzonych, mogących eskalować konflikt . Systemy autonomiczne, takie jak autonomiczne pojazdy wojskowe czy drony, mogą być podatne na błędy w programowaniu, zakłócenia czy cyberatak, co w rezultacie może prowadzić do sytuacji, gdzie decyzje podjęte przez te systemy nie są zgodne z intencjami dowództwa lub prowadzą do niekontrolowanych działań.

1	2	3	4
ID	**ZE10.2**	**ZT10.2**	**ZB10.2**
Nazwa	**Konieczność restrukturyzacji zasobów ludzkich**	**Złożoność systemów sensorycznych, monitorujących otoczenie zrobotyzowanych linii produkcyjnych**	**Sabotaż i ataki cybernetyczne**
Ryzyko	Średnie	Średnie	Wysokie
Opis	W związku z wprowadzeniem automatyzacji i robotyzacji w przedsiębiorstwie, konieczne jest nabywanie nowych umiejętności przez pracowników w celu efektywnej współpracy z systemami automatycznymi i robotami. Może to wymagać dodatkowego szkolenia lub pozyskania nowych, wykwalifikowanych pracownikó .	Zwiększanie percepcji systemów autonomicznych w systemach produkcyjnych wiąże się z koniecznością coraz powszechniejszego zastosowania czujników przyspieszeń, temperatury, ciśnienia, emisji akustycznej, systemów wizyjnych. Rozpoznawanie mowy ludzkiej, analiza gestów, czy systemy haptyczne przestają już być „technologiami przyszłości”.	Systemy autonomiczne i robotyka są podatne na ataki cybernetyczne, które mogą zakłócić ich funkcje lub przejąć kontrolę nad nimi, co może prowadzić do potencjalnie niebezpiecznych sytuacji. [77]
Czynniki	Kluczowym czynnikiem ryzyka jest tutaj dostęp do wykwalifikowanej kadry oraz specjalistycznych szkoleń.	Do kluczowych czynników ryzyka w tym obszarze należy zaliczyć ograniczoną dostępność przemysłowych wersji czujników, wspomagających postępującą autonomizację systemów produkcyjnych.	Czynnikiem ryzyka jest potencjalna podatność tych systemów na manipulacje, zakłócenia czy przejęcie zdalne przez atakujących, co może prowadzić do utraty kontroli nad urządzeniami autonomicznymi oraz ich nieprzewidywalnego zachowania. Ataki cybernetyczne mogą skierować się zarówno na oprogramowanie, jak i na same sensory czy systemy sterowania, co stwarza ryzyko manipulacji danych czy przejęcia kontroli nad urządzeniami. W przypadku systemów autonomicznych zastosowanych w wojsku, takie ataki mogą prowadzić do niebezpiecznych sytuacji na polu walki lub w zakresie bezpieczeństwa narodowego.

1	2	3	4
ID	**ZE10.3**		**ZB10.3**
Nazwa	**Zależność od dostawców technologii**		**Wycieki technologii**
Ryzyko	Wysokie		Wysokie
Opis	W zakresie dostępności systemów autonomicznych i robotyzacji istnieje duże zróżnicowanie oferty. MŚP często podejmują niewłaściwe decyzje i tym samym uzależniają się od danego dostawcy. Relacje z nieodpowiednim dostawcą technologii mogą narażać firmę na ponoszenie dodatkowych kosztów wynikających ze zmian w warunkach umowy, awarii usług czy problemów finansowych dostawc .		Przekazywanie technologii autonomicznych lub robotycznych nieprzyjaznym państwom lub organizacjom może stanowić zagrożenie, ponieważ może to prowadzić do zwiększenia zdolności militarnych wrogów. [77]
Czynniki	Czynnikiem, który wpływa tutaj na zwiększenie ryzyka jest wybór niewłaściwego dostawcy powodowany presją walki konkurencyjnej.		Czynnikiem ryzyka jest potencjalna utrata poufnych danych, planów czy schematów związanych z tymi zaawansowanymi technologiami, co może prowadzić do ich nieautoryzowanego wykorzystania przez inne państwa, grupy przestępcze lub inne podmioty. Inne państwa mogą zdobyć istotne informacje dotyczące strategii wojskowej czy zdolności obronnej. To z kolei może osłabić przewagę militarną państwa, umożliwiając potencjalnym przeciwnikom zrozumienie i przeciwdziałanie zastosowanym technologiom.
ID			**ZB10.4**
Nazwa			**Zagrożenia w zakresie prywatności i bezpieczeństwa danych**
Ryzyko			Wysokie
Opis			Wykorzystywanie robotów i urządzeń autonomicznych do zbierania danych osobowych lub monitorowania działań może naruszać prywatność i bezpieczeństwo jednostek. [59]

1	2	3	4
Czynniki			Czynnikiem ryzyka jest potencjalne gromadzenie, przetwarzanie oraz niebezpieczne ujawnienie danych osobowych, w tym informacji dotyczących obywateli czy pracowników wojskowych, przez te zaawansowane technologie. Systemy autonomiczne, zwłaszcza w sferze militarno-obronnej, mogą zbierać duże ilości danych w czasie rzeczywistym w celu podejmowania decyzji autonomicznych. Jeśli te dane nie są odpowiednio zabezpieczone, mogą stanowić cel dla ataków na prywatność lub być wykorzystane w celach szpiegowskich.
ID			**ZB10.5**
Nazwa			**Zmiany w rynku pracy**
Ryzyko			Wysokie
Opis			Automatyzacja i robotyzacja mogą prowadzić do utraty miejsc pracy i destabilizacji rynku pracy, co może wpłynąć na bezpieczeństwo socjalne i stabilność społeczeństwa. [78]
Czynniki			Czynnikiem ryzyka jest potencjalna utrata miejsc pracy tradycyjnych, co może prowadzić do wzrostu bezrobocia, niezadowolenia społecznego oraz konieczności dostosowania systemów edukacyjnych i szkoleniowych do nowych realiów.

Źródło: opracowanie własne

2 Zalecenia i rekomendacje – podejście dedukcyjne

Budowanie rekomendacji odnośnie do przeciwdziałania zagrożeniom związanym z wprowadzaniem technologii cyfrowych do przedsiębiorstw jest podporządkowane celom nadrzędnym, jakim jest podnoszenie konkurencyjności MŚP. Prezentowane w tej części raportu rozważania mają wskazać możliwe działania po stronie firm, samorządu gospodarczego oraz polityki gospodarczej, które przyczynią się do realizacji wspomnianych celów. Zarekomendowanie konkretnych zachowań firmom oraz zaprojektowanie inicjatyw na szczeblu samorządu gospodarczego i polityki gospodarczej uczyniono odwołując się implicite do tych teorii i doktryn ekonomicznych, które są przywoływane tak przez teoretyków, jak i praktyków gospodarczych i coraz częściej stają się teoretycznymi uzasadnieniami prowadzonej polityki ekonomicznej lub stanowią podstawę strategii realizowanych przez firm. Zalecenia dla podmiotów mikroekonomicznych oparto na tezach i założeniach takich koncepcji i teorii przedsiębiorstwa, jak:

- koncepcja przedsiębiorstwa jako organizacji uczącej się,
- koncepcje strategii konkurencyjnej,
- koncepcje firmy w ramach nowej ekonomii instytucjonalnej – teoria kosztów transakcyjnych, teoria agencji, teoria praw własności,
- zasobowa teoria przedsiębiorstwa,
- koncepcja firmy w ramach teorii aglomeracji i nowej geografii ekonomiczne.

Aspekty mezoekonomiczne prowadzonych rozważań oparto na teoretycznych podstawach nowej ekonomii instytucjonalnej, nowej teorii konkurencji [79] oraz pośrednio nawiązano do idei korporatywizmu [80]. Natomiast w odniesieniu do zaleceń pod adresem polityki gospodarczej można stwierdzić, że wyraźnie pobrzmiewają w nich po pierwsze, tezy doktryny liberalnej w wersji instytucjonalnej i doktryny wspierania rynku, a po drugie, liberalno-instytucjonalnej polityki gospodarczej [81].

Obok teorii i doktryn, które stanowią podbudowę zawartych tutaj poglądów, autorzy odwołali się do swoich doświadczeń płynących ze współpracy konsultacyjnej i doradczej z MŚP. Dodatkową inspiracją były także inne obserwacje praktyczne, zawarte w publikacjach fachowych.

W najprostszym ujęciu w tej części raportu chodzi o:

- zdefiniowanie środków, których zastosowanie powinno zbudować przewagę cyfrową i zapewnić podtrzymanie tej przewagi, jeśli już została osiągnięta oraz stanowić prewencję przeciwko wystąpieniu luki cyfrowej (odnosi się do tych

wszystkich przypadków, gdzie luka cyfrowa jeszcze się nie pojawiła i nie została zdiagnozowana),

- określenie sposobów „zasypania" luki cyfrowej – albo jej likwidacji albo zmniejszenia w kierunku budowania przewagi cyfrowej w miejsce luki cyfrowej (chodzi o te wszystkie przypadki, gdzie luka cyfrowa wystąpiła i została zdiagnozowana).

Warto w tym miejscu zaznaczyć, że najlepszą prewencję przed wystąpieniem luki cyfrowej stanowi strategia, która zmierza albo do zbudowania przewagi cyfrowej albo też do jej utrzymania. De facto chodzi więc w tej części raportu o stworzenie instrumentarium służącego do zbudowania przewagi cyfrowej, utrzymania osiągniętej przewagi cyfrowej, przyjęcia strategii prewencji przed wystąpieniem potencjalnej luki cyfrowej oraz strategii przeciwdziałania realnej luce cyfrowej.

Należy podkreślić, że zaproponowane tutaj rekomendacje, aczkolwiek podają wskazane kierunki działań, to jednak nie mogą być przedmiotem bezrefleksyjnego wdrożenia w każdym przedsiębiorstwie. W tym miejscu pokazano czynniki, które należy uwzględnić przy budowie instrumentarium służącego do przeciwdziałania luce cyfrowej, natomiast konkretne recepty muszą już mieć charakter indywidualny uwzględniający specyfikę każdego przedsiębiorstwa. Właściwą perspektywą do rozpatrywania luki cyfrowej jest więc perspektywa konkretnej firmy z uwzględnieniem jej indywidualnych właściwości. Nie oznacza to, że wyklucza się możliwość wystąpienia przypadków podobnych, zbliżonych, charakteryzujących się pewnymi wspólnymi tendencjami czy prawidłowościami. Te są oczywiście możliwe, ale ostateczna strategia cyfrowa każdej firmy winna mieć jednak charakter zindywidualizowany.

2.1. Rekomendacje dla strategii przedsiębiorstw

Przedstawione w części I raportu zagrożenia związane z cyfryzacją wymagają odpowiednich dostosowań w skali mikroekonomicznej – na poziomie każdego pojedynczego przedsiębiorstwa.

W niniejszym opracowaniu założono, że luka cyfrowa jest szczególnym przypadkiem luki konkurencyjnej, stąd też punktem wyjścia do budowy rekomendacji odnośnie do „zasypania luki cyfrowej" powinny być zalecenia o charakterze bardziej ogólnym odnoszące się do likwidowania luki konkurencyjnej.

Zgodnie z przyjętym w tym opracowaniu poglądem, że zachowanie firmy w gospodarce rynkowej winno być zorientowane na osiągnięcie lub zachowanie określonego poziomu konkurencyjności, zalecenia odnośnie do zachowań MŚP można zakwalifikować do trzech grup:

- zalecenia dotyczące pozycji konkurencyjnej,
- zalecenia dotyczące potencjału konkurencyjnego,
- zalecenia dotyczące strategii konkurencyjnej.

Zawężając w tym momencie pole zainteresowań do zagadnień związanych w cyfryzacją można per analogia stwierdzić, że zachowanie firmy w gospodarce rynkowej w sferze cyfrowej winno być zorientowane na osiągnięcie lub zachowanie określonego poziomu różnicy (przewagi, luki) cyfrowej. Aby to uzyskać konieczne jest rozważenie i ewentualne wprowadzenie w życie trzech poniższych grup rekomendacji:

- zalecenia dotyczące pozycji cyfrowej,
- zalecenia dotyczące potencjału cyfrowego,
- zalecenia dotyczące strategii cyfrowej.

2.1.1. Pozycja cyfrowa

Zgodnie z przyjętym w niniejszym raporcie rozumieniem pozycji cyfrowej zabiegi firm dotyczące zajęcia pożądanej pozycji cyfrowej powinny odnosić się zarówno do rynku krajowego (wewnętrznego), jak i do rynków zagranicznych. W poniższym wywodzie uwaga zostanie zogniskowana na aspekcie pozycji cyfrowej w powiązaniu z rynkami zagranicznymi.

Zajęcie przez daną firmę możliwie najlepszej pozycji cyfrowej uwarunkowane jest przeprowadzeniem właściwej diagnozy tejże pozycji. Diagnoza winna mieć charakter indywidualny i specyficzny dla konkretnego przedsiębiorstwa. W części I raportu zaproponowano listę zmiennych/mierników, które mogą być użyteczne w punkcie wyjścia do przeprowadzenia wspomnianej diagnozy pozycji cyfrowej. Tak rozumiana pozycja cyfrowa może być opisana przez następujące zmienne:

- rentowność (relatywna, tzn. w porównaniu z konkurentami z branży) działań podejmowanych w ramach procesu cyfryzacji (stosunek osiągniętych wyników i poniesionych nakładów w związku z cyfryzacją),
- skala nakładów na cyfryzację w relacji do nakładów najważniejszych konkurentów,
- poziom kosztów cyfryzacji (relatywny w zestawieniu z głównymi konkurentami),
- cechy stosowanych technologii cyfrowych w porównaniu z cechami technologii używanych przez konkurentów,
- znajomość osiągnięć firmy i jej osiągnięć w zakresie cyfryzacji na rynku oraz związane z tym postrzeganie firmy przez otoczenie

Powyższy zestaw zmiennych ma charakter orientacyjny, kierunkowy i nie jest on oczywiście zamknięty. Może on być dowolnie rozbudowywany w zależności od sytuacji, w jakiej znajduje się konkretna rozpatrywana firma

Rekomendacje związane z pozycją cyfrową sprowadzają się do postulatu „łączenia sił", nawiązywania współpracy, podejmowania wspólnych działań w obszarze cyfryzacji w oparciu o posiadane (lub potencjalne) przewagi wynikające z lokalizacji firm w Polsce. Budowanie tak rozumianej pozycji cyfrowej winno sprzyjać wykorzystaniu korzyści skali działania w zakresie cyfryzacji w postaci niższych kosztów jednostkowych pozyskania technologii cyfrowych oraz innych zasobów potrzebnych w sferze cyfryzacji. Środkiem

umożliwiającym realizację tych korzyści może być konsolidacja pojawiających się działań cyfryzacyjnych przedsiębiorstw w większe inicjatywy, zdolne do osiągania korzystnych warunków w kontraktach cyfryzacyjnych. Tego rodzaju działania predysponują MŚP do zajmowania dobrej pozycji finansowej, która na długą metę jest warunkiem sine qua non rozwoju firm.

Realizacja omawianego zalecenia zależna jest między innymi od siły istniejących izb przemysłowo-handlowych, stowarzyszeń branżowych itp. organizacji rozwijających współpracę pomiędzy przedsiębiorstwami w różnych sferach, w tym także w sferze cyfryzacji. Ponadto wdrożenie omawianego zalecenia uwarunkowane jest stosowaną polityką konkurencji, a w szczególności ustawodawstwem antymonopolowym, którego implementacja winna mieć zrównoważony, rozważny, trzeźwy, rozsądny i wolny od demagogii charakter. Zagadnienie to dotyczy prowadzonej przez państwo szeroko rozumianej polityki gospodarczej i zostanie rozwinięte w podrozdziale 2.2. – Implikacje dla polityki gospodarczej.

Drugi dezyderat dotyczący poprawy lub obrony satysfakcjonującej pozycji cyfrowej związany jest z podejmowaniem wysiłków mających zapewnić firmie zajęcie pozycji cyfrowej określanej jako niszowa. Postulat ten jest szeroko dyskutowany w literaturze dotyczącej strategii konkurencyjnej przedsiębiorstwa. Sprowadza się on do zalecenia, aby firma starała się znaleźć na rynku niszę lub nieckę, w której będzie mogła działać w warunkach względnego monopolu. Jest to równoznaczne z jednoczesnym posia-daniem wysokiego udziału w rynku i znajdowaniem się w pozycji sprzyjającej osiąganiu dobrej sytuacji finansowej. Niektórzy autorzy uważają, że zajęcie pozycji niszowej wymaga stosowania odmiennego podejścia, w porównaniu z dwoma standardowymi, typami strategii tj. przywództwa kosztowego (wiodąca pozycja kosztowa) i strategii różnicowania [82]. Istotą strategii przywództwa kosztowego jest uzyskanie trwałej przewa-gi kosztów nad konkurentami. Niższe koszty umożliwiają oferowanie niższych cen niż inni. Z kolei istotą strategii różnicowania jest osiągnięcie przewagi różniczkowej (przewagi „inności") nad konkurentami. Oznacza to, że w jednym lub w wielu aspektach oferta danego przedsiębiorstwa różni się korzystnie (w ocenie nabywców) od innych ofert. M. E. Porter wymienia też trzeci podstawowy typ strategii: strategię koncentracji na danym segmencie rynku (fokus). O ile poprzednie dwie strategie zakładały opero-wanie przedsiębiorstwa na całym rynku branżowym, o tyle ta strategia zakłada świa-dome skupienie się na wybranym segmencie – niecce (niszy) rynkowej. Wydaje się jednak, że strategię koncentracji można uznać za specyficzny wariant strategii różnicowania lub kosztowej – przedsiębiorstwo tak kształtuje swoją strategię, aby osiągnąć przewagę różniczkową lub kosztową tylko w ocenie ograniczonej grupy nabywców (segmentu rynku).

Powyższe rozróżnienie trzech typów strategii ma w tym miejscu duże znaczenie ze względu na fakt, że każdy z typów strategii rodzi prawdopodobnie różne skutki, jeśli chodzi o rezultat procesu konkurowania, czyli zajętą lub osiągniętą w efekcie procesu konkurowania pozycję konkurencyjną. Można bowiem postawić trzy hipotezy:

1. skuteczna strategia przywództwa kosztowego sprzyja zdobyciu wysokiego udziału w rynku,

2. skuteczna strategia różnicowania powinna umożliwiać osiągnięcie dobrej sytuacji finansowej
3. skuteczna strategia koncentracji na danym segmencie rynku jednocześnie sprzyja zdobyciu wysokiego udziału w rynku i osiągnięciu dobrej sytuacji finansowej.

Trzeci typ strategii posiada więc istotne zalety, a poza tym wydaje się, że jest to typ strategii, którego przyjęcie jest realistyczne przez nowo wchodzącego na rynek zagraniczny konkurenta polskiego – nie są tutaj bowiem wymagane duże (relatywnie) nakłady inwestycyjne.

Należy tutaj podkreślić, że świadomy i uzasadniony wybór właściwej strategii dopasowanej do warunków działania konkretnego przedsiębiorstwa ma pierwszorzędne znaczenie i ma wpływ na możliwość wykorzystania takie albo innej strategii cyfryzacji.

Kolejnym ważnym zagadnieniem jest to, że zajęcie i utrzymanie właściwej pozycji cyfrowej na rynkach zagranicznych (czyli pozycji w obszarze cyfryzacji w konfrontacji z konkurentami działającymi na tych rynkach) nie powinno ograniczać się do stosowania praktycznie najbardziej popularnej strategii ekspansji na te rynki, to znaczy strategii eksportowej. Wątek ten zostanie rozwinięty w podrozdziale 2.1.3.

Powyższy wywód na temat ogólnej strategii konkurencji ma w tym miejscu uzasadnienie ze względu na fakt, iż strategia cyfryzacji jest pochodną ogólnej strategii konkurencyjnej przedsiębiorstwa i jest zazwyczaj w stosunku do niej wtórna w tym tego słowa znaczeniu, że określone pociągnięcia w sferze cyfrowej muszą być jednak podporządkowane założeniom całościowej strategii przedsiębiorstwa. Ważne jest jednak także dostrzeżenie, że realizowana całościowa strategia przedsiębiorstwa wywiera silny wpływ na strategię cyfryzacji, bowiem od wyników rynkowych i finansowych firmy zależą możliwości przeznaczania określonych nakładów na cyfryzację. Nie można także nie zauważyć, że istnieje również zależność w drugą stronę – efekty działań w sferze cyfryzacji mogą wywierać znaczący wpływ na ogólną strategię przedsiębiorstwa otwierając szansę podboju nowych rynków, zwiększania udziałów w rynkach dotychczasowych, czy wykorzystania także innych niż strategia eksportowa form obecności na tych rynkach itp. Kompetencje w dziedzinie cyfryzacji są tutaj niezbędne, a te powiązane są przecież między innymi z zajmowaną pozycją cyfrową. Można więc mówić o występowaniu swego rodzaju sprzężenia zwrotnego pomiędzy ogólną strategią przedsiębiorstwa a strategią cyfryzacji.

2.1.2. Potencjał cyfryzacyjny

Budowanie zaleceń dotyczących potencjału cyfryzacyjnego należałoby rozpocząć od przedstawienia wzorca opisującego stan pożądany w zakresie poszczególnych czynników ten potencjał wyznaczających. Zdaniem niektórych badaczy dostosowania firm na drodze do budowy optymalnego potencjału cyfryzacyjnego winny zmierzać do pewnego idealnego wzorca, którego charakterystykę przedstawiono poniżej (tabela 1).

Tabela 1. Charakterystyka zasobów składających się na idealny stan potencjału cyfryzacyjnego przedsiębiorstwa.

Sfera	Charakterystyka zasobów w dziedzinie cyfryzacji
1	2
Informacje	Wiarygodne prognozy sytuacji w zakresie cyfryzacji i kierunków jej rozwoju, określenie aktualnych i przyszłych potrzeb klientów pod kątem cyfryzacji działań naszej firmy (czego klienci/odbiorcy oczekują od nas w dziedzinie cyfryzacji? jakie są trendy rynkowe?), prognoza zachowań klientów w sferze cyfryzacji, znajomość potencjału ekonomicznego oraz strategii cyfryzacyjnych firm kon urencyjnych.
B+R	W tej sferze występuje znany dylemat – robić czy kupować (make or buy)? W przypadku większości MŚP rozwiązanie „robić w zakresie B+R w sferze cyfryzacji" nie jest możliwe do zrealizowania – posiadanie własnych komórek B+R wspomagane współpracą z ośrodkami naukowymi, wyposażenie w sprzęt najnowszej generacji, zatrudnienie ludzi o najwyższej wiedzy, doświadczeniu i kreatywności, wysokie środki finansowe, przeznaczane na ten cel – te elementy potencjału cyfryzacyjnego wymagałyby bowiem zbyt wysokich w stosunku do możliwości nakładów.
Produkcja	Cyfryzacja procesów produkcyjnych wiązałaby się ze stosowaniem następujących rozwiązań – najnowocześniejsze technologie przy użyciu maszyn i urządzeń o najwyższej jakości, nowoczesne systemy komputerowe wspomagające procesy technologicznego przygotowania produkcji oraz zarządzanie produkcją, najwyższa fachowość kadry technicznej, przygotowanej do zastosowania nowoczesnych systemów zarządzania produkcją.
Zarządzanie jakością	Cyfryzacja zarządzania jakością – pełne zaangażowanie kierownictwa i pozostałych pracowników w realizację programów zapewnienia jakości, posiadanie przez przedsiębiorstwo certyfikatów jakości, stosowanie kompleksowego systemu zarządzania jakością TQM, stosowanie systemów i procedur zapewnienia jakości.
Logistyka	Cyfryzacja logistyki – optymalizacja dostaw, np. poprzez zastosowanie metody just-in-time lub ekonomicznej partii, ale z poszanowaniem postulatów związanych z rezyliencją, posiadanie nieprzerwanego i stabilnego dostępu do źródeł zasobów (surowców), dogodna lokalizacja w stosunku do zasobów, wysoka jakość kadr.
Dystrybucja	Cyfryzacja dystrybucji – posiadanie sprawnej sieci dystrybucji o optymalnej gęstości, obejmującej swym zasięgiem cały obsługiwany rynek, najwyższa jakość kadr zajmujących się dystrybucją i sprzedażą, możliwość wpływu na kanały dystrybucji.
Marketing	Cyfryzacja marketingu – wysoka jakość kadr, możliwe najwyższe nakłady fina - sowe, pełne znajomość i umiejętność komponowania instrumentów marketing-mix, wysoka ranga marketingu w przedsiębiorstwie.
Finanse	Cyfryzacja finansów skoncentrowana na zapewnieniu następujących warunków: niski poziom kosztów całkowitych, wysoki potencjał finansow , pełen dostęp do zewnętrznych źródeł finansowania, pełne wykorzystanie instrumentów rachunkowości zarządczej, najwyższa jakość kadry zajmującej się finansami, skomputeryzowanie.

Tabela 1. cd. Charakterystyka zasobów składających się na idealny stan potencjału cyfryzacyjnego przedsiębiorstwa

1	2
Organizacja i zarządzanie	Cyfryzacja w zakresie organizacji i zarządzania zorientowana na zapewnienie następujących warunków: najwyższa jakość kadry menedżerskiej, posiadanie i realizowanie planów operacyjnych i strategicznych, system motywacji, budujący klimat pracy promujący dobrą robotę, decentralizacja zarządzania, elastyczność podejmowania decyzji, prostota i klarowność struktury organizacyjnej oraz sprawność systemów komunikacji wewnętrznej, właściwa forma organizacyjna.
Zatrudnienie	Cyfryzacja działań w zakresie zatrudnienia ze zwróceniem szczególnej uwagi na lojalność pracowników, odpowiedni poziom wykształcenia, klarowna, świadomie i konsekwentnie realizowana polityka kadrowa, skłonność pracowników do innowacji i zmian, chęć podnoszenia kwalifikacji oraz wiara w sukces rynkowy organizacji.
Zasoby niewidzialne	Cyfryzacja wspomagająca zasoby niewidzialne – wysoka renoma firm, kultura organizacyjna przedsiębiorstwa i dostrzeganie jej przez zewnętrznych partnerów, umiejętność tworzenia i posiadanie lobby sprzyjającego firmie, umiejętność przewidywania zachowań przedsiębiorstw konkurencyjnych, wykorzystanie dotychczasowych kontaktów handlowych w poszerzaniu udziału na rynku.

Źródło: adaptacja na podstawie [83] oraz [84].

Do pomiaru potencjału cyfryzacyjnego danej firmy użyteczny może być zestaw zmiennych opisujących potencjał cyfryzacyjny przedsiębiorstwa, do których przykładowo można zaliczyć:

- posiadana w firmie wiedza na temat cyfryzacji – potrzeby, trendy, tendencje, technologie itp.,
- jakość kadry kierowniczej i wykonawczej w sferze cyfryzacji,
- wyposażenie firmy w technologie cyfrowe,
- wyposażenie firmy w sprzęt służący do cyfryzacji,
- reputacja (image, renoma) firmy w zakresie cyfryzacji,
- nakłady finansowe na cyfryzację pozostające w dyspozycji firmy,
- system motywacyjny w sferze wprowadzania cyfryzacji,
- sposób zorganizowania działań w sferze cyfryzacji,
- postawy pracowników w odniesieniu do cyfryzacji,
- ranga nadawana w firmie problemom cyfryzacji.

Zaproponowany katalog mierników potencjału cyfryzacji nie ma niezmiennego charakteru i powinien być sytuacyjnie modyfikowany. Mierniki te mogą być wykorzystywane zarówno w procesie diagnozy potencjału cyfryzacyjnego, jak i w obszarze prognozowania tegoż potencjału, a ponadto może być użyteczny w definiowaniu pożądanego/zamierzonego stanu szeroko rozumianych zasobów firmy w sferze cyfryzacji, które łącznie stanowią potencjał cyfryzacyjny przedsiębiorstwa.

Tworzenie potencjału cyfryzacyjnego przez firmy powinno być procesem ciągłym, uwzględniającym zmiany w otoczeniu rynkowym. Ze względu na ograniczoność zasobów firmy winny koncentrować środki na problemach kluczowych, wynikających ze strategii rozwoju przedsiębiorstwa. Innymi słowy ograniczoność zasobów, a precyzyjniej rzecz określając – rozsądna relacja zaangażowanych zasobów do uzyskanych rezultatów – nakazuje stosowanie pewnej hierarchii ważności w budowaniu i rozwijaniu poszczególnych czynników potencjału cyfryzacyjnego, który – należy o tym stale pamiętać – nie jest bytem niezależnym, lecz jest tylko ważną częścią ogólnego potencjału konkurencyjnego przedsiębiorstwa, który obejmuje przecież także inne sfery. Zrozumiałe jest więc, że menedżerowie powinni przywiązywać różną wagę do poszczególnych czynników potencjału cyfryzacji. Warto w tym miejscu jeszcze raz przypomnieć, że w przypadku każdej firmy z osobna powinna zostać przeprowadzona diagnoza odnośnie do tego, jakie wagi menedżerowie przyznają poszczególnym miernikom potencjału cyfryzacyjnego.

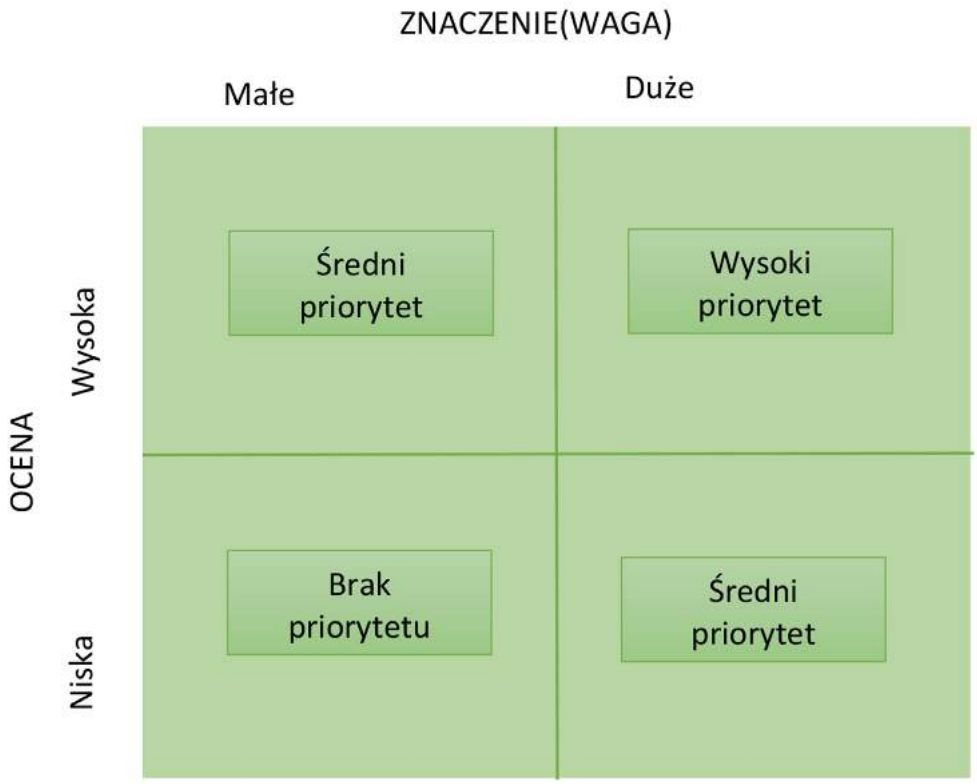
Mechaniczna interpretacja wyników uzyskanych w takiej diagnozie nakazywałaby wystąpienie z rekomendacją, że polskie MŚP winny posługiwać się w budowaniu potencjału cyfryzacji ustaloną w drodze diagnozy hierarchią ważności składników potencjału cyfryzacyjnego. Dodatkowym czynnikiem, który powinien być brany pod uwagę winny być także wyniki oceny sytuacji w obrębie poszczególnych czynników cyfryzacji w badanych przedsiębiorstwach. Czym innym jest bowiem ranga ważności przypisywana danemu czynnikowi, a czym innym ocena sytuacji występującej w zakresie tego czynnika.

Po raz kolejny trzeba przypomnieć o indywidualnym co do istoty charakterze oceny ważności oraz oceny sytuacji w zakresie poszczególnych czynników/zasobów potencjału cyfryzacji. Nawet gdyby udało się przeprowadzić rozległe badania statystyczne w obrębie reprezentacyjnej grupy MŚP (na potrzeby tego raportu badań takich nie prowadzono), to i tak nie byłoby rozsądne formułowanie kategorycznych zaleceń dla wszystkich przedsiębiorstw, a w szczególności uproszczone mechaniczne wcielenie w życie sformułowanych zaleceń w odniesieniu do każdej indywidualnej firmy. Nie istnieje bowiem mechaniczny algorytm przekładający uśrednione wyniki populacji przedsiębiorstw biorących udział w badaniu statystycznym na jednoznaczne rekomendacje dla poszczególnych, indywidualnych firm, zarówno należących do próby badawczej, jak i znajdujących się poza nią. Uzyskane wyniki badań mogłyby być co najwyżej zostać wykorzystane w następujących celach:

- inspiracja i zachęta do przeprowadzenia badań zorientowanych na praktyczne potrzeby poszczególnych przedsiębiorstw – wydaje się, że badania o nastawieniu praktycznym, użytecznym dla kreowania strategii poszczególnych firm powinny dotyczyć populacji przedsiębiorstw działających w określonej branży,
- punkt wyjścia do operacjonalizacji zmiennych charakteryzujących konkurencyjność przedsiębiorstwa, który uwzględnienie w przypadku konkretnej branży byłoby najbardziej uzasadnione,
- punkt odniesienia dla wyników uzyskanych w odniesieniu dla przedsiębiorstw należących do konkretnej branży i podstawa do refleksji na temat odmienności w danej branży w porównaniu z szerszą, zróżnicowaną branżowo populacją przedsiębiorstw.

Zaleceniem, które można zbudować na podstawie przeprowadzonych badań, jest postulat prowadzenia w obrębie poszczególnych przedsiębiorstw systematycznych i wnikliwych analiz ich sytuacji cyfrowej (pozycji cyfrowej, potencjału cyfrowego i strategii cyfrowej-instrumentów cyfryzacji), przede wszystkim na tle branży, w której dane firmy działają. Należy dokonywać diagnozy i monitorowania poglądów na temat ważności poszczególnych czynników potencjału cyfrowego wśród kluczowych pracowników danej firm, a następnie poglądy te winno konfrontować się z wynikami dla całej branży lub wybranych jej przedstawicieli (np.: głównych konkurentów, liderów rynku, itp.).

Przy podejmowaniu praktycznych działań dotyczących budowy potencjału cyfrowego należałoby przestrzegać zasady, aby realizowanym posunięciom nadawać pewne priorytety. W pierwszej kolejności należałoby zwracać uwagę na te czynniki potencjału cyfrowego, które oceniane są jako ważne (mają dużą wagę, duże znaczenie dla osiągnięcia przewagi cyfrowej) i w obrębie których luka cyfrowa (dystans dzielący daną firmę od rywali) jest największa. Drugi priorytet powinny mieć czynniki ważne, ale z niewielką luką oraz czynniki mniej ważne, ale z dużą luką. Najmniej uwagi powinno się natomiast poświęcać czynnikom mało ważnym i charakteryzującym się małą luką. Zaproponowaną koncepcję hierarchii działań w obrębie potencjału konkurencyjnego można ująć w postaci poniższej dwuwymiarowej macierzy znaczenia(wagi)-oceny czynników potencjału cyfrowego (Rysunek 1).



Rysunek 1. Macierz znaczenia (wagi) i oceny czynników potencjału cyfrowego/cyfryzacji

Źródło: opracowanie własne.

2.1.3. Strategia cyfrowa

Optymalna konfiguracja zasobów firmy w sferze cyfryzacji konstytuuje potencjał cyfrowy (potencjał cyfryzacji). Samo posiadanie dobrego potencjału cyfryzacji jednak nie wystarcza. Jego wykorzystanie na konkurencyjnym rynku wymaga stosowania odpowiednich instrumentów cyfryzacji, czyli realizacji określonej strategii cyfryzacji. Jak podniesiono to wcześniej firmy mają do wyboru trzy, a właściwie dwa „czyste" typy strategii konkurencyjnej (w praktyce strategia przedsiębiorstwa jest mieszanką elementów wywodzących się z tych typów i ma najczęściej charakter eklektyczny):

- strategia przywództwa kosztowego,
- strategia różnicowania,
- strategia koncentracji uwagi na określonym segmencie rynku (uważa się, że jest to szczególny przypadek pierwszego lub drugiego typu strategii).

Identyfikacja podstawowych cech dwóch „czystych" typów strategii konkurencyjnej stanowi jedną z podstaw budowania zaleceń normatywnych odnośnie do pożądanej strategii firm polskich w związku z konkurowaniem na rynkach zagranicznych i na względnie otwartym rynku krajowym.

Zamieszczony w p. 2.1.1. wywód dotyczący wiodących cech dwóch podstawowych typów strategii konkurencyjnej (strategii przywództwa kosztowego i strategii różnicowania) wskazuje na konieczność jasnego, w miarę jednoznacznego „zdeklarowania" się firmy konkurującej na danym rynku w kwestii wyboru realizowanej strategii. Uważa się bowiem, że sukces rynkowy odnoszą tylko te przedsiębiorstwa, które postawiły na jedną z podstawowych strategii konkurencyjnych. Niezdecydowanie, z wyjątkiem nielicznych przypadków, grozi „ugrzęźnięciem" między strategiami i zazwyczaj kończy się niepowodzeniem.

„Nieokreśloność" strategiczna firm polskich rywalizujących na rynkach zagranicznych, a także na rynku polskim może być znaczącym ograniczeniem dla poprawy ich konkurencyjności. Coraz częściej wskazuje się na występowanie wśród menedżerów MŚP poważnej obawy, że istotnym, potencjalnym zagrożeniem dla konkurencyjności firm polskich może być obniżenie konkurencyjności cenowej na rynkach zagranicznych na skutek wzrostowego wyrównywania się poziomu cen w Polsce i w UE, a także w szerszym otoczeniu. Wynika z tego rekomendacja, aby w realizowanych strategiach konkurencyjnych przesuwać punkt ciężkości z konkurencji kosztowej na konkurencję poprzez różnicowanie.

Drugi postulat, jaki nasuwa się po uważnym przestudiowaniu cech obu typów strategii konkurencyjnej, sprowadza się do skonstatowania, że możliwość osiągnięcia niektórych przewag konkurencyjnych, jakie stwarzają te strategie, implikuje konieczność wyjścia poza tradycyjne i dotychczas dominujące formy ekspansji firm polskich na rynki zagraniczne – czyli poza eksport pośredni lub bezpośredni. Rozwijanie eksportu jest uważane w teorii internacjonalizacji firmy za oczywisty, pierwszy etap ekspansji na rynki zagraniczne. Ograniczanie się na dłuższą metę tylko do eksportu może być jednak przejawem krótkowzroczności menedżerów. Menedżerowie często uważają, że kultywowanie i podtrzymywanie ewentualnych pierwszych sukcesów osiągniętych w obsza-

rze tego sposobu ekspansji zagranicznej powinno prowadzić tylko do dalszego rozwoju eksportu. Równie często brakuje świadomości możliwości, a czasami także zasobów do podjęcia bardziej zaawansowanych form internacjonalizacji, a w szczególności zagranicznych inwestycji bezpośrednich. Czynnikiem pośrednio świadczącym o korzyściach z dokonywania zagranicznych inwestycji bezpośrednich są sukcesy licznych inwestorów zagranicznych na rynku polskim.

Ogólny, generalny postulat, jaki można zgłosić pod adresem firm polskich, a w szczególności firm z tzw. polskim rodowodem, to konieczność dalszej i przyspieszonej restrukturyzacji ich działalności pod kątem ich dostosowania do wymagań konkurencyjnego rynku. Wspólną cechą spotykanych w literaturze definicji jest podkreślenie, że restrukturyzacja oznacza radykalną zmianę, dostosowanie o charakterze gruntownym i kompleksowym. Ważne jest też wskazanie na konieczność wzajemnego dopasowania przedsiębiorstwa i otoczenia, w którym ono działa. Należy też zauważyć, że niektóre firmy mają już za sobą niejednokrotnie zakończone sukcesem radykalne, czasami dotkliwe w skutkach postępowania restrukturyzacyjne i w ich wypadku lepszym rozwiązaniem będzie elastyczne i ewolucyjne harmonizowanie ich działalności ze zmianami zachodzącymi w otoczeniu, czy wręcz wywieranie wpływu na otoczenie.

W przypadku stwierdzenia różnic w potencjale konkurencyjnym danego przedsiębiorstwa i jego głównych rywali można mówić o występowaniu luki konkurencyjnej. Proces restrukturyzacji przedsiębiorstwa powinien zmierzać do zlikwidowania lub zniwelowania tej luki. Na podstawie rozlicznych wyników badań dostępnych w źródłach literaturowych można stwierdzić, że procesy restrukturyzacyjne podejmowane w polskich przedsiębiorstwach winny zmierzać do zlikwidowania następujących rodzajów luk: luka technologiczna, luka inwestycyjna, luka badawczo-rozwojowa, luka innowacyjna, luka majątkowa, luka kadrowa, luka edukacyjna, luka marketingowa, itp. Szczególnym, jeszcze bardziej zawężonym i specyficznym rodzajem luki jest rozpatrywana tutaj luka cyfrowa.

Do przeprowadzenia diagnozy rozmiarów luki w obrębie strategii cyfryzacji można wykorzystać zestaw wskaźników zaproponowany w części I niniejszego raportu. Zestaw instrumentów konkurowania składających się na strategię cyfryzacji może obejmować, takie składniki jak:

- kompatybilność rozwiązań w zakresie cyfryzacji z potrzebami dostawców i klientów oraz konsumentów,
- elastyczność dostosowywania w czasie rozwiązań cyfrowych do potrzeb odbiorców,
- podnoszenie poziomu nowoczesności wykorzystywanych technologii cyfrowych,
- zapewnienie potencjalnym kooperantom dobrego dostępu do wykorzystywanych rozwiązań cyfrowych (informacji itp.),
- szerokość asortymentu stosowanych narzędzi cyfryzacji dopasowana do potrzeb rynku,
- reklama i promocja kompetencji cyfrowych stosowanych przez przedsiębiorstwo,
- zakres świadczonych usług okołosprzedażownych (w tym szkoleniowych) w zakresie cyfryzacji oraz ceny tychże usług,

- warunki płatności za świadczone usługi cyfrowe, rozbudzanie nieznanych dotychczas potrzeb odbiorców (kreowanie potrzeb) w zakresie świadczonych usług cyfrowych.

Warto jednocześnie podkreślić, że sposoby likwidacji rozmaitych luk, wliczając w to lukę cyfrową, mają z perspektywy zarządzania strategicznego wiele cech wspólnych. Część wymienionych luk ma charakter podobny dla różnych przedsiębiorstw i różnych branż. Część ma natomiast charakter specyficzny. Wydaje się, że nawiązanie współpracy pomiędzy polskimi firmami mogłoby być obiecującym środkiem do zidentyfikowania, zbadania i pomiaru tych luk. Przynajmniej część luk można by także próbować usunąć wspólnymi siłami. Jest to dotychczas niezbyt dobrze zagospodarowany obszar współpracy w ramach samorządu gospodarczego, izb przemysłowo-handlowych, stowarzyszeń branżowych, itp. działających w polskiej gospodarce.

Obiecującym instrumentem, dającym się wykorzystać do zmniejszania lub zlikwidowania luki konkurencyjnej, w tym także w szczególności luki cyfrowej/cyfryzacyjnej, mogą być koncepcje zarządzania strategicznego, a w szczególności jego składnik – planowanie strategiczne. Pojawiające się sceptyczne opinie odnośnie do zarządzania strategicznego negują nie tyle jego istotę i praktyczną przydatność, ile zbytni technokratyzm, formalizm i zmechanizowanie niektórych metod. Wiele argumentów przemawia jednak za tym, żeby planować. Pożytki płynące z planowania strategicznego są następujące:

- planowanie strategiczne umożliwia wzajemne dopasowanie firmy otoczenia,
- wymusza dokonanie całościowej analizy otoczenia i kompleksowej analizy wnętrza firm,
- daje możliwość osiągnięcia dopasowania prospektywnego /dynamicznego/,
- wyznacza kierunki i cele przyszłych działań firm, porządkuje krótkookresowe działania firm,
- pozwala lepiej przewidywać zagrożenia i wykorzystywać szanse,
- firm, które planują strategicznie wypadają przeciętnie lepiej,
- w firmach z rozdzieloną własnością i zarządzaniem jest to standard działania.

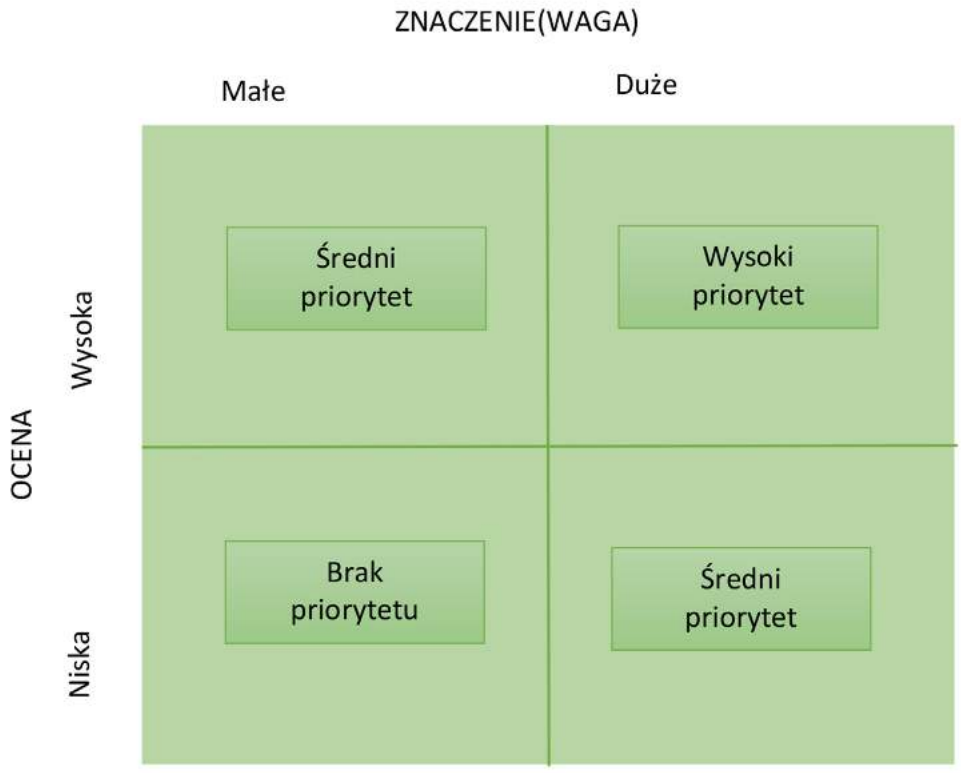
Niestety planowanie strategiczne wiąże się też z pewnymi uciążliwościami. Lista trudności i kłopotów z planowaniem strategicznym jest następująca:

- planowanie strategiczne zabiera dużo czasu i wysiłku,
- planowanie strategiczne usztywnia funkcjonowanie firm,
- w tym rodzaju planowania występuje duży margines błędu,
- planowanie strategiczne niekiedy traktowane jest jako atrapa, wykazująca, że w firmie coś się dzieje.

Wiele przesłanek wskazuje na to, że planowanie strategiczne traktowane jest często jako sfera umiejętności niezwykle rzadkich i bardzo skomplikowanych. Konieczne jest odmitologizowanie planowania strategicznego.

Przechodząc do prezentacji bardziej konkretnych zaleceń dotyczących zmniejszenia luki cyfryzacyjnej w zakresie instrumentów cyfryzacji, należy zauważyć, że najlepszą podstawę do budowy rekomendacji stanowi dobre rozpoznanie niedomagań w tej sferze. Podobnie jak w przypadku rozważania potencjału cyfryzacyjnego, tak i tutaj konieczne jest przeprowadzenie diagnozy, służącej ocenie zbioru instrumentów cyfryzacji. Należy tego dokonać indywidualnie w każdej firmie. Ewentualnie zebrane zbiorcze wyniki nie upoważniają do wysuwania uniwersalnych recept dla szerszej populacji przedsiębiorstw. Konieczne są badania porównawcze sytuacji w poszczególnych branżach i w pojedynczych firmach i podejmowanie decyzji na podstawie indywidualnych i szczegółowych uwarunkowań. Znaczenie uzyskanych wyników badawczych można – podobnie jak w przypadku potencjału cyfryzacyjnego – rozpatrywać w kategoriach inspiracji i zachęty do dalszych studiów, dostarczenia podstaw metodycznych tych studiów oraz punktu odniesienia dla następnych, bardziej zindywidualizowanych rezultatów.

Analogicznie jak w przypadku potencjału cyfryzacji w formułowaniu operacyjnych programów zmniejszenia (likwidacji, zamknięcia) luki cyfrowej w zakresie instrumentów cyfryzacji, dla nadania podejmowanym działaniom stosownej hierarchii ważności użyteczna może być macierz znaczenia (wagi) i oceny sytuacji w zakresie instrumentów konkurowania. Macierz tę przedstawiono na poniższym rysunku (Rysunek 2).



Rysunek 2. Macierz znaczenia (wagi) i oceny instrumentów cyfryzacji

Źródło: opracowanie własne.

Podsumowując zamieszczone w tym podrozdziale uwagi dotyczące pozycji cyfrowej, potencjału cyfrowego i instrumentów cyfryzacji należy zwrócić uwagę na problem związany z prowadzeniem przez przedsiębiorstwa działalności na różnych rynkach. Firmy takie stają przed dylematem standaryzacji-różnicowania strategii (instrumentów konkurowania), standaryzacji-różnicowania zasobów i umiejętności oraz pozycji konkurencyjnych na różnych rynkach. Gdy firma działa na różnych rynkach, to różne mogą być strategie konkurencyjne, czyli kombinacje instrumentów konkurowania prowadzące do osiągnięcia przewagi konkurencyjnej – pojawia się więc hipoteza odmienności strategii. Hipoteza odmienności strategii rodzi hipotezę zróżnicowania wymogów zasobowych i umiejętności potrzebnych do zastosowania określonych instrumentów konkurowania, czyli do wdrożenia określonych strategii konkurencyjnych. Można więc mówić o występowaniu w przedsiębiorstwach działających na wielu rynkach swego rodzaju „rozdarcia" albo „schizofrenii" strategiczno-zasobowej – z jednej strony występują czynniki przemawiające za unifikacją i standaryzacją, a z drugiej strony – za różnicowaniem i dostosowaniem do specyfiki oddzielnych rynków. W pierwszym przypadku rozwiązaniem jest realizacja strategii globalnej, a w drugim – strategii multilokalnej.

Na zakończenie tego punktu raz jeszcze należy podkreślić, że zagregowane (obejmujące swoim zakresem określoną populację przedsiębiorstw) studia sytuacji i luki cyfrowej mogą być zaledwie punktem wyjścia do budowy zaleceń normatywnych pod adresem konkretnych, pojedynczych przedsiębiorstw. Dokonując generalizacji wniosków i tym bardziej generalizacji rekomendacji pod adresem przedsiębiorstw należy zwracać uwagę na to, aby nie stracić z pola widzenia specyfiki ich jednostkowych sytuacji i tożsamości strategicznej. Po badaniach międzysektorowych, sektorowych, branżowych itp. winny następować precyzyjne, zindywidualizowane i „skrojone na miarę" studia konkurencyjności poszczególnych przedsiębiorstw. Wśród przesłanek, które wydają się być wystarczającymi argumentami za prowadzeniem zindywidualizowanego samodzielnego badania sytuacji konkurencyjnej w zakresie cyfryzacji można wymienić następujące:

- prowadzenie pomiaru pozwala ocenić znaczenie poszczególnych elementów potencjału cyfryzacyjnego i instrumentów cyfryzacji dla osiągania przez przedsiębiorstwo przewagi konkurencyjnej w zakresie cyfryzacji – wyznaczyć krytyczne czynniki / obszary sukcesu;
- umożliwia to przedsiębiorstwu diagnozę obszarów i rozmiaru własnego niedopasowania, czyli oszacowanie wielkości luki w obrębie poszczególnych elementów potencjału i instrumentów cyfryzacji oraz ich konfiguracji, na tle konkurentów, a także ocenę znaczenia luk w poszczególnych obszarach dla przyszłości przedsiębiorstwa, wartościowanie ich wpływu;
- pomiar pozycji cyfrowej pomaga w podejmowaniu decyzji operacyjnych i strategicznych, zmierzających do likwidacji lub ograniczenia rozmiarów luki cyfrowej;
- regularne badania wymuszają podejmowanie selektywnych działań naprawczych – w tych obszarach luki, gdzie są najbardziej potrzebne;

- są także podstawą do stworzenia praktyki monitoringu tych problemów w przedsiębiorstwie, ukształtowania świadomości znaczenia takiej praktyki oraz zdobywania niezbędnych umiejętności badawczo-analitycznych, doświadczenia potrzebnego do ciągłego, świadomego tworzenia odpowiednio elastycznego potencjału cyfrowego i doboru instrumentów cyfryzacji umiejętnie ten potencjał wykorzystujących.

2.2. Implikacje dla polityki gospodarczej

Poniżej zarysowano na zasadzie haseł kierunkowe wskazania dla polityki gospodarczej sformułowane w drodze dedukcyjnej[1]. Zasadniczą tezę w prezentowanym tutaj podejściu stanowi pogląd, że podstawę do możliwości realizowania efektywnych i skutecznych strategii cyfrowych stanowi silna baza przedsiębiorstw albo innymi słowy silna tkanka firm, nastawionych na ekspansję, rozwój i podwyższanie konkurencyjności. Ekspansja, rozwój i konkurencyjność winny odnosić się nie tylko do rynku krajowego, ale także do rynków zagranicznych. Polityka gospodarcza powinna więc sprzyjać budowaniu wyrazistej i cechującej się coraz większym potencjałem ekonomicznym populacji przedsiębiorstw z powodzeniem rywalizujących z konkurentami zagranicznymi zarówno na rynku krajowym, jak i na rynkach międzynarodowych.

Zestaw ogólnych zaleceń dla polityki gospodarczej obejmuje w związku z tym następujące działania:

- Pobudzanie współpracy:
  - polityka konkurencji, w tym prokonkurencyjna regulacja sektorowa,
  - wspieranie wszelkiego rodzaju projektów realizowanych przez firmy w kooperacji z instytucjami badawczo-naukowymi i z zaplecza edukacji,
  - pomoc w nawiązywaniu relacji z jednostkami naukowymi i badawczo-naukowymi (tzw. match-making),
  - promowanie powiązań z uniwersytetami,
  - regulacje ochrony patentowej.
- Pobudzanie przedsiębiorczości:
  - środki oddziałujące na kapitał ludzki poprzez wspieranie wszelkiego rodzaju szkoleń dla pracowników, którzy potencjalnie mogą stać się twórcami firm odpryskowych,
  - właściwy kształt prawa pracy zachęcający do tworzenia własnych firm,
- Pozytywne nastawienie do inwestorów zagranicznych,
- Dbałość o dostęp do rynku krajowego dla firm zagranicznych oraz o dostęp do rynków zagranicznych dla firm krajowych – polityka traktatowa,
- Udział w procesie regulacji rynku dla AI (regulacje UE i krajowe), w tym wdrażaniu założeń „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020” [37],

32 Uzupełnieniem zastosowanego tutaj podejścia dedukcyjnego powinno stać się zidentyfikowanie dobrych praktyk zastosowanych w realizowanych instrumentach polityki gospodarczej, zorientowanych na budowanie postępu w zakresie cyfryzacji. Kilka przykładów takich praktyk podano w dalszej części raportu.

- Aktywnaj rola w procesie standaryzacji nowych technologii, w tym:
  - Adopcji standardu RAMI 4.0 na gruncie krajowym,
  - Popularyzacji standardów projektowania map transformacji cyfrowej z zastosowaniem audytu metodą ADMA,
- Wprowadzenie regulacji ograniczających uzależnienie od zagranicznych łańcuchów dostaw w obszarach kluczowych dla bezpieczeństwa narodowego,
- Obniżanie ryzyka związanego z działalnością na rynkach zagranicznych – umowy o ochronie inwestycji, zapobieganiu podwójnemu opodatkowaniu, itp.
- Rozwijanie ubezpieczeń kredytów i kontraktów eksportowych,
- Zabezpieczenie kluczowych sektorów gospodarki poprzez ustanowienie środków regulacyjnych chroniących kluczowe gałęzie przedsiębiorstw przed wykupem lub kontrolą ze strony podmiotów zagranicznych, które mogłyby zagrażać bezpieczeństwu narodowemu,
- Wdrożenie mechanizmów kontroli inwestycji zagranicznych w sektorach kluczowych dla bezpieczeństwa narodowego, takich jak infrastruktura krytyczna czy technologie związane z obronnością,
- Wdrożenie polityki inwestycyjnej, która uwzględnia aspekty bezpieczeństwa narodowego, szczególnie w obszarach związanych z nowymi technologiami,
- Popularyzacja idei przywództwa technologicznego – szkolenie liderów, promocja najlepszych rozwiązań, wprowadzenie systemu wyzwań technologicznych dla rozwiązywania problemów na styku gospodarka – społeczeństwo,
- Rozwój kompetencji cyfrowych – pracowników oraz managerów:
  - Kompetencji w zakresie programowania,
  - Kompetencji w zakresie Big-Data i Data-Science,
  - Kompetencji w zakresie wizualizacji danych,
- Intensyfikacja współpracy między sektorem publicznym a prywatnym w dziedzinie badań i rozwoju technologii związanych z cyberbezpieczeństwem,
- Intensyfikacja współpracy z partnerami międzynarodowymi w celu zwalczania kradzieży technologii i nieuczciwej konkurencji,
- Promowanie rozwoju krajowych źródeł dostaw, zwłaszcza w obszarach związanych z bezpieczeństwem narodowym,
- Opracowanie i wdrożenie ogólnokrajowego programu mającego na celu zidentyfikowanie i zwalczanie zagrożeń związanych z nowymi technologiami,
- Utworzenie specjalnych jednostek odpowiedzialnych za nadzór nad cyberbezpieczeństwem w sektorach kluczowych gospodarki,
- Zapewnienie odpowiedniej jakości infrastruktury dla kluczowych procesów (w tym własnych),
- Krzewienie postaw etycznych w wykorzystaniu i wdrażaniu technologii,
- Rozwijanie krajowych źródeł dostaw, zwłaszcza w obszarach związanych z nowymi technologiami.

2.3. Zalecenia dla samorządu gospodarczego

Obok działań indywidualnych w zakresie przeciwdziałania luce cyfrowej, podejmowanych przez poszczególne przedsiębiorstwa oraz oprócz rozwijania powiązań między firmami, warte rozważenia jest także prowadzenie współpracy w ramach instytucji samorządu gospodarczego oraz z instytucjami samorządu gospodarczego. Organizacje tego typu mogą spełniać bardzo pożyteczne funkcje, choć niestety dość ograniczona jest skłonność przedsiębiorstw do wspólnego działania we własnym interesie oraz artykułowania własnych interesów za pośrednictwem tego typu organizacji. Argumenty uzasadniające taką postawę na pewno istnieją i są różne. W warunkach pomyślnej koniunktury na rynku przedsiębiorstwa są przede wszystkim skoncentrowane na obsłudze napływających zamówień i nie są zainteresowane wchodzeniem w interakcje, które nie dotyczą bezpośrednio ich bieżącej aktywności. Badania pokazują, że w warunkach dobrej koniunktury w branży firmy nie są zainteresowane wspólnymi działaniami na rzecz poprawy swojej konkurencyjności. Wysuwa się też tezę, że firmy próbujące globalizować swoją aktywność mają coraz większe wymagania, jeśli chodzi o jakość lokalnego otoczenia, ale przejawiają coraz mniejszą skłonność do angażowania się w aktywność samorządu gospodarczego oraz innych instytucji otoczenia biznesu. Niektórzy autorzy wskazywali także na niską skłonność przede wszystkim dużych, międzynarodowych przedsiębiorstw do współpracy w ramach inicjatyw lokalnych.

Niezbyt przychylne nastawienie do kooperacji z samorządem gospodarczym jest charakterystyczne również dla części polskich MŚP. Działania samorządu gospodarczego są zazwyczaj oceniane jako przydatne, ale niestety słabo realizowane, co może częściowo wyjaśniać ich niechęć do kooperacji ze wspomnianymi instytucjami.

Tymczasem działania lokalnych instytucji reprezentujących samorząd gospodarczy, mogą wspierać wysiłki przedsiębiorstw nakierowane na poprawę konkurencyjności, w tym między innymi w zakresie „zasypywania" luki cyfrowej. Zdaniem autorów, zestaw pożądanych inicjatyw po stronie samorządu gospodarczego, które będą sprzyjały eksploatacji pożytków związanych ze współpracą przedsiębiorstw obejmuje wszelkie działania nakierowane na:

- niwelowanie barier dla lokalnej przedsiębiorczości, które obejmują nadmierne przeciążenie firm obowiązkami pozyskiwania różnego typu pozwoleń na prowadzenia aktywności gospodarczej i rejestracji ich działalności – pomoc samorządu w tym zakresie może przyczynić się do zwiększenia liczby podmiotów gospodarczych oraz wzmocnienia ich łącznego potencjału, co może wpłynąć na wzrost możliwości „zasypywania" luki cyfrowej,
- reprezentowanie zrzeszonych firm wobec lokalnych, narodowych i międzynarodowych organów władzy oraz instytucji regulujących ład gospodarczy – głos samorządu w sprawach cyfryzacji może stać się tym samym silniejszy od głosu indywidualnych i rozproszonych MŚP,
- rozbudowę zasobów informacyjnych przedsiębiorstw w działających w instytucjach samorządu gospodarczego i likwidację asymetrii informacji pomiędzy aktorami gry rynkowej w zakresie cyfryzacji,

- świadczenie za pomocą wyspecjalizowanych jednostek usług doradczych i szkoleniowych odnoszących się do przygotowania i wdrażania strategii cyfryzacji,
- pobudzanie współpracy między członkami instytucji samorządu gospodarczego w dziedzinach, w których ujawniają się wspólne interesy potencjalnych kooperantów w zakresie cyfryzacji,
- tworzenie otoczenia, które będzie sprzyjało i ułatwiało nawiązywanie relacji przez firmy lokalne z rynkiem międzynarodowym – szczególną rolę w budowaniu zwiększonej konkurencyjności warunkującej ekspansję na rynki zagraniczne mogą odegrać technologie cyfrowe,
- ustanawianie dedykowanych grup roboczych lub komisji ds. bezpieczeństwa cyfrowego w ramach samorządu gospodarczego, skupiających ekspertów z zakresu cyberbezpieczeństwa; organizacja regularnych spotkań i konferencji, na których eksperci będą dzielić się wiedzą na temat najnowszych zagrożeń,
- zachęcanie samorządów do wspólnego podejmowania działań przeciwdziałających zagrożeniom cyfrowym, zwłaszcza w obszarze wymiany informacji na temat incydentów bezpieczeństwa i organizowanie warsztatów i szkoleń skierowanych do przedsiębiorstw, które promują wspólną obronę przed cyberatakami,
- ustanawianie systemów monitorowania bieżących ryzyk związanych z technologiami cyfrowymi i dostarczanie bieżących raportów oraz analiz dla przedsiębiorstw działających na danym obszarze samorządu gospodarczego,
- współpraca z agencjami bezpieczeństwa narodowego na terenie samorządu w celu uzyskiwania informacji dotyczących potencjalnych zagrożeń. wspieranie MŚP poprzez organizację konsultacji z ekspertami ds. cyberbezpieczeństwa, którzy pomogą dostosować strategie bezpieczeństwa do aktualnych standardów i najlepszych praktyk, w tym tworzenie puli specjalistów ds. bezpieczeństwa, do których firm mogą się zwracać w przypadku wątpliwości czy sytuacji krytycznych,
- zachęcanie do nawiązywania partnerstw publiczno-prywatnych w obszarze cyberbezpieczeństwa, w których samorząd gospodarczy współpracuje z agencjami rządowymi, aby wzmocnić ogólną odporność na cyberzagrożenia, co ułatwi wymianę informacji między sektorem prywatnym a publicznym w kontekście cyberbezpieczeństwa,
- opracowywanie planów reagowania na sytuacje kryzysowe związane z bezpieczeństwem cyfrowym, obejmujących procedury działania, komunikację kryzysową i przywracanie działalności po incydentach, a nawet organizowanie regularnych ćwiczeń symulacyjnych, aby ocenić gotowość i skuteczność planów reagowania,
- udzielanie wsparcia prawno-konsultacyjnego dla MŚP w zakresie cyberprawa, zwłaszcza w przypadkach związanych z incydentami bezpieczeństwa,
- promowanie innowacji zgodnych z normami bezpieczeństwa oraz etycznego wykorzystania technologii.

3 Zalecenia i rekomendacje – podejście indukcyjne bazujące na studiach przypadków

Rekomendacje odnośnie do przeciwdziałania zagrożeniom związanym z wprowadzaniem technologii cyfrowych oraz „zasypania" luki cyfrowej MŚP sformułowane w drodze dedukcyjnej zaprezentowano w rozdziale 2. W poniższych rozważaniach natomiast w drodze indukcyjnej, autorzy podjęli próbę identyfikacji najlepszych praktyk oraz wyodrębnienia kluczowych obszarów, które wymagają szczególnej uwagi w kontekście eliminacji luki cyfrowej na podstawie studiów przypadków przedsiębiorstw wdrażających strategię cyfryzacji oraz doświadczenia eksperckiego autorów zbudowanego w ramach realizacji projektów o charakterze analityczno-doradczym.

Celem tego rozdziału jest przede wszystkim dostarczenie praktycznych wskazówek, które pozwolą polskim MŚP skutecznie radzić sobie z wyzwaniami związanymi z transformacją cyfrową. Autorzy skupili badania wokół identyfikacji zarówno sukcesów, jak i wyzwań/zagrożeń, jakie mogą napotkać przedsiębiorstwa podczas eliminacji luki cyfrowej. Na tej podstawie opracowane zostały kompleksowe zalecenia, które mogą stanowić inspirację dla innych firm pragnących skutecznie przyspieszyć swój rozwój poprzez pełne wykorzystanie potencjału nowoczesnych technologii.

Studia przypadków, które stanowią źródło inspiracji dla przedstawianych zaleceń, pozwoliły zgłębić różnorodne doświadczenia polskich MŚP w procesie przejścia na nowoczesne rozwiązania cyfrowe. Na podstawie przykładów udanych transformacji cyfrowych prezentowanych przez Fundację Platforma Przemysłu Przyszłości [85] możliwe jest zidentyfikowanie potencjalnych zagrożeń towarzyszącym procesom cyfryzacji oraz zaproponowanie rekomendacji dla podmiotów podążających tą drogą.

Studia przypadków obejmowały wdrażanie różnych technologii cyfrowych, z których najczęściej podejmowane działania łączyły się z zastosowaniem: Internetu Rzeczy (IoT), automatyzacji i robotyzacji procesów, rozwiązań chmurowych, analityki Big Data oraz rozszerzonej rzeczywistości (AR), sztucznej inteligencji (AI). Podejmowane transformacje dotyczyły przedsiębiorstw z różnych branż tj.: produkcja przemysłowa, przemysł meblarski, motoryzacyjny, farmaceutyczny, tytoniowy, lotniczy, dystrybucja oraz górnictwo i hutnictwo. Poniżej zaprezentowane zostały przykładowe rozwiązania w ramach wdrażania danej technologii cyfrowej oraz korzyści, które najczęściej wskazywały przedsiębiorstwa w procesie implementacji rozwiązań cyfrowych.

Przemysłowy Internet Rzeczy (IoT) i analityka Big Data

Przykładowe rozwiązania: integracja systemów monitorujących urządzenia wykorzystywane w procesie produkcji lub usprawniania w systemie wsparcia posprzedażowego, cyfrowa dokumentacja i zdigitalizowane zarządzanie infrastrukturą.

Korzyści:

- mniejsza liczba przestojów,
- obniżone koszty wytwarzania za sprawą skrócenia czasu poszczególnych działań,
- eliminowanie błędów i awarii,
- usprawnienie procesów utrzymania ruchu,
- pozyskanie dodatkowego czasu dla pracowników,
- łatwiejsze planowanie napraw,
- krótszy w stosunku do dotychczasowego podejścia czas zwrotu z inwestycji,
- poprawa ogólnego bezpieczeństwa funkcjonowania,
- możliwość zdalnego monitorowania oraz modyfikacji wybranych parametrów,
- możliwość szybkiej reakcji w razie awarii lub usterki,
- wyższy ogólny poziom bezpieczeństwa pracowników,
- podniesienie jakości produktów.

Automatyzacja i robotyzacja

Przykładowe rozwiązania: automatyzacja procesów produkcyjnych, unowocześnienie systemów wsparcia kooperacji człowieka z robotem; wprowadzanie oprogramowania ułatwiającego kontrolę procesów wytwórczych, logistycznych i projektowania produktów.

Korzyści:

- utrzymanie płynności ruchu,
- wsparcie pracy człowieka przy pomocy cyfrowych asystentów,
- w pełni kontrolowane i powtarzalne procesy,
- zwiększenie wydajności produkcji,
- zdecydowana poprawa jakości procesów i produktów,
- skuteczne i szybkie reagowanie w razie awarii,
- łatwiejsze wypełnienie norm produktowych i procesowych,

- ograniczenie zużycia energii,
- szybki zwrot z inwestycji,
- wysoki poziom integracji maszyn różnych producentów,
- cyfryzacja dotychczas papierowego obiegu dokumentów,
- ograniczenie częstotliwości zmian pracowników przy poszczególnych stanowiskach,
- integracja nowych systemów informatycznych z tymi już istniejącymi,
- lepsza realizacja specyficznych wymagań klientów,
- uwolnienie czasu pracy pracowników,
- poprawa bezpieczeństwa i lepsze wykorzystanie surowców,
- wydłużenie efektywnego czasu pracy maszyn i urządzeń.

Rozwiązanie chmurowe (Cloud computing)

Przykładowe rozwiązania: monitorowanie urządzeń procesu produkcyjnego, cyfrowe projektowanie i cyfrowa personalizacja oferty biznesowej.

Korzyści:

- niższy koszt wdrożenia,
- podniesienie kompetencji pracowników (uczenie się poprzez powielanie elementów),
- wcześniejsze reagowanie na usterki/zapobieganie problemom,
- dostępność oferty bez wychodzenia z domu,
- możliwość gromadzenia i szybkiego analizowania danych o wyborach klientów,
- możliwość działania na nowych rynkach bez konieczności otwierania salonów sprzedażowych.

Rozszerzona rzeczywistość (AR), sztuczna inteligencja (AI)

Przykładowe rozwiązania: wdrożenie aplikacji do wirtualnej i rozszerzonej rzeczywistości, wirtualne szkolenia, wykorzystanie sztucznej inteligencji (AI) do wykrywania uszkodzeń infrastruktury.

Korzyści:

- skrócenie czasu poświęcanego na przygotowywanie raportów,
- usprawniona kontrola i zdalne treningi,
- szkolenia z wykorzystaniem VR,
- obniżenie kosztów wstrzymania produkcji w przypadku awarii,
- optymalne wykorzystanie podzespołów i lepsze planowanie prac serwisowych,
- zapewnienie ciągłości pracy urządzeń,
- utrzymanie ciągłości pracy i rozszerzenie działalności (np.: w obliczu pandemii COVID-19),
- ujednolicenie dokumentów technicznych,
- krótsze przestoje maszyn.

Transformacja cyfrowa oprócz ewidentnych korzyści związanych z poprawą wydajności i efektywności procesów w niektórych przypadkach może stwarzać również zagrożenia dla przedsiębiorstw. Prezentowane udane wdrożenia technologii cyfrowych i związane z nimi korzyści stanowią dla autorów punkt odniesienia w próbie identyfikacji potencjalnych zagrożeń związanych z procesem implementacji technologii cyfrowych. Lista tychże zagrożeń jest następująca:

- zbyt ogólna analiza potrzeb i związany z nią nieodpowiedni dobór parametrów, które należy monitorować i na ich podstawie podejmować decyzje,
- wybór i zastosowanie nieodpowiednich metod analizy potrzeb/nieodpowiednia dokładność audytu przed wdrożeniem technologii,
- wybór nieodpowiedniego dostawcy technologii, który często odpowiada również za instalację i uruchomienie,
- nieodpowiednio dopasowane do realnych potrzeb szkolenia pracowników,
- za długi czas wdrażania technologii cyfrowych ze względu na niemożliwość przestojów procesów,
- wysokie koszty inwestycji,
- komplikacje związane z integracją systemów,
- nieodpowiednia kalkulacja zwrotu z inwestycji.

Na podstawie studiów przypadków dotyczących wdrażania różnorodnych technologii cyfrowych, jak również na podstawie obszernie cytowanych, w części pierwszej i drugiej opracowania, wybranych pozycji literatury przedmiotu i obowiązujących aktów prawnych oraz doświadczenia eksperckiego zbudowanego w ramach realizacji projektów o charakterze analityczno-doradczym autorzy podjęli ryzyko sformułowania i zapro-

ponowania szeregu rekomendacji dotyczących przeciwdziałania zagrożeniom związanym z wprowadzaniem technologii cyfrowych nie tylko w MŚP, ale i dużych podmiotach, zarówno polskich, jak i zagranicznych:

1. **Dokładna analiza potrzeb i celów biznesowych**
   Przedsiębiorstwa powinny przeprowadzić dokładną analizę potrzeb i celów biznesowych stosując różnorodne metody oceny i priorytetyzacji działań. Zdefiniowanie klarownych celów ułatwi wybór odpowiednich rozwiązań, eliminując niepotrzebne inwestycje. Warto podkreślić, iż zastosowanie odpowiednich metod analizy powinno nastąpić przed wyborem technologii i jej dostawcy.
2. **Organizacja kompetentnego zespołu specjalistów odpowiedzialnych za wybór najlepszego rozwiązania** (dokładność audytu przed wdrożeniem)
   Warto skorzystać z usług ekspertów branżowych przed wdrożeniem nowych technologii. Specjaliści mogą pomóc w wyborze najlepszych rozwiązań dostosowanych do konkretnych potrzeb przedsiębiorstwa oraz zminimalizować ryzyko niepowodzenia wdrożenia.
3. **Odpowiedni dobór parametrów**
   Przedsiębiorstwa powinny przygotować dokładny audyt przed wdrożeniem technologii w celu eliminacji kłopotów z integracją systemów. Systemy powinny być łatwo dostosowywalne do zmieniających się potrzeb biznesowych oraz umożliwiać płynne skalowanie w miarę rozwoju firm .
4. **Przemyślany wybór dostawcy technologii – instalacja, uruchomienie i serwis**
   Przedsiębiorstwa powinny dokonać szczegółowej oceny oferty wdrożenia technologii cyfrowej biorąc pod uwagę nie tylko czynniki finansowe, ale również instalację, uruchomienie systemów oraz przyszły serwis.
5. **Wybór i przekazanie kompetencji menedżerowi projektu odpowiedzialnemu za proces wdrożenia zmian**
   Tworzenie zespołów projektowych z kompetentnymi liderami warunkuje przejrzystość zadań i skuteczne wdrażania technologii cyfrowych.
6. **Zapewnienie odpowiedniego poziomu i zakresu szkoleń dla pracowników** (np.: utrzymanie specjalistycznych szkoleń technicznych w wersji on-line).
   Zapewnienie, że zespół jest dobrze przygotowany do obsługi nowych urządzeń cyfrowych, zminimalizuje niechęć pracowników do wprowadzania zmian i zwiększy efektywność procesu wdrażania.
7. **Zachowanie równowagi pomiędzy czasem wdrażania technologii a utrzymaniem ciągłości procesów**
   Przedsiębiorstwa powinny oszacować czas potrzebny na wdrożenie technologii cyfrowej w stosunku do utrzymania ciągłości operacji biznesowych. Zbyt długotrwała konieczność przerw w realizacji procesów biznesowych negatywnie wpłynie na ich efektywność, a w efekcie na wynik finansowy.

8. **Regularna aktualizacja oprogramowania**
   Zapewnienie regularnych aktualizacji oprogramowania i systemów operacyjnych jest kluczowe dla utrzymania bezpieczeństwa i efektywności działania technologii.

9. **Bezpieczeństwo danych**
   MŚP powinny inwestować w odpowiednie rozwiązania bezpieczeństwa, a także szkolenia z zakresu cyberbezpieczeństwa dla pracowników.

10. **Monitorowanie i wczesne wykrywanie zagrożeń**
    W oparciu o studia przypadków, MŚP powinny implementować systemy monitorowania, umożliwiające wczesne wykrywanie potencjalnych zagrożeń i wypracować skuteczne procedury reagowania na sytuacje awaryjne oraz na sygnały alarmowe.

11. **Testowanie odporności systemów**
    Bazując na doświadczeniach firm, rekomenduje się regularne testowanie odporności systemów na ataki cybernetyczne. Organizacja symulacji ataków pozwala na ocenę skuteczności systemów obronnych i zidentyfikowanie potencjalnych luk w bezpieczeństwie.

12. **Kontrola dostępu i uprawnień**
    Wdrażanie systemów zarządzania tożsamościami oraz regularne przeglądy dostępów w celu minimalizacji ryzyka nieuprawnionego dostępu powinny uwzględniać kontrolę dostępu i uprawnień pracowników MŚP do systemów cyfrowych.

13. **Szyfrowanie danych**
    Rekomenduje się stosowanie technologii szyfrowania danych, zwłaszcza wrażliwych dla bezpieczeństwa narodowego, informacji biznesowych. Istotna jest edukacja pracowników na temat bezpiecznego obchodzenia się z danymi oraz korzyści wynikających ze stosowania szyfrowania.

14. **Współpraca z agencjami bezpieczeństwa narodowego**
    Ustanowienie kanałów komunikacji z odpowiednimi organami rządowymi w celu wymiany informacji o aktualnych zagrożeniach mogą przynieść korzyści. Zaleca się aktywną współpracę z instytucjami bezpieczeństwa narodowego w celu wymiany informacji na temat potencjalnych zagrożeń, a także skorzystania z ich eksperckiej wiedzy.

15. **Zgłaszanie incydentów bezpieczeństwa narodowego**
    Należy wspierać inicjatywy związane z obowiązkowym i szybkim zgłaszaniem incydentów bezpieczeństwa narodowego w odpowiednich instytucjach.

16. **Ocena wpływu na bezpieczeństwo narodowe**
    Przed wdrożeniem nowych technologii, przedsiębiorstwa powinny przeprowadzić ocenę potencjalnego wpływu na bezpieczeństwo narodowe, zwłaszcza jeśli ich działalność obejmuje kluczowe sektory gospodarki.

17. **Zabezpieczenia przed zagrożeniami zewnętrznymi**
    Rekomendowane jest wdrażanie zabezpieczeń specjalnie dostosowanych do ochrony przed zagrożeniami zewnętrznymi, które mogą mieć wpływ na bezpieczeństwo narodowe, takie jak ataki ze strony państw obcych.

18. **Przestrzeganie standardów bezpieczeństwa narodowego**
Przedsiębiorstwa powinny stosować się do ustalonych standardów bezpieczeństwa narodowego w sektorach, które są kluczowe dla stabilności kraju.

19. **Działania zapobiegawcze i reaktywne**
Rutyną powinno być planowanie zarówno działań zapobiegawczych, jak i reaktywnych w przypadku sytuacji kryzysowej związanej z bezpieczeństwem narodowym.

20. **Cyberresilience**
Wdrażanie strategii odporności, czyli zdolności do przetrwania i funkcjonowania pomimo ataków czy incydentów cybernetycznych, z uwzględnieniem aspektów narodowego bezpieczeństwa jest koniecznością.

21. **Podejście do łańcucha dostaw**
Rekomenduje się analizę i zabezpieczanie łańcucha dostaw pod kątem bezpieczeństwa narodowego, w tym stosowanie odpowiednich zabezpieczeń u partnerów biznesowych.

Zakończenie

Oddajemy do rąk przedsiębiorcom z sektora MŚP nie tylko narzędzie, ale kompleksowe podejście do wyzwań związanych z wprowadzaniem nowych technologii cyfrowych do przedsiębiorstw. W świetle analizy przeprowadzonej w ramach tej pracy, stwierdzamy, że transformacja cyfrowa stanowi zarówno szansę, jak i potencjalne zagrożenie dla konkurencyjności i bezpieczeństwa państwa.

Opracowane rekomendacje, oparte na podejściu dedukcyjnym oraz studiach przypadków, mają na celu wsparcie przedsiębiorców w rozumieniu i zarządzaniu ryzykiem cyfrowym. Macierz ryzyk, zalecenia dotyczące strategii przedsiębiorstw, pozycji cyfrowej, potencjału cyfryzacyjnego oraz strategii cyfrowej, stanowią kompleksowy zestaw narzędzi, które mogą pomóc w zminimalizowaniu potencjalnych zagrożeń.

Nasze zalecenia nie ograniczają się jedynie do sfery przedsiębiorstw. W kontekście państwa, kluczowe jest ustanowienie kompleksowych strategii zarządzania ryzykiem cyfrowym, skupiających się na regulacjach prawnych, szkoleniach, podnoszeniu świadomości cyfrowej oraz monitorowaniu zagrożeń dla rynku pracy. Państwo, jako istotny gracz na wyższym poziomie, pełni kluczową rolę w zapewnieniu cyberbezpieczeństwa i ochrony infrastruktury krytycznej.

Niezależnie od skali przedsiębiorstwa, od mikro do dużych korporacji, nasze rekomendacje przewidują elastyczne i skalowalne podejście do zarządzania cyfrowym ryzykiem.

Należy dążyć do tego, aby polityka gospodarcza państwa i działania samorządu gospodarczego były spójne z celami przedsiębiorstw, tworząc tym samym synergiczny efekt w kontekście konkurencyjności i bezpieczeństwa państwa.

Podsumowując, przyszłość zależy od tego, jak skutecznie przedsiębiorcy wykorzystają potencjał cyfrowy, minimalizując jednocześnie ryzyko z nim związane. Dlatego też nasze rekomendacje nie są jedynie statycznym zestawem środków, lecz dynamicznym narzędziem, które powinno ewoluować wraz z postępem technologicznym i zmieniającym się otoczeniem biznesowym.

Wierzymy, że efektywne zarządzanie cyfrowym ryzykiem przyczyni się do trwałej konkurencyjności przedsiębiorstw oraz bezpieczeństwa państwa, tworząc jednocześnie korzystne warunki dla rozwoju i innowacji.

Zachęcamy przedsiębiorców do aktywnego uczestnictwa w procesie cyfryzacji, do poszukiwania nowych rozwiązań i innowacyjnych strategii. Wspólnie możemy kształtować przyszłość, w której technologie cyfrowe staną się motorem rozwoju gospodarczego, a jednocześnie będą bezpieczne i zgodne z interesem państwa. Nasze rekomendacje niech będą przewodnikiem w tej podróży, a ich skuteczne wdrożenie przyniesie wymierne korzyści dla każdego uczestnika tej dynamicznej transformacji.

Bibliografia

[1] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, i B. Stiller, „Landscape of IoT security”, *Comput Sci Rev*, t. 44, s. 100467, maj 2022, doi: 10.1016/J.COSREV.2022.100467.

[2] P. Williams, I. K. Dutta, H. Daoud, i M. Bayoumi, „A survey on security in internet of things with a focus on the impact of emerging technologies”, *Internet of Things*, t. 19, s. 100564, sie. 2022, doi: 10.1016/J.IOT.2022.100564.

[3] I. H. Sarker, A. I. Khan, Y. B. Abushark, i F. Alsolami, „Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions”, *Mobile Networks and Applications*, t. 28, nr 1, s. 296–312, luty 2023, doi: 10.1007/S11036-022-01937-3/TABLES/1.

[4] F. Ullah *i in.*, „Cyber security threats detection in internet of things using deep learning approach”, *IEEE Access*, t. 7, s. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[5] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, i I. D. Moscholios, „Securing the Internet of Things: Challenges, threats and solutions”, *Internet of Things*, t. 5, s. 41–70, mar. 2019, doi: 10.1016/J.IOT.2018.11.003.

[6] T. Mazhar *i in.*, „Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence”, *Brain Sciences 2023, Vol. 13, Page 683*, t. 13, nr 4, s. 683, kwi. 2023, doi: 10.3390/BRAINSCI13040683.

[7] „Attacks On Critical Infrastructure - IOCTA 2016”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.europol.europa.eu/iocta/2016/attacks-on-ci.html

[8] M. F. Boninsegni, A. Roy, M. Bakpayev, S. Kumar, J. P. Peronard, i T. Reimer, „Opportunities of and threats to consumer well-being in the age of Fourth Industrial Revolution (IR 4.0) technologies”, *Digital Policy, Regulation and Governance* , t. 24, nr 1, s. 93–105, luty 2022, doi: 10.1108/DPRG-06-2021-0080/FULL/XML.

[9] Y. Li i Q. Liu, „A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, *Energy Reports*, t. 7, s. 8176–8186, lis. 2021, doi: 10.1016/J.EGYR.2021.08.126.

[10] „What is a Data Breach? | IBM”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.ibm.com/topics/data-breach

[11] Albekov, Vovchenko, Andreeva, i Sichev, „Block Chain and Financial Controlling in the System of Technological Provision of Large Corporations”, *EUROPEAN RESEARCH STUDIES JOURNAL*, t. XX, nr Issue 3B, s. 3–12, lis. 2017, doi: 10.35808/ERSJ/760.

[12] V.-A. ROTUNDU, „Impact of Blockchain Technology: Benefits and Security Risk and Threats”, *Informatica Economica*, t. 26, nr 2, s. 37–45, 2022, Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://ideas.repec.org/a/aes/infoec/v26y2022i2p37-45.html

[13] „As Virtual Currency Use in Human and Drug Trafficking Increases, So Do the Challenges for Federal Law Enforcement | U.S. GAO". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcemen

[14] N. Gupta, „Security and Privacy Issues of Blockchain Technology", *Studies in Big Data*, t. 60, s. 207–226, 2020, doi: 10.1007/978-981-13-8775-3_10/COVER.

[15] K. Jurczyk, „Cryptocurrencies and blockchain – challenges and threats", *The Review of Economics, Finance & Investments*, t. 1, nr 1, s. 1, lis. 2020, doi: 10.53752/REFI.2020.1.15.

[16] G. Atici, „A review on blockchain governance", *Corporate governance: Theory and practice/Conference proceedings*, s. 128–133, 2022, doi: 10.22495/CGTAPP23.

[17] C. Dion-Schwarz, D. Manheim, i P. B. Johnston, „Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats", *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, kwi. 2019, doi: 10.7249/RR3026.

[18] „Zagrożenia związane z kryptowalutami i korzyści z prawodawstwa UE". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.europarl.europa.eu/news/pl/headlines/economy/20220324STO26154/zagrozenia-zwiazane-z-kryptowalutami-i-korzysci-z-prawodawstwa-ue

[19] F. Felici, A. G. Rodríguez, P. Mieczkowski, K. Mikulski, T. Piekarz, i B. Sztokfisz, „Raport 5G. Szanse, zagrożenia, wyzwania", Kraków, 2020. [Online]. Dostępne na: https://ik.org.pl/publikacje/raport-5g-szanse-zagrozenia-wyzwania/

[20] „How 5G Technology Affects Cybersecurity: Looking to the Future | UpGuard". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.upguard.com/blog/how-5g-technology-affects-cybersecurity

[21] B. Hassib i J. Shires, „Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy", *Middle East Policy*, t. 29, nr 1, s. 90–103, mar. 2022, doi: 10.1111/MEPO.12616.

[22] J. A. Olaode i A. Ramon, „5G Security Threats and its Possible Protections in the Digital Society", *SSRN Electronic Journal*, maj 2022, doi: 10.2139/SSRN.4116931.

[23] R. Radu i C. Amon, „The governance of 5G infrastructure: between path dependency and risk-based approaches", *J Cybersecur*, t. 7, nr 1, s. 1–16, grudz. 2021, doi: 10.1093/CYBSEC/TYAB017.

[24] „Enhancing Access to and Sharing of Data", *Enhancing Access to and Sharing of Data*, lis. 2019, doi: 10.1787/276AACA8-EN.

[25] „5G zrewolucjonizuje siły zbrojne? | CyberDefence24". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://cyberdefence24.pl/armia-i-sluzby/siec-5g-rewolucja-w-obszarze-wojskowym

[26] „EU-NATO Task Force on the resilience of critical infrastructure: Final assessment report | European Commission". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6e-e2df736_en

[27] KPMG, „How to manage five key cloud computing risks"

[28] „Cybersecurity and Cloud Computing: Risks and Benefits | Rewind". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits

[29] R. Gupta, R. Agarwal, i S. Goyal, „A Review of Cyber Security Techniques for Critical Infrastructure Protection", *International Journal of Computer Science & Engineering Technology*, t. 5, nr 4, s. 331–334, 2014.

[30] „Solving the Interruption of Critical Government Services due to Cloud Outages - Government Technology Insider". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://governmenttechnologyinsider.com/solving-the-interruption-of-critical-government-services-due-to-cloud-outages/

[31] „11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance | ITwiz". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance/

[32] „Cloud computing: An overview of economic and policy issues | Think Tank | European Parliament". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2016)583786

[33] „Narodowe Standardy Cyberbezpieczeństwa, Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) v. 1.00 – luty 2020, Ministerstwo Cyfryzacji". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf

[34] „Defence Artificial Intelligence Strategy - GOV.UK". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.gov.uk/government/publications/defence-artificia--intelligence-strategy/defence-artificial-intelligence-strateg

[35] A. Ibrahim, D. Thiruvady, J. G. Schneider, i M. Abdelrazek, „The Challenges of Leveraging Threat Intelligence to Stop Data Breaches", *Front Comput Sci*, t. 2, s. 562053, sie. 2020, doi: 10.3389/FCOMP.2020.00036/BIBTEX.

[36] R. Nishant, M. Kennedy, i J. Corbett, „Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda", *Int J Inf Manage*, t. 53, s. 102104, sie. 2020, doi: 10.1016/J.IJINFOMGT.2020.102104.

[37] „Monitor Polski 2021 r. poz. 23". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.dziennikustaw.gov.pl/MP/2021/23

[38] „Artificial Intelligence & Machine Learning in Cyber Security : Aalpha". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.aalpha.net/articles/artificia--intelligence-and-machine-learning-in-cyber-security/

[39] S. Qureshi, „Cycles of development in systems of survival with artificial intelligence: a formative research agenda”, *Inf Technol Dev*, t. 29, nr 2–3, s. 171–183, lip. 2023, doi: 10.1080/02681102.2023.2236424.

[40] M. Szczepański, „Economic impacts of artificial intelligence (AI)”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf

[41] „Deepfake Increasing Threat of Identities, US Department Of Homeland Security”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pd

[42] „12 Risks and Dangers of Artificial Intelligence (AI)”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://builtin.com/artificial-intelligence/risks-of-artificial- -telligence

[43] „Sztuczna inteligencja: szanse i zagrożenia | Aktualności | Parlament Europejski”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.europarl.europa.eu/news/pl/headlines/society/20200918STO87404/sztuczna-inteligencja-szanse-i--zagrozenia

[44] „Militarisation of AI has implications for security and warfare”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.dailymaverick.co.za/opinionista/2023-07-18-militarisation-of-ai-has-severe-implications-for-global-security-and-warfare/

[45] R. Buchan i A. Lubin, „The Rights to Privacy and Data Protection in Times of Armed Conflict Autonomous Cyber Capabilities under International Law”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://ccdcoe.org/uploads/2022/06/The--Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pd

[46] „Artificial Intelligence and National Security”, Congressional Research Service. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://sgp.fas.org/crs/natsec/R45178.pdf

[47] M. Hilbert, „Big Data for Development: A Review of Promises and Challenges”, *Development Policy Review*, t. 34, nr 1, s. 135–174, sty. 2016, doi: 10.1111/DPR.12142.

[48] A. Gholami i E. Laure, „Big Data Security and Privacy Issues in the CLOUD”, *International Journal of Network Security & Its Applications (IJNSA)*, t. 8, nr 1, s. 59–79, 2016, doi: 10.5121/ijnsa.2016.8104.

[49] K. Atłasik, „How do companies use big data”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://softwaremill.com/how-do-companies-use-big-data/

[50] „Is Big Data Dangerous? The Risks Uncovered [With Examples]”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://careerfoundry.com/en/blog/data-analytics/is-big-data-dangerous/

[51] J. Kelly, „Big Data and War: Can a Cyberattack Justify an Armed Response?” Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://news.virginia.edu/content/big-data-and-war-can-cyberattack-justify-armed-response

[52] G. B. Mueller, B. Jensen, B. Valeriano, R. C. Maness, i J. M. Macias, „Cyber Operations during the Russo-Ukrainian War". 2023.

[53] S. Armenia, M. Angelini, F. Nonino, G. Palombi, i M. F. Schlitzer, „A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs", *Decis Support Syst*, t. 147, s. 113580, sie. 2021, doi: 10.1016/J.DSS.2021.113580.

[54] M. Górka, „Cybersecurity Politics – Conceptualization of the Idea", *Polish Political Science Yearbook*, t. 50, nr 1, s. 1–19, grudz. 2021, doi: 10.15804/PPSY202112.

[55] G. Weimann, „Gabriel Weimann Cyberterrorism How Real Is the Threat?", 2004, Dostęp: 3 grudzień 2023. [Online]. Dostępne na: www.usip.org

[56] P. Lis i J. Mendel, „Cyberattacks on Critical Infrastructure: an Economic Perspective", *Economics and Business Review*, t. 5, nr 2, s. 24–47, 2019, doi: 10.18559/EBR.2019.2.2.

[57] F. Bakhsh, „Security Basics for Protecting Critical Infrastructure from Cyber Threats", 2023. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://audit.wa.gov.au/wp-content/uploads/2023/06/Report-24_-Security-Basics-for-Protecting-Critical-Infrastructure-from-Cyber-Threats.pdf

[58] „Cybersecurity threat trends report - Cisco Umbrella". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://umbrella.cisco.com/info/cybersecurity-threat-trends-report?utm_medium=search-paid&utm_source=google&utm_campaign=UMB_EU_EN_GS_Nonbrand_Threats&utm_content=UMB-FY21-Q4-content-ebook-2021-cyber-security-threat-trends&_bt=621846767951&_bk=cyber+security+threats&_bm=p&_bn=g&_bg=141046486773&gad_source=1&gclid=EAIaIQobChMIw9qKpojQggMVAxWiAx1V6g-pEAAYAiAAEgLC2_D_BwE

[59] S. Landau, „Understanding Data Breaches as National Security Threats | Lawfare". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.lawfaremedia.org/article/understanding-data-breaches-national-security-threats

[60] „2023 Cyber Strategy of the Department of Defense". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

[61] M. F. Fitzpatrick Ritu Gill Jennifer Giles, M. Fitzpatrick, i R. Gill, „Information Warfare: Lessons in Inoculation to Disinformation Information Warfare: Lessons in Inoculation to Disinformation Recommended Citation Recommended Citation", t. 52, nr 1, s. 3–9, 2022, doi: 10.55540/0031-1723.3132.

[62] P. Popow, „Cyberzagrożenia w sektorze ochrony zdrowia – raport ENISA – Cyberpolicy NASK". Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://cyberpolicy.nask.pl/cyberzagrozenia-w-sektorze-ochrony-zdrowia-raport-enisa/

[63] „Quantum Computing and the Financial System: Spooky Action at a Distance?" Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System--Spooky-Action-at-a-Distance-50159

[64] D. Wedmann, „Kryptografia a komputer kwantowy”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.wojsko-polskie.pl/woc/articles/publikacje-r/kryptografia-komputer-kwantowy

[65] „Europe’s missing plan on quantum cybersecurity threats – EURACTIV.com”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.euractiv.com/section/cybersecurity/news/europes-missing-plan-on-quantum-cybersecurity-threats/

[66] D. Hoffmann, „Supercomputers offer tools for nuclear testing — and solving nuclear mysteries”, The Washington Post. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.washingtonpost.com/national/national-security/supercomputers--offer-tools-for-nuclear-testing--and-solving-nuclear-mysteries/2011/10/03/gIQAjnngdM_story.html

[67] E. T. Jensen, „Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense”, *J. Int’l L*, t. 207, 2002, Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://digitalcommons.law.byu.edu/faculty_scholarship

[68] E. Parker, „When a Quantum Computer Is Able to Break Our Encryption, It Won’t Be a Secret”, RAND. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to--break-our-encryption.html

[69] R. Arel, „Explore the impact of quantum computing on cryptography”, TechTarget. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.techtarget.com/searchdatacenter/feature/Explore-the-impact-of-quantum-computing-on-cryptography

[70] M. van Amerongen, „Technologie kwantowe w obronności i bezpieczeństwie”, Przegląd NATO. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.nato.int/docu/review/pl/articles/2021/06/03/technologie-kwantowe-w-obronnosci--i-bezpieczenstwie/index.html

[71] C. Savoie, „All your Quantum Cybersecurity Questions, Answered”, ZAPATA AI. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://zapata.ai/quantum-cryptography/

[72] R. J. Chase i G. Laporte, „The Next Generation of Crime Tools and Challenges: 3D Printing, article”, *National Institute of Justice Journal*, nr 279, s. 1–9, 2018.

[73] V. Bharadwaj, M. Brock, B. Heing, R. Miro, i N. Mukarram, „U.S. Intellectual Property and Counterfeit Goods-Landscape Review of Existing/Emerging Research”, 2020. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.uspto.gov/sites/default/files/documents/USP O-Counterfeit.pdf

[74] C. Mclean, Y. T. Lee, S. Jain, i C. Hutchings, „Modeling and Simulation of Hazardous Material Releases for Homeland Security Applications”, 2021. doi: 10.6028/NIST.IR.7786.

[75] C. Cohen, „AI in Defense: Navigating Concerns, Seizing Opportunities”. Dostęp: 4 grudzień 2023. [Online]. Dostępne na: https://www.nationaldefensemagazine.org/articles/2023/7/25/defense-department-needs-a-data-centric-digital-security--organization

[76] „Automatyzacja i robotyzacja pola walki odpowiedzią na zagrożenia militarne [ANALIZA] | Defence24”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://defence24.pl/automatyzacja-i-robotyzacja-pola-walki-odpowiedzia-na-zagrozenia-militarne-analiza

[77] A. Etzioni i O. Etzioni, „Pros and Cons of Autonomous Weapons Systems”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/

[78] „Automatyzacja pracy – jak wpływa na rynek zatrudnienia? - Money.pl”. Dostęp: 3 grudzień 2023. [Online]. Dostępne na: https://www.money.pl/gospodarka/automatyzacja-pracy-jak-wplywa-na-rynek-zatrudnienia-6769823796616160a.html

[79] M. H. Best, *The New Competition. Institutions of Industrial Restructuring*. Cambridge: Polity Press, 1993.

[80] A. Cawson, „Wprowadzenie. Wielość korporatywizmów: o konieczności mediatyzacji interesów na szczeblu pośrednim”, w *Władza i społeczeństwo*, J. Szczupaczyński, Red., Warszawa: Wydawnictwo Naukowe Scholar, 1995, s. 173–185.

[81] M. Gorynia, „Koncepcja liberalno-instytucjonalnej polityki przemysłowej”, *Gospodarka Narodowa*, t. 68, nr 1–2, s. 1–9, 1996.

[82] M. E. Porter, *Strategia konkurencji. Metody analizy sektorów i konkurentów*. Warszawa: Państwowe Wydawnictwo Ekonomiczne, 1992.

[83] M. J. Stankiewicz, Red., *Budowanie potencjału konkurencyjności przedsiębiorstw: stan i kierunki rozwoju potencjału konkurencyjności polskich przedsiębiorstw w kontekście dostosowań gospodarki do wymagań Unii Europejskiej*. Toruń: Towarzystwo Naukowe Organizacji i Kierownictwa, 1999.

[84] M. Gorynia, *Luka konkurencyjna na poziomie przedsiębiorstwa a przystąpienie Polski do Unii Europejskiej*. Poznań: Wydawnictwo Akademii Ekonomicznej w Poznaniu, 2002.

[85] „Case studies - Platforma Przemysłu Przyszłości”. Dostęp: 4 grudzień 2023. [Online]. Dostępne na: https://przemyslprzyszlosci.gov.pl/case-studies/

Spis rysunków, tabel

Spis rysunków

Rysunek 1. Macierz znaczenia (wagi) i oceny czynników potencjału cyfrowego/cyfryzacji 53

Rysunek 2. Macierz znaczenia (wagi) i oceny instrumentów cyfryzacji 57

Spis tabel

Tabela 1. Charakterystyka zasobów składających się na idealny stan potencjału cyfryzacyjnego przedsiębiorstwa 50

Platforma
Przemysłu
Przyszłości

Zagrożenia dla przedsiębiorstw sektora MŚP i interesu narodowego w erze cyfryzacji – to publikacja skierowana do menedżerów, którzy szukają praktycznych rekomendacji dotyczących niwelowania zagrożeń związanych z wprowadzeniem technologii cyfrowych do przedsiębiorstw. W opracowaniu zawarty jest katalog konkretnych zaleceń, których spełnienie może ograniczyć wystąpienie niebezpiecznych dla przedsiębiorstwa incydentów i ryzyk. Celem publikacji jest zwrócenie uwagi nie tylko na pozytywne efekty zmian, ale co najważniejsze pobudzenie refleksji na temat zagrożeń z punktu widzenia interesu publicznego i bezpieczeństwa narodowego.

Platforma Przemysłu Przyszłości – Fundacja powołana przez Ministerstwo Rozwoju i Technologii w celu wzmacniania kompetencji i konkurencyjności podmiotów prowadzących działalność na terytorium Polski – przedsiębiorców, koordynatorów klastrów, podmiotów działających na rzecz innowacyjnej gospodarki oraz partnerów społecznych i gospodarczych w zakresie cyfryzacji.

www.przemyslprzyszlosci.gov.pl