2024

Zapobieganie niekontrolowanej utracie potencjału konkurencyjnego przedsiębiorstw

z wykorzystaniem technologii cyfrowych

Platforma
Przemysłu
Przyszłości

2024

Zapobieganie niekontrolowanej utracie potencjału konkurencyjnego przedsiębiorstw

z wykorzystaniem technologii cyfrowych

materiał przygotowany w ramach prac
grupy ds. wykorzystania technologii cyfrowych w sytuacji
zagrożeń Fundacji Platforma Przemysłu Przyszłości

Opracowali:
dr hab. Joanna Kuczewska
Marek Ostafil
Piotr Wojciechowski

Warszawa, 3 grudnia 2024 roku

Platforma
Przemysłu
Przyszłości

Spis treści

Streszczenie

Celem niniejszego opracowania jest dostarczenie przedsiębiorstwom (głównie MŚP) katalogu działań prewencyjnych zapobiegających niekontrolowanej utracie potencjału konkurencyjnego z wykorzystaniem technologii cyfrowych.

W raporcie zaprezentowano kluczowe technologie cyfrowe oraz przykłady ich zastosowania w działaniach prewencyjnych związanych z zagrożeniami zewnętrznymi tj.: fizycznymi, zdrowotnymi czy geopolitycznymi. Przedstawiono także możliwości zbudowania lokalnego systemu bezpieczeństwa, ze szczególnym uwzględnieniem roli organizacji klastrowych, które mogą być istotnym aktorem całości systemu.

Przedstawiono także przykładowe zadania dla przedsiębiorstw z wykorzystaniem technologii cyfrowych. W ostatniej części raportu przedstawiono autorski katalog działań prewencyjnych z wykorzystaniem technologii cyfrowych.

Od strony metodycznej niniejsze opracowanie bazuje częściowo na danych wtórnych zebranych na podstawie literatury przedmiotu. Jednakże, w związku z brakiem krajowych opracowań tego typu, raport opiera się przede wszystkim na doświadczeniu eksperckim autorów niniejszego opracowania.

Summary

The purpose of this study is to provide enterprises (mainly SMEs) with a catalog of preventive actions to prevent uncontrolled loss of competitive potential using digital technologies.

The report presents key digital technologies and examples of their use in preventive activities related to threats e.g. physical, health or geopolitical risks. Possibilities of building a local security system were also presented, with particular emphasis on the role of cluster organizations, which may be an important actor in the overall system.

Examples of tasks for enterprises using digital technologies were also presented. The last part of the report presents an original catalog of preventive actions using digital technologies.

As for the methodological side, this study is based partly on secondary data collected on the basis of the literature on the subject, but primarily, due to the lack of this type of studies in the country, on the expert experience of the authors of this study.

Wstęp

W obliczu wysoce turbulentnego otoczenia gospodarczego przedsiębiorstwa, szczególnie z sektora mikro, małych i średnich firm (MŚP), muszą stawiać czoła różnorodnym zagrożeniom zewnętrznym tj.: zagrożeniom fizycznym, zdrowotnym czy wynikającym z sytuacji geopolitycznej. Ryzyko związane z utratą potencjału konkurencyjnego wymaga od tych podmiotów wdrażania działań prewencyjnych, które pozwolą im nie tylko przetrwać w trudnych warunkach, ale także utrzymać zdolność do konkurowana, wdrażania innowacji i rozwoju. W kontekście dynamicznie postępującej cyfryzacji, technologie cyfrowe stają się kluczowym narzędziem we wzmacnianiu konkurencyjności oraz budowaniu odporności na kryzysy.

Niniejszy raport powstał w ramach prac Think tanku powołanego przez Fundację Platforma Przemysłu Przyszłości. Jest to pierwsze opracowanie tego typu przygotowane przez polskich ekspertów i dotyczące sytuacji polskiej gospodarki. Ma ono na celu dostarczenie przedsiębiorstwom (głównie MŚP) katalogu działań prewencyjnych i sposobów wykorzystania technologii cyfrowych w zapobieganiu niekontrolowanej utracie ich potencjału konkurencyjnego. Raport został opracowany na potrzeby praktyki gospodarczej, aby wesprzeć przedsiębiorstwa zarówno w ich bieżącej, jak i strategicznej działalności.

Rozważania w drugiej części raportu kontynuują tematykę rozpoczętą w części pierwszej, skupiając się na identyfikacji kluczowych technologii oraz ich zastosowaniu w różnych obszarach, takich jak: systemy wczesnego ostrzegania, cyfrowa komunikacja, automatyzacja procesów, czy cyberbezpieczeństwo. Porusza on także kwestię luki cyfrowej, która ogranicza potencjał wdrażania nowoczesnych rozwiązań przez przedsiębiorstwa oraz wskazuje na znaczącą rolę klastrów w budowaniu lokalnych systemów bezpieczeństwa. Ponadto identyfikuje zadania, które powinny podjąć przedsiębiorstwa, aby skutecznie wdrażać działania prewencyjne i budować odporność w czasach wysokiego ryzyka wystąpienia zagrożeń zewnętrznych. Wskazuje na konieczność włączania się we wspólne inicjatywy podejmowane w klastrach wspierające wdrożenie działań prewencyjnych. Rozważania zamyka autorski katalog rekomendacji związanych z zapobieganiem niekontrolowanej utracie potencjału konkurencyjnego przedsiębiorstw z wykorzystaniem technologii cyfrowych.

Raport ukierunkowany jest na udzielenie odpowiedzi na następujące pytania badawcze:

1. Jakie działania prewencyjne z wykorzystaniem technologii cyfrowych mogą podjąć przedsiębiorstwa, szczególnie z sektora MŚP, aby chronić swój potencjał konkurencyjny przed zagrożeniami zewnętrznymi?
2. Jaka jest rola klastrów jako organizacji bezpośredniego wsparcia w tym procesie?

Mając na uwadze bezprecedensowy charakter opracowania autorzy stanęli przed wyjątkowo trudnym zadaniem – jego przygotowanie wymagało wielu analiz i poszukiwań w literaturze przedmiotu, a także zebranie wielu doświadczeń praktycznych. Należy także pamiętać, iż przedstawiony katalog działań prewencyjnych nie jest katalogiem zamkniętym i z pewnością będzie podlegał weryfikacji. Postęp w dziedzinie cyfryzacji powoduje, że w szybkim tempie pojawiają się kolejne technologie wraz ze swoimi zaletami, jak i wadami.

Rekomendacje związane z zapobieganiem niekontrolowanej utracie potencjału konkurencyjnego przedsiębiorstw z wykorzystaniem technologii cyfrowych zostały opracowane w oparciu o następujące źródła:

1. przegląd literatury międzynarodowej i krajowej,
2. analiza dostępnych wyników badań naukowych,
3. analiza doniesień medialnych,
4. zaprezentowanie przykładów efektów współpracy klastrowej,
5. analiza własnych obserwacji i doświadczeń autorów wynikających ze współpracy i bezpośrednich kontaktów z przedsiębiorstwami, w tym z racji pełnionych funkcji koordynatorów klastrów.

1. Kluczowe technologie cyfrowe i ich wykorzystanie w działaniach prewencyjnych

Wykorzystanie kluczowych technologii cyfrowych stało się integralnym elementem strategii rozwoju oraz wzmacniania konkurencyjności małych i średnich przedsiębiorstw (MŚP) . W obliczu gwałtownego postępu rewolucji cyfrowej oraz rosnącej niestabilności środowiska biznesowego, spowodowanych m.in. przez pandemię i trwające konflikty militarne, MŚP są zmuszone do wprowadzania strategii cyfrowej transformacji, aby utrzymać przewagę konkurencyjną i sprostać dynamicznie zmieniającym się potrzebom klientów.

Wdrażanie kluczowych technologii cyfrowych stało się jednym z głównych priorytetów organizacji i instytucji międzynarodowych, mając na celu wspieranie procesu transformacji cyfrowej MŚP, jak również budowanie odporności przedsiębiorstw i gospodarek w obliczu niestabilności.

To jak ważne są obecnie technologie cyfrowe pokazuje m.in. szeroko zakrojona działalność Komisji Europejskiej w ramach programu „Droga ku cyfrowej dekadzie”. Przewodnicząca KE Ursula von der Leyen zapowiedziała, że Europa powinna dążyć do osiągnięcia cyfrowej suwerenności do 2030 roku. W tej wizji kluczową rolę odgrywają takie elementy jak: tworzenie europejskiej chmury obliczeniowej, wspieranie rozwoju etycznej sztucznej inteligencji, zapewnienie bezpiecznej cyfrowej tożsamości dla wszystkich użytkowników Internetu oraz rozwój infrastruktury superkomputerów i zaawansowanych technologii łączności (Komisja Europejska 2021).

W kontekście rynku wewnętrznego program Cyfrowej Dekady oznacza intensyfikację działań w zakresie strategii przemysłowej oraz likwidację barier na jednolitym rynku. Działania te mają na celu maksymalne wykorzystanie potencjału technologii, produktów i usług cyfrowych, co ma przyczynić się do zwiększenia efektywności gospodarki europejskiej oraz wzmocnienia jej globalnej odporności i konkurencyjności (Komisja Europejska 2020). Ponadto w ramach realizacji strategii cyfrowej UE przygotowała listę projektów cyfrowych zaakceptowanych przez kraje członkowskie, które uwzględniają technologie mające kluczowe znaczenie dla MŚP (Komisja Europejska 2021):

1. budowa wspólnej ogólnoeuropejskiej infrastruktury przetwarzania danych,
2. projektowanie układów elektronicznych i innych elementów elektronicznych o niskim poborze mocy,

3. wdrożenie w całej Europie korytarzy 5G,
4. budowa zintegrowanej sieci komunikacyjnej z wykorzystaniem superkomputerów i komputerów kwantowych oraz ultra bezpiecznej kwantowej infrastruktury komunikacyjnej,
5. wprowadzenie sieci centrów monitorowania bezpieczeństwa obsługiwanej przez sztuczną inteligencję,
6. uruchomienie europejskiej infrastruktury usług w technologii Blockchain,
7. tworzenie europejskich ośrodków innowacji cyfrowych (EDIH).

Zagadnieniem przewidywania trendów technologicznych zajmują się również firmy doradcze i audytorskie działające w zakresie doradztwa strategicznego. Na przykład w 2023 roku McKinsey wskazał 15 kluczowych trendów technologicznych, do których zaliczono takie technologie jak (McKinsey 2023):

1. stosowana sztuczna inteligencja (Applied AI),
2. uczenie maszynowe (Machine Learning – ML),
3. generatywna AI (Generative AI),
4. technologie kwantowe (Quantum technologies),
5. zaawansowana łączność.

Również Deloitte wyróżnił 6 trendów, dzieląc je na dwie kategorie: „oczy skierowane w niebo” (obejmujące technologie immersyjne, sztuczną inteligencję i wielochmurowe środowiska) oraz „stopy mocno na ziemi” (koncentrujące się na elastyczności, modernizacji mainframe oraz zdecentralizowanych ekosystemach opartych na Blockchain) (Deloitte 2023).

Firma doradcza Gartner wskazała natomiast trendy w rozwoju kluczowych strategicznych technologii, w tym technologii cyfrowych takich jak (Gartner 2023):

1. sztuczna inteligencja (np. wykorzystanie do analizy i formułowania zaleceń, które pozwalają przedsiębiorstwu podejmować szybsze i dokładniejsze decyzje),
2. zarządzanie modelami sztucznej inteligencji (w zakresie zaufania, ryzyka i bezpieczeństwa modeli AI: Trust, Risk and Security in AI Models – AI TRiSM),
3. branżowe platformy chmurowe (Industry Cloud Platforms),
4. inżynieria platform (Platform Engineering),
5. realizacja wartości bezprzewodowej (Wireless-Value Realization),
6. superaplikacje (Superapps),
7. adaptacyjna AI (Adaptive AI),
8. technologie zrównoważone (Sustainable Technologies).

Zwiększenie efektywności operacyjnej jest jednym z kluczowych powodów dla których transformacja cyfrowa jest niezbędna. Przedsiębiorstwa, które inwestują w nowoczesne technologie, nie tylko szybko dostosowują się do zmieniających się warunków rynkowych, ale również zyskują przewagę konkurencyjną, wprowadzając innowacyjne rozwiązania i reagując dynamicznie na oczekiwania klientów. Wprowadzenie nowoczesnych technologii pozwala na optymalizację procesów biznesowych i produkcyjnych, co z kolei przekłada się na oszczędność czasu i zasobów. Automatyzacja rutynowych zadań takich jak obsługa dokumentacji, czy zarządzanie zapasami, umożliwia przedsiębiorstwom skoncentrowanie się na bardziej strategicznych aspektach rozwoju. Wykorzystanie technologii cyfrowych jest zatem kluczowe w procesie budowania odporności, zwłaszcza w kontekście konkurencyjności.

Równie istotną rolę technologie cyfrowe odgrywają w procesie budowania odporności przedsiębiorstw poprzez działania ze strony państwa. Systemy wczesnego ostrzegania, platformy komunikacji, wykorzystanie sztucznej inteligencji w zarządzaniu kryzysowym, czy cyberbezpieczeństwo to kluczowe procesy wsparcia budowy odporności przedsiębiorstw w tym wymiarze.

1.1. Systemy wczesnego ostrzegania i monitorowania

Systemy wczesnego ostrzegania (SWO) są szczególnym systemami informacyjnymi, których zadaniem jest sygnalizowanie użytkownikowi zagrożeń występujących w otoczeniu lub wewnątrz systemu. Sygnały ostrzegawcze powinny być przekazywane z odpowiednim wyprzedzeniem, aby użytkownik był w stanie podjąć zapobiegawcze lub kompensujące działania ochronne, eliminujące lub zmniejszające skutki sygnalizowanych zagrożeń. Systemy wczesnego ostrzegania powinny dostarczać przede wszystkim ostrzeżeń o zagrożeniach mających istotne znaczenie dla działalności i istnienia organizacji. Ponadto informacje wczesnego ostrzegania odnoszą się zwłaszcza do zdarzeń trudno przewidywalnych, mających charakter zaskoczenia. Zaskoczenie jest to sytuacja, gdy w chwili pozyskania informacji o zagrożeniu nie jest możliwe podjęcie w pełni skutecznego przeciwdziałania (Zoleński 2005).

Do kluczowych elementów systemów wczesnego ostrzegania należą (Zoleński 2005):

1. Detekcja zagrożeń – wykorzystanie różnorodnych źródeł danych, takich jak satelity, czujniki, informacje meteorologiczne czy analizy społeczne.
2. Analiza danych – przetwarzanie informacji w celu oceny ryzyka i prawdopodobieństwa wystąpienia danego zagrożenia (mapy ryzyka).
3. Wczesne ostrzeganie – przesyłanie alertów, które mogą być przekazywane do społeczności, instytucji rządowych i innych organizacji.
4. Reakcja – planowanie i wdrażanie działań, które minimalizują skutki zagrożeń, np. informowanie obywateli, organizacja ewakuacji czy dostarczenie pomocy humanitarnej.
5. Edukacja i trening – przygotowanie społeczności i organizacji na potencjalne zagrożenia poprzez programy informacyjne.

1.2. Cyfrowe platformy komunikacyjne i wymiana informacji

Cyfrowe platformy komunikacyjne i wymiana informacji umożliwiają szybki i efektywny przepływ danych między interesariuszami. Są to zróżnicowane i przeważnie rozbudowane rozwiązania technologiczne, które wykorzystując Internet i pokonując bariery terytorialne umożliwiają podmiotom współpracę oraz współtworzenie w zakresie niedostępnym w ramach tradycyjnych form współpracy (Drążek, Komorowski 2021).

Platformy cyfrowe odgrywają również kluczową rolę w komunikacji między przedsiębiorstwami a państwem w sytuacjach zagrożenia. Umożliwiają szybkie przekazywanie informacji w sytuacjach nadzwyczajnego zagrożenia, takich jak klęski żywiołowe, cyberataki czy pandemie. Za ich pośrednictwem możliwe jest szybkie i skuteczne informowanie o wystąpieniu zagrożenia, przesyłanie danych z systemów monitorujących, poznawanie aktualnych ostrzeżeń, a także korzystanie z najnowszych wytycznych od organów państwowych.

Przykładami platform cyfrowych wspierających komunikację między przedsiębiorstwami a państwem w sytuacjach zagrożeń są:

1. Departament GovTech Polska – podejmuje działania w sektorze publicznym na rzecz koordynacji strategicznych projektów cyfrowych, w które angażuje przedsiębiorstwa, urzędników i obywateli. Platforma GovTech łączy sektor publiczny z firmami technologicznymi w celu tworzenia innowacyjnych rozwiązań technologicznych, które mogą być wykorzystywane m.in. w prewencji zagrożeń i zarządzaniu kryzysowym (GovTech 2024). Podobne platformy utworzono w innych krajach, np.: United States Digital Service (USDS) oraz agencja 18F w USA, Canadian Digital Service (CDS) w Kanadzie, inicjatywy „Better for Business” wraz z programami Accelerator w Nowej Zelandii, Smart Nation w Singapurze, Tech4Germany w Niemczech, serwis Doffin w Norwegii i wiele innych (Łożykowski & Sarnowski 2019).
2. Regionalny System Ostrzegania (RSO) – jest to system rejestracji ostrzeżeń i narzędzie do szybkiego przekazywania informacji o zagrożeniach (np. klęskach żywiołowych.
3. Asseco Data Systems i ComCERT – są to inicjatywy sektora prywatnego, które dostarczają systemy ochrony cyfrowej, wykorzystywane w sektorze publicznym i prywatnym w Polsce (Asseco Data Systems 2024; ComCERT 2024).
4. ENISA Threat Landscape – europejska inicjatywa dostarczająca narzędzi wczesnego ostrzegania i raportów na temat cyber zagrożeń, wspierająca zarówno firmy, jak i administrację publiczną w ochronie przed atakami (ENISA 2024).

Mimo niewątpliwych korzyści dla przedsiębiorstw działających praktycznie w każdej branży, platformy wprowadziły też nowe zagrożenia. Pierwszym z nich jest próba wykorzystania ich jako narzędzia monopolizacji rynku i wykorzystania pozycji dominującej wobec ich użytkowników lub do wywierania wpływu na decyzje szerokich grup odbiorców (Eisenmann i in. 2006). Drugie zagrożenie związane jest, tak jak w przypadku praktycznie każdej technologii cyfrowej, z cyberbezpieczeństwem.

1.3. Automatyzacja i sztuczna inteligencja w zarządzaniu kryzysowym

Sztuczna inteligencja (AI) w ostatnich latach zyskała szczególne znaczenie w zarządzaniu publicznym ze względu na znaczący postęp w rozwoju technologicznym i zwiększeniem możliwości jej zastosowania w świadczeniu usług publicznych, w tym w zarządzaniu kryzysowym (Sienkiewicz-Małyjurek, 2024).

Sienkiewicz-Małyjurek (2024) wśród systemów sztucznej inteligencji wskazuje między innymi następujące technologie:

1. Systemy automatyzacji procesów – realizacja formalnych zadań logicznych, eksploracja danych, wnioskowanie oparte na przypadkach, inteligentne czujniki.
2. Systemy wieloagentowe – analityka mowy, widzenie komputerowe (rozpoznawanie obrazu), tłumaczenie w czasie rzeczywistym, chatboty, awatary.
3. Analityka predykcyjna – statystyczna analiza danych, przetwarzanie dużych zbiorów danych, uczenie maszynowe.
4. Sztuczne sieci neuronowe – algorytmy genetyczne, strategie ewolucyjne.
5. Drzewa decyzyjne – klasyfikacje, wspomaganie procesów podejmowania decyzji.

Technologie AI i automatyzacja mają różnorodne zastosowanie w działaniach prewencyjnych i przeciwdziałania zagrożeniom podejmowanych zarówno przez przedsiębiorstwa, jak i państwa (Tabela 1. i 2.).

Do działań podejmowanych przez przedsiębiorstwa można zaliczyć:

1. Monitorowanie i prognozowanie zagrożeń – z pomocą AI analizowane są dane, identyfikowane i przewidywane są potencjalne zagrożenia, np.: awarie techniczne, zmiany w łańcuchach dostaw czy ryzyka cyberataków.
2. Zarządzanie operacjami kryzysowymi – wspierane wdrażaniem automatyzacji procesów, np. poprzez uruchamianie protokołów awaryjnych lub optymalizację zasobów w krytycznych momentach.
3. Personalizacja komunikacji – AI umożliwia dostosowanie komunikatów kryzysowych do różnych grup interesariuszy, np. pracowników, klientów czy dostawców.

Natomiast do działań podejmowanych przez państwo można zaliczyć m.in.:

1. Systemy wczesnego ostrzegania – AI przetwarza dane z czujników IoT, systemów meteorologicznych, satelitów lub monitoringu środowiskowego, aby przewidywać m.in. trzęsienia ziemi, katastrofy naturalne epidemie, incydenty bezpieczeństwa czy powodzie i ostrzegać przed innymi.
2. Decyzje strategiczne – analityka predykcyjna wykonywana za pomocą technologii AI wspiera prognozowane skutków kryzysów i planowanie działań zapobiegawczych na poziomie krajowym. Przykładem takich działań było prognozowanie rozwoju pandemii COVID-19, optymalizacja zasobów medycznych oraz analiza efektywności wprowadzanych obostrzeń.
3. Automatyzacja wsparcia obywateli – systemy AI obsługują linie wsparcia, zarządzają informacjami kryzysowymi i przyspieszają dystrybucję pomocy.

Tabela 1. Przykłady wykorzystania AI we wsparciu wydajności procesów biznesowych.

Procesy biznesowe	Firma	Wykorzystanie AI
Logistyka zewnętrzna i wewnętrzna (planowanie dostaw i zarządzanie zapasami)	Amazon	Wykorzystanie AI do zarządzania magazynami, gdzie roboty oparte na AI sortują produkty i optymalizują ich rozmieszczenie. AI wspiera ponadto systemy planowania dostaw.
Wykorzystanie bazy wiedzy firmy	Amazon	Stworzenie własnego, wewnątrzfirmowego systemu wsparcia pracowników wykorzystującego AI – Cedric.
Wykorzystanie bazy wiedzy firmy	Lufthansa	Wykorzystanie AI do tworzenia komunikatów wewnętrznych i zewnętrznych – w tym notatek prasowych z gwarancją poprawności językowej, równościowej i inkluzywności.

Analiza i wykorzystanie danych	Coca-Cola	Analiza ogromnych zasobów danych, zarządzanie kanałami mediów społecznościowych, aplikacją mobilną oraz działem e-commerce tworząc z AI kompletną oś zarządzania firmą i wykorzystania IT w działaniach operacyjnych.
Predykcja preferencji klientów	Nike	Prototypowanie i tworzenie nowych produktów przez klientów w czasie rzeczywistym.

Źródło: opracowanie własne

Tabela 2. Przykłady wykorzystania AI w zakresie działań prewencyjnych podejmowanych przez państwo.

Kraj	Sytuacja kryzysowa	Wykorzystanie AI
Australia	Wykrywanie pożarów	Wykorzystywana w systemach monitorowania lasów, które analizują dane z kamer termowizyjnych, dronów oraz satelitów w celu wykrywania pożarów w początkowej fazie, co pozwala na szybsze działania straży pożarnej oraz ewakuację mieszkańców.
Izrael	Analiza zagrożeń wojennych	Wykorzystywana do analizy danych wywiadowczych, zdjęć satelitarnych oraz komunikacji radiowej w celu przewidywania działań wroga. Służy także do monitorowania granic, wykrywania ataków rakietowych oraz analizowania danych wywiadowczych w celu zapobiegania zagrożeniom terrorystycznym.
Chiny	Pandemia Covid-19	Wspieranie analizy w zakresie kontaktów międzyludzkich oraz wyników testów, co pozwoliło na szybsze reagowanie na wzrost zachorowań.

Japonia	Trzęsienia ziemi	Wykorzystywana do analizy danych sejsmicznych w celu przewidywania możliwego wystąpienia trzęsienia ziemi, co pozwala na natychmiastowe powiadomienia mieszkańców oraz władz.
USA	Prognozowanie huraganów oraz powodzi	Pomaga w analizie danych meteorologicznych, satelitarnych i hydrologicznych w celu przewidywania huraganów, powodzi czy innych zjawisk atmosferycznych. Pozwala to na skuteczniejsze planowanie ewakuacji i rozmieszczanie zasobów.

Źródło: opracowanie własne

Technologie AI i automatyzacja mogą znaleźć zastosowanie w zarządzaniu kryzysowym do nadzorowania przebiegu zdarzeń, analizy wielu rozproszonych informacji, czy też wspomagania procesów podejmowania decyzji.

Automatyzacja procesów biznesowych wspierana przez AI znacząco przyspiesza realizację wielu zadań, które wcześniej wymagały uwagi pracowników. Przerzucenie monotonnych i czasochłonnych czynności na automatyzację i sztuczną inteligencję sprawia, że specjaliści mogą skupić się na naprawdę ważnych zadaniach, co przekłada się na zwiększenie konwersji, lepsze wyniki oraz wyższy poziom satysfakcji zespołu.

Jednak wykorzystanie technologii, czy algorytmów sztucznej inteligencji obarczone jest ryzykiem wynikającym z wyzwań związanych z niedojrzałością badań i doświadczeń w tym zakresie. Jednym z kluczowych zagrożeń jest sposób postrzegania AI przez użytkowników, ich ignorancja oraz przypisywanie AI cech ludzkich lub wręcz mitycznych. Z technologicznego punktu widzenia AI można postrzegać jako zamknięty system sterowania oparty na mechanizmie sprzężenia zwrotnego. Technologie AI nie są mityczne, a kluczowymi aspektami ich implementacji są konkretne wymagania techniczne, takie jak wystarczająca moc obliczeniowa oraz szczegółowa wiedza techniczna dotycząca zastosowania wybranych algorytmów uczenia maszynowego (Fałkowski i in. 2024a).

1.4. Cyberbezpieczeństwo jako warunek funkcjonowania odpornej gospodarki cyfrowej

Cyberbezpieczeństwo stało się jednym z najważniejszych warunków budowania silnej, odpornej i bezpiecznej gospodarki zarówno na poziomie krajowym, jak i w kontekście globalnej konkurencji oraz konfliktów międzynarodowych. Ich przebieg pokazuje, że cyberprzestrzeń jest również teatrem działań wojennych, które przekraczają fizyczne granice i obszary wojny konwencjonalnej. W dzisiejszym cyfrowym świecie, w którym gospodarki w coraz większym stopniu opierają się na różnego rodzaju technologiach, połączonych systemach, infrastrukturze i przepływie danych, cyberbezpieczeństwo jest podstawowym czynnikiem zapewniającym bezpieczeństwo na poziomie narodowym, ale też struktur i organizacji międzynarodowych. Cyberbezpieczeństwo jest bowiem nie tylko wymogiem technicznym, ale podstawowym filarem długoterminowej odporności gospodarczej i bezpieczeństwa w coraz bardziej połączonym i cyfrowym świecie. Aby ochronić infrastrukturę krytyczną, ale też budować zaufanie do gospodarki cyfrowej tj. zapewnić możliwości rozwoju technologicznego i funkcjonowania różnorodnych obszarów życia gospodarczego, zapewnienie wysokiego poziomu cyberbezpieczeństwa jest absolutnie konieczne.

Infrastruktura krytyczna, do której zaliczają się m.in.: sieci energetyczne, systemy transportowe, opieka zdrowotna, usługi finansowe i wodociągi w dużej mierze wykorzystuje dziś systemy cyfrowe. Udany cyberatak na tę infrastrukturę może sparaliżować gospodarkę kraju lub jej poszczególne gałęzie, poprzez zakłócenie podstawowych usług i spowodowanie znacznych strat finansowych, a nawet spowodować zagrożenie życia ludzkiego. Ochrona przed cyberatakami jest również niezwykle istotna w firmach produkcyjnych, które w dobie Przemysłu 4.0 coraz częściej włączają praktycznie każde urządzenie czy maszynę do systemu informatycznego.

Jednym z przykładów pokazujących jak organizacje międzynarodowe starają się ograniczyć cyber ryzyka jest Dyrektywa UE NIS2 (KE 2022) (dyrektywa dot. sieci i systemów informatycznych). Nakazuje ona krajom członkowskim wprowadzić bardziej rygorystyczne standardy cyberbezpieczeństwa w celu ochrony podstawowych usług, w tym sektora energetycznego, transportowego i zdrowotnego. Dyrektywa wymaga, aby zarówno firmy prywatne, jak i instytucje publiczne podejmowały proaktywne kroki w celu zabezpieczenia swoich systemów cyfrowych. Co istotne, ofiarami większości cyber ataków padają w ogromnej mierze małe i średnie przedsiębiorstwa. Nacisk UE na cyberbezpieczeństwo infrastruktury krytycznej znacznie wzrósł po kilku cyberatakach, takich jak atak ransomware WannaCry z 2017 r. (GDPR.pl 2017), który uderzył w szpitale i systemy transportowe w wielu krajach, powodując ogromne zakłócenia funkcjonowania systemów i szkody dla gospodarki (Frankowicz 2017).

Jak pokazują raporty cyberataki skutkują ogromnymi stratami finansowymi zarówno dla podmiotów, które padły ich ofiarami, jak i dla całych gospodarek, zakłócając działalność biznesu i wpływając tym na spadek konkurencyjności gospodarek krajowych (Arroyabe i in. 2024). Wiele podmiotów zaczyna wymagać od swoich kooperantów i poddostawców zapewnienia wysokiego poziomu cyberbezpieczeństwa, aby uniknąć sytuacji, w której małe firmy były słabym punktem całego cyfrowego systemu i tym samym pozwoliły cyberprzestępcom na jego infiltrację i atak. Silne systemy i polityki w zakresie cyberbezpieczeństwa pomagają złagodzić te zagrożenia, zapewniając firmom i całym ich sieciom możliwość bardziej bezpiecznego działania.

Poniżej zaprezentowano przykłady z wybranych krajów, które pokazują, w jaki sposób cyberbezpieczeństwo chroni infrastrukturę krytyczną, cyfrowe systemy wykorzystywane w sektorach prywatnym i publicznym oraz chroni państwa i organizacje przed cyberatakami (Tabela 3.).

Tabela 3. Rola cyberbezpieczeństwa w zakresie ochrony gospodarki cyfrowej. Przykłady z wybranych krajów.

Kraj	Naruszenia / ataki cybernetyczne	Działania prewencyjne
Stany Zjednoczone	W 2021 r. atak ransomware Colonial Pipeline doprowadził do zamknięcia głównego rurociągu paliwowego, powodując niedobory paliwa i zakłócenia gospodarcze na Wschodnim Wybrzeżu USA (Easterly 2023).	Ataki typu ransomware, których celem stały się zarówno podmioty sektora publicznego, jak i prywatnego (w tym MŚP) w 2021 r. kosztowały amerykańskie firmy miliardy dolarów w różnych formach: w płatnościach okupu, utraconej produktywności i zniszczonej reputacji. W związku z tym Rząd Stanów Zjednoczonych wzmocnił środki cyberbezpieczeństwa, wydając Dekrety Prezydenckie (Executive Order 14,028) mające na celu poprawę odporności infrastruktury krytycznej i nakazujące współpracę między sektorem publicznym i prywatnym w celu ochrony podstawowych usług przed przyszłymi zagrożeniami cybernetycznymi. Agencja Cybersecurity and Infrastructure Security Agency (CISA) podjęła kroki w celu zwalczania rosnącej liczby ataków ransomware poprzez tworzenie partnerstw publiczno-prywatnych i inicjatywy wymiany informacji (CISA 2023, Wood 2023).

Kanada	Zagrożenia wobec infrastruktury krytycznej, operacji cyfrowych i handlowych.	Canadian Center for Cyber Security odgrywa kluczową rolę w ochronie krajowej infrastruktury. W związku z rosnącymi zagrożeniami cybernetycznymi dla podstawowych usług, w tym opieki zdrowotnej i systemów finansowych, Kanada wzmocniła swoją politykę w zakresie cyberbezpieczeństwa, aby zapewnić odpowiednią ochronę kluczowym branżom, takie jak energetyka i bankowość. Opracowana krajowa strategia cyberbezpieczeństwa podkreśla również znaczenie współpracy międzynarodowej, biorąc pod uwagę transgraniczny charakter zagrożeń cybernetycznych (CCfCS 2024). Kanadyjska Karta Cyfrowa, której cyberbezpieczeństwo jest kluczowym elementem, zapewnia bezpieczeństwo operacji cyfrowych dla firm i tym samym mitygujący ryzyka płynące z cyber zagrożeń (CDC 2024). Kanadyjska Giełda Cyber zagrożeń (CCTX) pomaga firmom dzielić się informacjami o zagrożeniach, zapewniając, że branże kluczowe dla kanadyjskiej gospodarki, takie jak energetyka i zaawansowane technologie cyfrowe pozostają bezpieczne i konkurencyjne na arenie międzynarodowej (CCTX 2024).

Japonia	Naruszenia ochrony własności intelektualnej, łańcuchów dostaw i innych procesów biznesowych.	Cybersecurity Strategy of Japan ma na celu ochronę infrastruktury cyfrowej, zapobiegania naruszeniom danych i zabezpieczenia urządzeń IoT. Celem jest stworzenie systemu, w którym firmy i osoby fizyczne mogą bezpiecznie uczestniczyć w pełni cyfrowej gospodarce (CSJ 2021). SME Cybersecurity Initiative pomaga małym firmom wdrażać stosunkowo łatwo i w sposób efektywny kosztowo środki cyberbezpieczeństwa w celu ochrony przed naruszeniami danych, kradzieżą własności intelektualnej i atakami na łańcuch dostaw (CI 2017).

Źródło: opracowanie własne.

Podsumowując, kluczowe technologie cyfrowe wykorzystywane są szeroko w działaniach prewencyjnych i obejmują różne obszary działań, zapewniając budowę i utrzymanie odporności na zagrożenia zarówno ze strony przedsiębiorstw, jak i państwa (Cyfrowa Polska 2022, KPMG & Microsoft 2024, Tabela 4.).

Tabela 4. Kluczowe technologie cyfrowe wykorzystywane w działaniach prewencyjnych.

Technologie cyfrowe	**Wykorzystanie w działaniach prewencyjnych**
Internet Rzeczy (Internet of Things – IoT)	Sieci czujników IoT pozwalają na monitorowanie środowiska naturalnego, przewidywanie klęsk żywiołowych (np. trzęsień ziemi, huraganów) oraz monitorowanie infrastruktury krytycznej, co pomaga w zarządzaniu ryzykiem w czasie rzeczywistym. W kontekście zdrowotnym IoT jest stosowane w urządzeniach medycznych na bieżąco monitorujących stan zdrowia pacjentów. Industrial Internet of Things (IIoT) jest stosowany w firmach przemysłowych w różnego rodzaju maszynach oraz urządzeniach w celu zwiększenia efektywności operacyjnej, poprawy jakości produktów i usług, oraz wspierania innowacji poprzez np.: zdalne monitorowanie maszyn w przemyśle, optymalizację łańcucha dostaw czy personalizację doświadczeń klientów.
Łańcuch bloków (Blockchain)	Technologia Blockchain jest wykorzystywana w zapewnianiu bezpieczeństwa transferu i operacji z wykorzystaniem danych, co jest kluczowe zwłaszcza w sektorze zdrowotnym i finansowym. W zakresie zdrowia publicznego Blockchain pomaga w zabezpieczaniu informacji o pacjentach, eliminując ryzyko nieuprawnionego dostępu do danych wrażliwych. W przedsiębiorstwach i gospodarce Blockchain może zapewnić transparentność i bezpieczeństwo np. w łańcuchach dostaw.
Sztuczna inteligencja (Artificial Intelligence – AI)	AI jest szeroko wykorzystywana do analizowania danych i prognozowania zagrożeń. W kontekście zdrowotnym, AI wspiera monitorowanie zdrowia publicznego, przewidując rozprzestrzenianie się chorób zakaźnych. W sektorze bezpieczeństwa narodowego AI jest stosowana do analizy ryzyka geopolitycznego oraz identyfikacji zagrożeń cybernetycznych, co ma kluczowe znaczenie dla przeciwdziałania atakom hackerskim i wojnom cybernetycznym.

Rozszerzona i wirtualna rzeczywistość (AR/VR)	Wykorzystywane są w szkoleniach medycznych oraz z zakresu reagowania kryzysowego. Mogą symulować katastrofy naturalne, ataki terrorystyczne, czy wybuchy epidemii, umożliwiając służbom ratunkowym i medycznym ćwiczenia w realistycznych warunkach bez zagrożenia dla życia. Technologie te wykorzystywane są również w przemyśle w przygotowywaniu bliźniaków cyfrowych czy też symulowaniu ustawiania maszyn i procesów przetwórczych.
Analiza danych, analiza dużych zbiorów danych (Big Data) oraz chmura obliczeniowa (Cloud computing)	Przetwarzanie i analiza dużych zbiorów danych umożliwia prognozowanie i szybkie reagowanie na zagrożenia, zarówno naturalne, jak i geopolityczne. W ochronie zdrowia analiza danych pomaga w zarządzaniu w walce z epidemiami oraz monitorowaniu zdrowia populacji na dużą skalę.
Cyberbezpieczeństwo	Cyberbezpieczeństwo jest kluczowe w eliminacji zagrożeń cyfrowych, geopolitycznych i zdrowotnych, szczególnie w obliczu rosnących zagrożeń cybernetycznych związanych z atakami niektórych państw i organizacji przestępczych. Wdrażanie zaawansowanych strategii cyberbezpieczeństwa oraz technologii (w tym szyfrowania, kontroli dostępu i wykrywania zagrożeń) jest niezbędne dla ochrony infrastruktury krytycznej, systemów finansowych oraz systemów ochrony zdrowia, a także w przedsiębiorstwach przemysłowych.

Źródło: opracowanie własne.

2. Luka cyfrowa polskich MŚP oraz rola klastrów w budowaniu lokalnego systemu bezpieczeństwa

2.1. Luka cyfrowa polskich MŚP

Koncepcja luki cyfrowej oparta na eklektycznej definicji konkurencyjności przedsiębiorstw, umożliwia identyfikację kluczowych zagrożeń związanych z wdrażaniem technologii cyfrowych.

Wśród najważniejszych problemów związanych z transformacją cyfrową, zwłaszcza wśród firm z grupy MŚP, można wymienić:

1. brak powszechnie znanej strategii cyfryzacji,
2. niską akceptację zmian wśród pracowników,
3. ograniczone kompetencje cyfrowe pracowników i kadry zarządzającej,
4. konieczność dostosowania się do dynamicznych zmian rynkowych,
5. silną konkurencję ze strony dużych firm,
6. zależność od dostawców technologii,
7. konieczność ciągłej aktualizacji systemów i wiedzy,
8. brak standaryzacji i kompatybilności systemów przy wprowadzaniu nowych technologii,
9. utrudnioną integrację rozwiązań cyfrowych,
10. wysokie koszty inwestycji w oprogramowanie i infrastrukturę,
11. kwestie związane z ochroną prywatności danych,
12. rosnące zagrożenia w zakresie cyberbezpieczeństwa.

„Zasypanie” luki cyfrowej jest zatem kluczowym wyzwaniem dla MŚP. Dlatego też zaleca się opracowanie spójnej strategii cyfryzacji, która pozwoli na wzmocnienie pozycji cyfrowej przedsiębiorstwa i umożliwi efektywne wykorzystanie dostępnych technologii, uwzględniając jednocześnie kwestie związane z bezpieczeństwem, standaryzacją i kompetencjami pracowników.

W ramach działań na rzecz transformacji cyfrowej i zmniejszania luki technologicznej warto uwzględnić następujące rekomendacje.

1. Przede wszystkim przedsiębiorstwa powinny przeprowadzić dokładną analizę potrzeb biznesowych, definiując jasne, konkretne cele, co pozwoli na wybór odpowiednich rozwiązań i uniknięcie zbędnych lub nietrafionych inwestycji.
2. Ważnym elementem jest także organizacja zespołu specjalistów odpowiedzialnych za audyt przedwdrożeniowy, który pozwoli dostosować technologie do specyficznych wymagań firmy.
3. Kolejnym krokiem jest przemyślany dobór dostawcy, uwzględniający nie tylko koszty, ale również instalację, uruchomienie i serwis.
4. Kluczowa jest również odpowiednia organizacja szkoleń dla pracowników, co zwiększa efektywność wdrażania nowych technologii.
5. W trakcie całego procesu należy zadbać o równowagę między czasem wdrażania, a utrzymaniem ciągłości procesów, regularnie aktualizować oprogramowanie i zapewnić odpowiedni poziom bezpieczeństwa danych, w tym inwestycje w cyberbezpieczeństwo i szkolenia dla personelu (Fałkowski i in. 2024, 2024a).

2.2. Rola klastrów w budowaniu lokalnego systemu bezpieczeństwa

Klastry odgrywają istotną rolę w ramach budowania konkurencyjności przedsiębiorstw oraz ich odporności na zagrożenia, z uwzględnieniem koncepcji luki cyfrowej. Stanowią one platformę zarówno wzajemnej współpracy wyspecjalizowanych przedsiębiorstw, jak i ich współdziałania z instytucjami edukacyjnymi i publicznymi. Pozwala to łączyć poziom mikro (pojedyncze przedsiębiorstwa) z poziomem makro (instytucje i organizacje państwowe). Dzięki swojej specyficznej strukturze organizacyjnej klastry są zdolne do koordynacji działań wspierających przedsiębiorstwa w podnoszeniu ich odporności oraz realizacji wspólnych inicjatyw ukierunkowanych na przeciwdziałanie zagrożeniom, uzupełniając tym samym wysiłki państwa w tym zakresie.

Organizacje klastrowe odgrywają istotną rolę w wielu obszarach, między innymi w (Baron 2016):

1. rozwoju innowacyjności,
2. rozwoju przedsiębiorczości,
3. promocji przedsiębiorstw,
4. rozwoju i promocji całej gospodarki,
5. wspierania systemu edukacji,
6. rozwoju gospodarczym poszczególnych regionów i całego kraju.

Do tej pory polskie klastry w niewielkim stopniu były traktowane jako istotny aktor lokalnych systemów bezpieczeństwa. Sytuację zmieniły doświadczenia zdobyte podczas pandemii COVID-19, które pokazały, że organizacje klastrowe w Polsce mogą odegrać niezwykle ważną rolę w sytuacjach zagrożenia.

Działania klastrów miały miejsce na poziomie regionalnym, krajowym, a także europejskim. Na poziomie regionalnym poszczególne klastry współpracowały z przedstawicielami administracji oraz ochrony zdrowia w zakresie dostarczania niezbędnych produktów np. środków ochrony indywidualnej (przyłbic, masek, gogli itp.). Jeśli chodzi o poziom krajowy to niezwykle ważną rolę odgrywał Związek Pracodawców Klastry Polskie (ZPKP) jako instytucja koordynująca współpracę klastrów. Na poziomie krajowym nawiązana została również współpraca międzyklastrowa, w wyniku której organizacje dzieliły się swoimi doświadczeniami oraz informowały o potrzebach i możliwościach ich zaspokajania przez członków innych klastrów. Dodatkowo ZPKP był swego rodzaju pośrednikiem pomiędzy klastrami krajowymi, a organizacją zrzeszającą klastry europejskie – European Cluster Alliance przy wykorzystaniu europejskiej platformy European Cluster Collaboration Platform. Na poziomie europejskim Związek zbierał zapotrzebowanie od ECA i przekazywał je na poziom krajowy i odwrotnie – informował ECA o możliwościach i potrzebach krajowych klastrów.

Należy również podkreślić rolę jaką odegrały klastry dla swoich członków, którzy również znaleźli się w nowej i bardzo trudnej sytuacji. Wśród działań jakie zostały zorganizowane można wymienić chociażby organizację giełd wewnątrzklastrowych na temat potrzeb i możliwości organizacji klastrowych, wsparcia w odbudowaniu zerwanych łańcuchów dostaw, organizację badań sytuacji na rynku, udział w różnego rodzaju konsultacjach ustaw i aktów wykonawczych, zgłaszanie potrzeb do władz administracyjnych itp. Współpraca nawiązana pomiędzy klastrami w tamtym okresie, pomimo zakończenia pandemii, trwa do dzisiaj i jest miejscem wypracowywania wspólnych stanowisk i tworzenia nowych projektów. Istotne jest także to, że doświadczenia klastrów zostały również wykorzystane na potrzeby organizacji pomocy dla ofiar wojny na Ukrainie.

Przykład współpracy dotyczący wsparcia podczas pandemii może być z pewnością rozszerzony i wykorzystywany w wielu innych obszarach występowania zagrożeń, w tym między innymi w obszarze cyberbezpieczeństwa. W Polsce nie mamy jeszcze zbyt wiele tego typu doświadczeń, ale można je znaleźć na poziomie europejskim czy światowym. Z pewnością warto je wykorzystać jako przykład i inspirację do zbudowania podobnego systemu na poziomie krajowym.

Klastry jako sieci przedsiębiorstw, instytucji badawczych, a czasem też władz samorządowych różnego szczebla wspierają współpracę, tworzenie innowacji i wymianę wiedzy między członkami, podmiotami partnerskimi, całymi branżami, a także między sektorami. Niezwykle istotna jest też rola klastrów w budowaniu i rozwijaniu wzajemnego zaufania.

Wśród wielu atutów klastrów w kontekście bezpieczeństwa można wymienić między innymi:

1. bezpośredni kontakt z przedsiębiorstwami i jednostkami B+R,
2. elastyczność,
3. zaufanie zbudowane pomiędzy organizacjami,
4. doświadczenie w budowaniu współpracy i wspólnych działań,
5. unikalna znajomość danej branży, jej potencjału, możliwości i problemów.

Wskazane wcześniej doświadczenia i przedstawione powyżej atuty pozwalają na określenie głównych funkcji, jakie organizacje klastrowe mogą pełnić w ramach budowania lokalnego systemu bezpieczeństwa. Należą do nich:

1. funkcja informacyjna,
2. funkcja edukacyjna i wspierająca innowacyjność,
3. funkcja organizatora i koordynatora działań,
4. funkcja ekspercka,
5. funkcja wspierająca tworzenie bezpiecznej infrastruktury.

Wśród szczególnych możliwości i potencjału klastrów ważnym obszarem działalności jest fakt, że służą one jako pomosty pomiędzy MŚP a instytucjami badawczymi, umożliwiając budowanie i wymianę wiedzy i najlepszych praktyk. Ten bezpośredni kontakt może skutkować nowymi projektami i znacznie ułatwić szybkie wdrażanie najnowocześniejszych rozwiązań w zakresie bezpieczeństwa, które w przeciwnym razie mogłyby być niedostępne dla MŚP ze względu na koszty lub brak wiedzy specjalistycznej. Klastry mogą i powinny dbać także o budowanie świadomości swoich członków w zakresie bezpieczeństwa oraz stosowania technologii cyfrowych. Może się to odbywać poprzez różnego rodzaju konferencje, szkolenia i wizyty umożliwiające poznawanie dobrych praktyk. Z pewnością ułatwia to zbudowane w organizacjach klastrowych dotychczasowe zaufanie między członkami, które wynika z długotrwałego partnerstwa. Jest ono niezbędne praktycznie w każdym aspekcie współpracy klastrowej, szczególnie w przypadku opracowywania rozwiązań z zakresu bezpieczeństwa.

Organizacje klastrowe odgrywają ważną rolę w promowaniu innowacji, także tych w dziedzinie cyberbezpieczeństwa, poprzez wspieranie działań badawczo-rozwojowych wśród MŚP i instytucji badawczych. Innowacje te są niezbędne do opracowywania nowych technologii, które mogą sprostać pojawiającym się zagrożeniom i wzmocnić odporność zarówno MŚP, jak i całej gospodarki.

Ważnym aspektem działalności klastrów w aspekcie bezpieczeństwa jest również ich działalność jako organizacji eksperckich. Żadne inne organizacje nie posiadają tak dogłębnej wiedzy na temat danej branży czy sektora gospodarki, jego możliwości, potencjału, ale także problemów i braków. Może to być wykorzystane między innymi w konsultacji różnego rodzaju dokumentów strategicznych, ustaw czy rozporządzeń, również tych dotyczących kwestii bezpieczeństwa. Funkcja ta była bardzo widoczna podczas pandemii COVID-19, podczas której polskie klastry brały udział w konsultacjach ustaw zarówno ogólnogospodarczych, jak i dotyczących danych sektorów.

Wiedza ta umożliwia również opracowywanie strategii sektorowych, między innymi w zakresie cyberbezpieczeństwa. Ta specjalistyczna wiedza jest nieoceniona dla MŚP, którym często brakuje zasobów, aby nadążyć za szybko zmieniającymi się zagrożeniami i technologiami. Wykorzystując specjalistyczną wiedzę klastrów, MŚP mogą wdrażać rozwiązania, które są znacznie lepiej dostosowane do ich unikalnych wyzwań i potrzeb.

Niezwykle istotną funkcją organizacji klastrowych, która może być skutecznie wykorzystana w aspekcie bezpieczeństwa, jest organizacja i koordynacja działań. W momencie pojawienia się danego zagrożenia w klastrach istnieje ogromny potencjał współpracy zarówno wśród ich członków, jak również z organizacjami spoza struktur klastrowych. Oprócz wypracowanego zaufania i schematów współpracy wymaga to również elastyczności oraz zasobów kadrowych o określonych umiejętnościach i kompetencjach. Było to doskonale widoczne podczas pandemii COVID-19, podczas której klastry z sukcesem koordynowały wsparcie zarówno pomiędzy swoimi organizacjami, jak i ze służbami medycznymi oraz administracją różnego szczebla.

Poniżej przedstawiono przykłady inicjatyw podejmowanych przez klastry w różnych krajach na rzecz budowania odporności i przeciwdziałania zagrożeniom. Może być to swoisty katalog najlepszych praktyk dla polskich organizacji klastrowych, które podejmują wysiłki na rzecz rozwoju podobnych działań prewencyjnych (Tabela 5.).

Tabela 5. Przykłady inicjatyw na rzecz budowania odporności i przeciwdziałania zagrożeniom podejmowanych przez klastry w różnych krajach.

Klaster	Przykłady działań
European Cyber Security Organization (ECSO)	Partnerstwo publiczno-prywatne na poziomie europejskim, które łączy MŚP z sektora cyberbezpieczeństwa z większymi przedsiębiorstwami, ośrodkami badawczymi i instytucjami akademickimi. ECSO oferuje MŚP dostęp do innowacyjnych rozwiązań i badań nad cyberbezpieczeństwem, pomagając im chronić ich zasoby cyfrowe. Dzięki wspólnym projektom ECSO pomaga budować świadomość w zakresie cyberbezpieczeństwa w UE, a także umożliwia MŚP wdrażanie zaawansowanych narzędzi i systemów cyberbezpieczeństwa, takich jak wykrywanie zagrożeń oparte na sztucznej inteligencji, bez konieczności opracowywania ich we własnym zakresie. Współpraca ta wzmacnia zarówno cyberbezpieczeństwo MŚP, jak i szerszą odporność gospodarczą UE poprzez podnoszenie ogólnego poziomu bezpieczeństwa podmiotów z sektora prywatnego i publicznego (ECSO 2024).

Keihanna Science City – Japonia	Skupia firmy technologiczne, MŚP, instytucje badawcze i instytucje publiczne. W ramach tego klastra MŚP zbudowały długotrwałe, oparte na zaufaniu relacje z większymi firmami i instytucjami badawczymi, co umożliwiło im skuteczną współpracę nad rozwiązaniami w zakresie cyberbezpieczeństwa. Na przykład kilka pilotażowych projektów w zakresie cyberbezpieczeństwa w ramach klastra koncentrowało się na zabezpieczaniu urządzeń IoT w produkcji – kwestii krytycznej dla MŚP w tym sektorze. Projekty te skorzystały na wzajemnym zaufaniu między partnerami, co ułatwiło otwartą wymianę danych i spostrzeżeń, prowadząc do stworzenia solidnych i dostosowanych do potrzeb mniejszych firm rozwiązań w zakresie cyberbezpieczeństwa (KSC 2024).
Industrial Cybersecurity Center of Excellence (ICSCoE) – Japonia	Klaster zrzesza liderów branży i MŚP w celu poprawy poziomu ich odporności na cyber zagrożenia. ICoE wykorzystuje swoje doświadczenie w reagowaniu kryzysowym i współpracy z różnymi interesariuszami – zarówno z sektora prywatnego, jak i publicznego, aby pomóc MŚP złagodzić ryzyko cyberataków wymierzonych w krytyczne sektory przemysłowe. Łącząc zasoby i wiedzę, członkowie klastra mogą skuteczniej reagować na cyber zagrożenia (ICSCoE 2024).
Cybersecurity Manufacturing Innovation Institute (CyManII) – USA	Partnerstwo publiczno-prywatne, które wspiera małe i średnie przedsiębiorstwa produkcyjne w zakresie podnoszenia poziomu cyberbezpieczeństwa. CyManII wspiera tworzenie relacji opartych na zaufaniu wśród swoich członków, tworząc bezpieczne środowiska, w których firmy mogą dzielić się wrażliwymi informacjami na temat luk w zabezpieczeniach bez obawy o utratę przewagi konkurencyjnej. To środowisko zaufania pozwala MŚP na otrzymywanie odpowiednio dostosowanych porad i rozwiązań, które zaspokajają ich specyficzne potrzeby w zakresie cyberbezpieczeństwa, jednocześnie przyczyniając się do tworzenia krajowej odporności gospodarczej poprzez zabezpieczenie krytycznej infrastruktury produkcyjnej (CyManII 2024).
Securitymadein.lu – Luksemburg	Klaster promujący innowacje w obszarze zabezpieczeń cybernetycznych. Wspiera MŚP w prowadzeniu projektów badawczo-rozwojowych związanych z cyberbezpieczeństwem, w szczególności w obszarach takich jak ochrona danych, bezpieczna komunikacja i szyfrowanie. Dzięki wspólnym wysiłkom badawczo-rozwojowym MŚP są w stanie opracowywać najnowocześniejsze rozwiązania, które nie tylko chronią ich własne operacje, ale także przyczyniają się do tworzenia ogólnej konkurencyjności UE na globalnym rynku (SMiL 2024).

Klaster Cyberbezpieczeństwa – Estonia	Obejmuje MŚP, instytucje publiczne i ekspertów ds. cyberbezpieczeństwa. Klaster ułatwia szybkie reagowanie na cyber zagrożenia poprzez dostarczanie MŚP aktualnych informacji na temat metod ataków i słabych punktów w infrastrukturze z której mogą korzystać MŚP. W przypadku cyberataku MŚP będące członkami klastra mogą uzyskać dostęp do zasobów zarządzania kryzysowego, takich jak zespoły ekspertów, które pomagają im wrócić do funkcjonowania po ataku, zminimalizować szkody i wzmocnić obronę przed przyszłymi incydentami. Ta zdolność szybkiego reagowania ma kluczowe znaczenie dla utrzymania odporności estońskiej gospodarki, zwłaszcza biorąc pod uwagę jej dużą zależność od infrastruktury cyfrowej (ECT 2024).
Silicon Saxony – Niemcy	Jeden z największych w Europie klastrów mikroelektroniki i ICT. Jego działania pokazują, w jaki sposób można wykorzystać wiedzę branżową w celu podniesienia poziomu cyberbezpieczeństwa MŚP. Koncentrując się na produkcji półprzewodników, klaster opracował zaawansowane rozwiązania, które uwzględniają konkretne zagrożenia w łańcuchu dostaw elektroniki, takie jak kradzież własności intelektualnej i manipulacje sprzętowe. MŚP w ramach klastra korzystają z odpowiednio dostosowanych rozwiązań, umożliwiających im zabezpieczenie swoich operacji przed zaawansowanymi cyber zagrożeniami, które są ukierunkowane konkretnie na ich sektor technologiczny (SS 2024).
Digital Technology Supercluster – Kanada	Odegrał kluczową rolę w opracowaniu rozwiązań w zakresie cyberbezpieczeństwa dla MŚP. Wykorzystując dogłębną wiedzę zgromadzoną w klastrze na temat sektorów (np. opieki zdrowotnej lub logistyki), MŚP będące jego członkami uzyskują dostęp do zaawansowanych narzędzi, które są ukierunkowane na konkretne słabe punkty w ich branżach. Na przykład w sektorze opieki zdrowotnej klaster pomógł opracować rozwiązania zabezpieczające urządzenia medyczne i dane pacjentów (DTS 2024).
Baskijskie Centrum Cyberbezpieczeństwa – Hiszpania	Centrum skupia MŚP, władze lokalne i ekspertów ds. cyberbezpieczeństwa w celu dzielenia się informacjami na temat najnowszych cyber zagrożeń i metod ataków. To środowisko wzajemnego zaufania pozwala MŚP uczyć się od siebie nawzajem i szybciej przyjmować najlepsze praktyki, zwiększając w ten sposób ogólną odporność i bezpieczeństwo regionalnej gospodarki (BCSC 2024).
Safe – Francja	Koordynuje działania badawczo-rozwojowe w zakresie cyberbezpieczeństwa, ze szczególnym naciskiem na działania zmierzające do stworzenia bezpiecznej infrastruktury. Ma być ona odporna na zaawansowane cyberataki na środowiska IoT tak, aby MŚP mogły bezpiecznie rozwijać swoją działalność w środowiskach wykorzystujących zaawansowane inteligentne systemy urządzeń i łączności bezprzewodowej (SAFE 2024).

Źródło: opracowanie własne.

Podsumowując, organizacje klastrowe pomagają definiować i rozpowszechniać najlepsze praktyki, które mogą być stosowane w różnych branżach. Ustanawiając standardy i promując środki bezpieczeństwa, klastry zapewniają, że firmy każdej wielkości mają narzędzia i wytyczne potrzebne do tworzenia bezpiecznej infrastruktury oraz budowania odporności całej gospodarki.

3. Zadania dla przedsiębiorstw z wykorzystaniem technologii cyfrowych. Rola i wsparcie klastrów.

Wykorzystanie technologii cyfrowych staje się kluczowym zadaniem dla przedsiębiorstw dążących do poprawy efektywności działań i budowania odporności w celu skutecznego przeciwdziałania różnorodnym zagrożeniom m.in.: fizycznym, zdrowotnym czy geopolitycznym. W niniejszym rozdziale autorzy opracowania proponują wyróżnienie kilku etapów transformacji cyfrowej, od zdobycia wiedzy, przez audyt technologiczny, planowanie wdrożenia, aż po implementację i doskonalenie rozwiązań. Jednocześnie wskazują, jak klastry wspierają te procesy, łącząc wiedzę i zasoby dla szybszego i efektywniejszego rozwoju technologicznego firm.

3.1. Pozyskanie wiedzy na temat technologii cyfrowych i możliwości ich zastosowania w przedsiębiorstwie

Członkostwo w organizacjach klastrowych oferuje MŚP możliwość zdobywania i pogłębiania wiedzy na temat technologii cyfrowych i rozwiązań w tym zakresie, wymiany doświadczeń, dostępu do ekspertów, technologii, a nawet wspólnych zakupów rozwiązań (zwiększając tym samym ich poziom zaawansowania i potencjalnie obniżając ponoszone koszty). Dzięki szkoleniom, współpracy, dostępowi do narzędzi, projektom badawczo-rozwojowym, doradztwu w zakresie technologii podwójnego zastosowania i usługom certyfikacyjnym, klastry pomagają MŚP w poruszaniu się po złożonym środowisku technologii cyfrowych, w tym również cyberbezpieczeństwa. Organizacje klastrowe mają potencjał by działać jako pomosty między MŚP, instytucjami badawczymi, dostawcami technologii, instytucjami, a nawet organami państwowymi, pomagając w ten sposób MŚP w podnoszeniu poziomu wiedzy, świadomości i bezpieczeństwa, a przez to radzenie sobie ze złożonymi wyzwaniami z zakresu szeroko rozumianego Przemysłu 4.0.

MŚP powinny wykorzystać członkostwo w klastrach w celu zdobywania wiedzy na temat technologii cyfrowych i ich skutecznego wykorzystania poprzez udział w różnorodnych inicjatywach klastrowych, takich jak:

1. Udział w szkoleniach, a przez to podnoszenie poziomu wiedzy i świadomości. Organizacje klastrowe organizują różnego rodzaju szkolenia, warsztaty, seminaria, a także konferencje i inne wydarzenia poświęcone w całości lub częściowo technologiom cyfrowym. Dzięki tym wydarzeniom MŚP mogą zdobyć praktyczną wiedzę na temat najnowszych zagrożeń, technologii i najlepszych praktyk, a dzięki sesjom warsztatowym z ekspertami mogą zdobyć wiedzę praktyczną. Praktycznie każda organizacja klastrowa posiada w swojej ofercie bardziej lub mniej rozwinięte usługi w tym zakresie. Oczywiście zależy to od branży, w której działa dany klaster (najbardziej rozwinięte jest to w klastrach IT oraz tych związanych z branżą przemysłową), a także od jego poziomu rozwoju. Dla przykładu organizacją,

która prowadzi warsztaty i szkolenia dotyczące konkretnych wyzwań związanych z cyberbezpieczeństwem jest ECSO. Tematyka dotyczy zagrożeń przed którymi stoją MŚP, takich jak phishing, ransomware i zgodność z przepisami dotyczącymi ochrony danych (GDPR/RODO). Dzięki tym warsztatom MŚP mogą zdobyć informacje na temat wykrywania zagrożeń, strategiach reagowania i ramach regulacyjnych (takich jak RODO), co umożliwia im skuteczniejsze zabezpieczenie swoich operacji. W Polsce podobną działalność prowadzi na przykład Klaster #CyberMadeInPoland.

2. Wymianę wiedzy i nawiązanie współpracy między MŚP, większymi firmami, instytutami badawczymi oraz ekspertami z zakresu określonych technologii. Dzięki aktywnemu udziałowi MŚP mogą być na bieżąco z pojawiającymi się nowościami, innowacjami i zagrożeniami. MŚP, dzięki członkostwu w klastrach, mają też większe możliwości dołączenia do projektów badawczo-rozwojowych, co pozwala im na wspólne opracowywanie rozwiązań dostosowanych do ich konkretnych potrzeb np. w zakresie cyberbezpieczeństwa. Takie zaangażowanie pomaga MŚP pozyskiwać i wypracowywać rozwiązania odpowiadające także na wyzwania branżowe.
3. Wsparcie procesu certyfikacji i standaryzacji, umożliwiające MŚP przyjęcie obowiązujących lub wypracowywanych standardów i ram działania np. w zakresie cyberbezpieczeństwa. Pomaga to MŚP zachować zgodność z przepisami UE i zwiększa ich wiarygodność w oczach partnerów, co obecnie może być kluczowym wyróżnikiem konkurencyjnym na rynkach globalnych. Proces certyfikacji jest kosztowny i może być bardzo skomplikowany, zwłaszcza dla mniejszych firm. Projekt CyberSec4Europe to finansowany przez UE projekt mający na celu opracowanie ram certyfikacji cyberbezpieczeństwa dla MŚP. Dzięki udziałowi w tym projekcie, którego jednym z filarów wspomagających realizację i dotarcie do MŚP są właśnie klastry, MŚP mogą uzyskać wskazówki dotyczące uzyskania certyfikacji zgodnie z europejskimi standardami cyberbezpieczeństwa. Projekt ten pomaga MŚP zapewnić zgodność ich działalności z najnowszymi wymogami regulacyjnymi UE.
4. Pozyskiwanie informacji na temat możliwości finansowania wdrożeń technologii cyfrowych. Często klastry w różny sposób pomagają MŚP ubiegać się o granty i dotacje, które można wykorzystać w tym obszarze poprzez zdobywanie wiedzy, rozwój i wdrażanie technologii. Finansowanie może być pozyskiwane indywidualnie lub w konsorcjach, których generatorem także mogą być klastry.
5. Zwiększenie aktywności przedsiębiorstw w pozyskiwaniu wiedzy na temat technologii cyfrowych oraz ich zastosowań np. poprzez dostęp do ekspertyz pozwala na wspieranie wdrożeń zmian organizacyjnych. Proces ten sprzyja akceptacji innowacji przez pracowników i stanowi pierwszy krok w realizacji transformacji cyfrowej, przygotowując firmę na wyzwania współczesnego rynku.

3.2. Analiza potrzeb danego przedsiębiorstwa w zakresie technologii cyfrowych (audyt technologiczny)

Aby skutecznie wdrażać rozwiązania technologii cyfrowych kluczowe znaczenie ma przeprowadzenie dogłębnej analizy w zakresie potrzeb i możliwości danego przedsiębiorstwa, czyli tzw. audyt technologiczny transformacji cyfrowej. Proces ten pomaga dostosować rozwiązania, procesy, procedury oraz zasoby do szczególnych wymagań branży przy jednoczesnym dostosowaniu się do najlepszych praktyk branżowych. Często wdrażanie technologii cyfrowych jest mniej skomplikowane i tańsze niż mogłoby się wydawać. Zazwyczaj głównym problemem w przypadku MŚP jest brak wiedzy oraz kwalifikacji (Balkan 2022). MŚP mogą małymi, acz systematycznymi działaniami podnosić swój poziom wiedzy oraz wdrażać i udoskonalać poszczególne rozwiązania. Częstym problemem wydaje się być też brak dostosowania oferty właśnie do potrzeb MŚP, przez co ponoszą one koszty na rozwiązania nie odpowiadające ich zapotrzebowaniu. Problem występuje również w kwestiach finansowania – MŚP rezygnują z pozyskiwania środków ponieważ np. minimalna wartość projektów jest zupełnie niedostosowana do ich potrzeb. Nieodpowiednio przeprowadzony proces wdrożenia nowego rozwiązania/ technologii może mieć negatywne skutki i obniżyć gotowość MŚP do kolejnych kroków transformacji cyfrowej.

Pierwszym krokiem dla MŚP może być nawiązanie współpracy z organizacjami wspomagającymi MŚP w obszarze wdrażania nowych technologii cyfrowych działającymi w ramach sieci klastrów. Organizacje te mają wiedzę, a często gotowe narzędzia pomagające w dokonaniu analizy i zrozumieniu obecnego stanu oraz określeniu potrzeb MŚP. Jeśli klastry nie posiadają takich rozwiązań czy możliwości, to często posiadają je ich członkowie będący dostawcą poszczególnych technologii.

Proces wstępnej analizy obejmuje identyfikację branży przedsiębiorstwa, jego zasobów cyfrowych, obecnej infrastruktury i ogólnej świadomości potrzeb i ryzyka. Celem jest zrozumienie poziomu cyfryzacji MŚP i stopnia wrażliwości danych, którymi się zajmują, a także identyfikacja odpowiednich zabezpieczeń procesowych i technologicznych zapewniających ochronę dostępu, procesów i krytycznych danych m.in.: poprzez ocenę bezpieczeństwa urządzeń, sieci i przemysłowych systemów sterowania.

Po wstępnej ocenie kluczowe znaczenie ma analiza poziomu świadomości w zakresie obecnych technologii w MŚP oraz korzyści jakie może przynieść ich wdrożenie. Obejmuje to ocenę tego, jak dobrze pracownicy znają technologie cyfrowe oraz podejście organizacji do przeprowadzania szkoleń. Wiele problemów z wdrażaniem nowych technologii wynika z błędów ludzkich, więc szkolenie i poprawa świadomości w tych zakresach są tutaj kluczowymi elementami. Niezwykle istotne jest też wprowadzenie właściwej kultury w zakresie cyberbezpieczeństwa, która powinna obejmować wszystkie działy i poziomy organizacji, a także powinna być aktywnie wspierana, wdrażana i stosowana przez zarząd i kadrę menadżerską.

Następnym krokiem powinno być przeprowadzenie kompleksowej analizy potrzeb, ryzyka i zagrożeń dla danej organizacji. Ten krok koncentruje się na identyfikacji konkretnych potrzeb i zagrożeń, które najprawdopodobniej wpłyną na MŚP, w oparciu o jego branżę, wielkość, charakterystykę prowadzonej działalności, poziom cyfryzacji oraz wykorzystywane technologie. Analiza powinna uwzględniać zarówno zagrożenia zewnętrzne, jak i zagrożenia wewnętrzne. Dobrym narzędziem wspomagającym może być w tym zakresie Cyberwatching.eu – europejska platforma, która oferuje narzędzia oceny ryzyka zaprojektowane specjalnie dla MŚP. Narzędzia te pomagają w identyfikacji i ustalaniu priorytetów ryzyka w oparciu o operacje biznesowe i podatności sektorowe badanych MŚP. Na przykład firmy z branży handlowej mogą skupić się na bezpieczeństwie płatności, a te z branży produkcyjnej mogą potrzebować rozwiązań ograniczających ryzyko związane z wykorzystaniem urządzeń IIoT i systemami przemysłowymi.

Dokładna analiza potrzeb przedsiębiorstwa w zakresie wdrażania technologii cyfrowych jako elementu budowania ich odporności i przeciwdziałania zagrożeniom jest niezwykle ważnym etapem procesu transformacji cyfrowej. Rzetelna i realna ocena potrzeb i możliwości wdrożenia technologii cyfrowych pozwoli na uniknięcie błędów związanych z nadmiernym wdrażaniem rozwiązań cyfrowych w jednym czasie lub wdrażaniem tych rozwiązań w nieodpowiedniej kolejności.

3.3. Opracowanie planu (mapy drogowej) wdrożenia

Kolejnym krokiem po zidentyfikowaniu potrzeb i możliwości przedsiębiorstwa jest opracowanie planu/mapy drogowej wdrożenia określonych rozwiązań (mapa/plan transformacji cyfrowej). Ich wdrożenie może być kluczowe dla dalszego rozwoju firmy i utrzymania bądź podniesienia jej pozycji konkurencyjnej na rynku. W przypadku środków cyberbezpieczeństwa kluczowe znaczenie dla małych i średnich przedsiębiorstw ma ochrona przed rosnącymi cyber zagrożeniami i zapewnienie ciągłości procesów produkcyjnych i biznesowych.

Plan transformacji cyfrowej (inaczej mapa transformacji) to zintegrowana strategia, która pomaga firmie zidentyfikować jak najlepiej wykorzystać technologie cyfrowe do zaspokojenia potrzeb klientów, zwiększenia efektywności operacyjnej i utrzymania konkurencyjności na dynamicznie zmieniającym się rynku. Bez opracowanej mapy każde przedsiębiorstwo może stracić cenne możliwości i zostać w tyle w szybko rozwijającej się globalnej cyfrowej gospodarce. Przez zrozumienie, jak i gdzie wprowadzić nowe technologie, przedsiębiorstwo może skoncentrować swoje zasoby tam, gdzie przyniosą one największe korzyści.

Można wyróżnić szereg korzyści dla przedsiębiorstwa z posiadania mapy drogowej transformacji cyfrowej. Są to między innymi :

1. Jasna wizja i wytyczne – mapa drogowa dostarcza przedsiębiorstwu jasnej wizji, gdzie chce się znaleźć w przyszłości i jakie cele chce osiągnąć dzięki transformacji cyfrowej. To pozwala na zrozumienie celów i kierunku działania przez wszystkich pracowników.
2. Skoncentrowane działania – dzięki mapie przedsiębiorstwo może skupić się na priorytetowych projektach i inwestycjach, które przyniosą największe korzyści w kontekście cyfrowej transformacji. Pozwala to uniknąć rozproszenia zasobów i czasu na mniej istotne działania.
3. Lepsze zarządzanie ryzykiem – mapa drogowa pozwala na identyfikację potencjalnych zagrożeń związanych z transformacją i wdrożeniem nowych technologii. Dzięki temu przedsiębiorstwo może podjąć odpowiednie działania zapobiegawcze lub przygotować się na ewentualne wyzwania.
4. Optymalizacja zasobów – mapa drogowa pomaga w określeniu potrzebnych zasobów, takich jak kapitał ludzki, finansowy i technologiczny, które są niezbędne do wdrożenia strategii cyfrowej transformacji. Pozwala to na bardziej efektywne alokowanie zasobów.
5. Podniesienie wydajności – poprzez dostosowanie procesów do nowoczesnych rozwiązań cyfrowych, przedsiębiorstwo może zwiększyć swoją wydajność i skuteczność operacyjną, co wpłynie pozytywnie na efektywność całej organizacji.

Aktualnie przedsiębiorcy, głównie z obszaru MŚP, stoją przed wieloma wyzwaniami, wśród których można wyróżnić m.in. niewystarczającą wiedzę o dostępnych technologiach, brak strategicznego podejścia do cyfrowej transformacji, a czasem wręcz opór pracowników przed zmianami. Opracowany dokument stanowi kierunkowy plan dla strategicznych decyzji inwestycyjnych, które mają na celu ogólną poprawę konkurencyjności, poprzez zwiększenie elastyczności, równocześnie zapewniając wzrost efektywności i wydajności oraz poprawę warunków pracy pracowników.

Mapa drogowa wraz z planem reagowania na incydenty jest również istotna z punktu widzenia cyberbezpieczeństwa. Postępując zgodnie z ustrukturyzowaną mapą opartą na najlepszych praktykach Unii Europejskiej, MŚP mogą podnieść poziom cyberbezpieczeństwa w organizacji i odporność na cyberataki, przygotowując się na potencjalne zakłócenia działalności operacyjnej.

3.4. Wdrożenie określonych technologii oraz ich stały monitoring i aktualizacja/doskonalenie

Wdrażanie mapy transformacji cyfrowej oraz odpowiednich technologii jest kolejnym etapem procesu. Następnym krokiem jest monitorowanie wdrożonych rozwiązań oraz aktualizacja i stałe doskonalenie systemu. Na tym etapie kluczową rolę odgrywają możliwości finansowania określonych technologii. Dlatego też tak ważne jest właściwe opracowanie mapy drogowej, aby zaproponowane rozwiązania były: odpowiednie dla danego przedsiębiorstwa, osiągalne finansowo i możliwe do wdrażania etapowo. Efektem końcowym całego przeprowadzonego procesu powinno być podniesienie konkurencyjności firmy i gotowość na sprawne funkcjonowanie na rynku.

Istotną częścią wdrażania mapy drogowej jest część dotycząca cyberbezpieczeństwa – przedsiębiorstwa powinny zbudować odpowiedni poziom bezpieczeństwa i odporności na cyber zagrożenia, w celu zapewnienia ciągłości działania i ochrony danych wrażliwych.

Samo monitorowanie procesów ma kluczowe znaczenie dla zapewnienia płynności i bezpieczeństwa operacji biznesowych w każdej firmie. Także MŚP powinny korzystać z narzędzi monitorujących systemy, infrastrukturę i sieci w celu wykrywania podejrzanych zachowań i działań, zwłaszcza w zakresie przetwarzania transakcji oraz funkcjonowania krytycznych systemów produkcyjnych i biznesowych.

Podsumowując, skuteczna transformacja cyfrowa przedsiębiorstwa i wdrażanie działań prewencyjnych przy wykorzystaniu technologii cyfrowych wymaga świadomego i systematycznego podejścia. Kluczowe etapy obejmują zdobycie wiedzy o możliwościach technologii cyfrowych, przeprowadzenie audytu technologicznego w celu identyfikacji potrzeb, opracowanie szczegółowego planu wdrożenia oraz implementację rozwiązań połączoną z ich monitorowaniem i doskonaleniem. W procesie tym szczególną rolę odgrywają klastry, które wspierają firmy poprzez dostęp do wiedzy eksperckiej, zasobów technologicznych i ułatwienie współpracy między różnymi podmiotami. Dzięki temu przedsiębiorstwa mogą skuteczniej wdrażać innowacje i zwiększać swoją konkurencyjność na rynku.

4. Katalog działań prewencyjnych z wykorzystaniem technologii cyfrowych dla przedsiębiorstw

W wielu wypadkach cyfrowa transformacja MŚP z którą mamy do czynienia w ostatnich latach, pomogła w osiągnięciu znacznie większej wydajności ich działania oraz budowaniu nowych przewag konkurencyjnych. Równocześnie coraz powszechniejsze wykorzystanie technologii cyfrowych zwiększa podatność firm na cyber zagrożenia. Cyberataki, takie jak ransomware lub sabotaż, a także inne zagrożenia, np. zakłócenia w łańcuchu dostaw mogą potencjalnie sparaliżować działalność MŚP, prowadząc do strat finansowych i utraty wiarygodności. Biorąc pod uwagę wkład MŚP w gospodarkę UE (stanowią one ponad 99% wszystkich przedsiębiorstw) ich dalszy rozwój ma kluczowe znaczenie dla ogólnej stabilności europejskiej gospodarki.

Rosnące znaczenie technologii cyfrowych oraz ich złożoność technologiczna stanowią poważne wyzwanie dla małych i średnich przedsiębiorstw, zwłaszcza w obliczu ostatnich wydarzeń na arenie międzynarodowej (pandemia, wojna hybrydowa i cyberataki związane z konfliktami zbrojnymi). MŚP są szczególnie narażone na cyber zagrożenia ze względu na ograniczone zasoby i niski poziom wiedzy technicznej na temat ich pokonywania. Cyberprzestępcy mają świadomość, że MŚP stanową bardzo łatwy cel i są podatne na wiele rodzajów cyberataków: od phishingu, przez ransomware, aż po ataki na infrastrukturę produkcyjną wykorzystującą niezabezpieczone inteligentne urządzenia. Zagrożenia te obejmują także sabotaż, awarie operacyjne, przerwy w łańcuchu dostaw i zakłócenia w dostawach energii.

Poniżej przedstawiono autorski katalog działań prewencyjnych z wykorzystaniem technologii cyfrowych zapobiegających niekontrolowanej utracie potencjału konkurencyjnego przedsiębiorstw. Można go podzielić na kilka kluczowych elementów:

1. Monitorowanie zagrożeń i predykcja ryzyka

Wdrożenie narzędzi cyfrowych do monitorowania otoczenia (zarówno do analiz bieżących, jak i predykcyjnych) w celu terminowego wykrycia zagrożeń, takich jak m.in.: cyberataki, zakłócenia łańcuchów dostaw czy zmiany regulacyjne. Wykorzystywane technologie cyfrowe opierają się głównie na zaawansowanych algorytmach analitycznych, sztucznej inteligencji oraz narzędziach do analizy Big Data. Umożliwiają również przedsiębiorstwom śledzenie zmian rynkowych, technologicznych, regulacyjnych i społecznych.

Kluczowe narzędzia i technologie:

1. algorytmy sztucznej inteligencji i uczenia maszynowego (AI/ML),
2. narzędzia analizy Big Data,
3. IoT – zbieranie danych z czujników i urządzeń w czasie rzeczywistym,
4. systemy zarządzania ryzykiem (GRC – Governance, Risk, Compliance),
5. narzędzia monitorowania mediów społecznościowych i Internetu,
6. narzędzia Business Intelligence (BI) – wizualizacja i analiza danych rynkowych,
7. platformy analizy rynku i konkurencji,
8. systemy geoinformacyjne (GIS) – monitorowanie zmian geograficznych i środowiskowych wpływających na biznes,
9. narzędzia predykcji makroekonomicznej (Bloomberg Terminal, Refinitiv Eikon),
10. monitoring technologiczny – śledzenie nowości technologicznych i patentów w branży.

2. Wdrożenie systemów cyberbezpieczeństwa

Ochrona systemów IT przed cyberatakami poprzez implementację zapór sieciowych, szyfrowania danych, systemów antywirusowych oraz testów penetracyjnych. Obejmuje następujące etapy działania:

1. Identyfikacja wszystkich krytycznych zasobów cyfrowych, w tym danych, oprogramowania i infrastruktury, które mogą zostać naruszone podczas cyberataku.
2. Mapowanie podatności w kontekście cyberbezpieczeństwa np. z wykorzystaniem narzędzi takich jak „Narzędzie samooceny cyberbezpieczeństwa" opracowane przez ENISA do mapowania podatności w różnych punktach infrastruktury IT (ENISA 2024a). Przy pomocy „Narzędzia samooceny cyberbezpieczeństwa" MŚP może samodzielnie przeprowadzić symulację możliwych cyber incydentów w celu dokonania oceny ich wpływu na możliwości technologiczne i operacje MŚP.
3. Zapewnienie ciągłości działania w obliczu cyber zagrożeń i odzyskiwanie danych po awarii. Planowanie ciągłości działania (Business Continuity Plan – BCP) (ENISA 2024b) i planowanie odtwarzania po awarii (Disaster Recovery Plan – DRP) (ENISA 2024c) powinny być integralnymi elementami strategii cyberbezpieczeństwa MŚP. Przykładami rekomendowanych narzędzi są m.in.: Plan Ciągłości Działania (BCP) i Disaster Recovery Plan (DRP). Opracowanie BCP ma na celu identyfikację procesów o znaczeniu krytycznym w organizacji i określenie kroków mających na celu utrzymanie tych procesów w obliczu zakłóceń wywołanych cyber zagrożeniami. Przy opracowaniu BCP należy wziąć pod uwagę takie scenariusze jak: ataki ransomware, phishing, sabotaż lub awaria infrastruktury. Wspomniana już ENISA przygotowała wytyczne dotyczące utrzymania ciągłości działania, specjalnie dostosowane dla MŚP. Z kolei Disaster Recovery Plan (DRP) koncentruje się na odzyskiwaniu danych i przywracaniu systemów po cyber ataku.
4. Zabezpieczenie przed sabotażem technologicznym oraz awariami infrastruktury i urządzeń. W tym obszarze niezwykle istotne będzie wdrożenie uwierzytelniania wieloskładnikowego (Multifactor Authentication – MFA). Zabezpieczenie dostępu do krytycznych zasobów cyfrowych poprzez zastosowanie uwierzytelniania wieloskładnikowego zapewnia, że tylko upoważniony personel może uzyskać dostęp do wrażliwych danych i systemów, zmniejszając ryzyko sabotażu spowodowanego bezprawnym użyciem danych uwierzytelniających. Niezwykle istotne jest też szyfrowanie danych i informacji zawierających własność intelektualną oraz krytyczne dane wykorzystywane w procesach biznesowych i produkcyjnych.
5. Zastosowanie najnowocześniejszych technologii w zapobieganiu efektom cyber ataków, np. poprzez wykorzystanie cyfrowych bliźniaków do zarządzania kryzysowego i utrzymania procesów.

Kluczowe narzędzia i technologie:

1. zapory sieciowe (firewalls),
2. systemy wykrywania i zapobiegania włamaniom do sieci komputerowych – Intrusion Detection System (IDS)/Intrusion Prevention System (IPS),
3. oprogramowanie antywirusowe i antymalware,
4. zarządzanie tożsamością i dostępem (Identity and Access Management – IAM) – zarządzanie pełnym cyklem życia tożsamości i uprawnień użytkowników we wszystkich zasobach przedsiębiorstwa oraz podstawowa kontrola bezpieczeństwa chmury,
5. szyfrowanie danych,
6. platformy zarządzania bezpieczeństwem informacji i zdarzeń – systemy SIEM (Security Information and Event Management) umożliwiające skuteczne wykrywanie i reagowanie na zagrożenia bezpieczeństwa poprzez analizowanie informacji i raportowanie ich z różnych źródeł i baz danych,
7. zabezpieczenie urządzeń końcowych, takich jak komputery, laptopy i smartfony – ochrona punktów końcowych (Endpoint Protection Platforms – EPP),
8. systemy analizy zachowania użytkowników – User Behaviour Analytics (UBA) –

wykrywanie anomalii w zachowaniu użytkowników w celu identyfikacji potencjalnych zagrożeń,
9. chmurowe zabezpieczenia danych (Cloud Security).

3. Organizacja szkoleń i budowanie świadomości pracowników

Regularne szkolenia dla pracowników w zakresie identyfikacji zagrożeń, takich jak phishing oraz procedury postępowania w sytuacjach kryzysowych. Budowanie świadomości zagrożeń wśród pracowników i organizacja skutecznych programów szkoleniowych, dostosowanych do specyfiki i potrzeb przedsiębiorstwa.

Kluczowe narzędzia i technologie:

1. platformy e-learningowe,
2. symulatory i gry edukacyjne (gamifikacja),
3. narzędzia do webinarów i wideokonferencji,
4. narzędzia do zarządzania szkoleniami (Learning Management Systems – LMS),
5. chatboty edukacyjne i asystenci AI,
6. mobilne aplikacje szkoleniowe,
7. rozszerzona i wirtualna rzeczywistość (AR/VR) – szkolenie pracowników i wizualizacja procesów np. logistycznych.

4. Tworzenie kopii zapasowych i planów odzyskiwania danych

Regularne tworzenie kopii zapasowych kluczowych danych w lokalizacjach fizycznych i chmurowych, zgodnie z zasadą 3-2-1 (CISA 2012), opracowanie strategii szybkiego przywracania funkcjonowania systemów w przypadku awarii poprzez opracowanie planu przywracania działania po awarii (plany odzyskiwania danych – Disaster Recovery Plan – DRP).
Kluczowe narzędzia i technologie:

1. systemy do tworzenia kopii zapasowych (Backup Solutions),
2. chmurowe rozwiązania do backupu (Cloud Backup),
3. platformy zarządzania odzyskiwaniem danych (Disaster Recovery Platforms),
4. systemy ochrony i replikacji danych,
5. oprogramowanie do tworzenia obrazów systemów,
6. narzędzia do testowania planów DRP.

5. Tworzenie inteligentnych łańcuchów dostaw

Zastosowanie technologii IoT oraz analityki predykcyjnej do monitorowania i optymalizacji procesów w łańcuchu dostaw. Poszukiwanie nowych dostawców, a tym samym zapewnienie ciągłości dostaw na wypadek zagrożenia powinno stanowić bardzo istotne działanie prewencyjne i odbywać się w sposób ciągły.

Kluczowe narzędzia i technologie:

1. IoT – śledzenie lokalizacji i stanu towarów w czasie rzeczywistym,
2. AI i ML – predykcja popytu, optymalizacja tras i analiza danych,
3. Blockchain – zapewnienie przejrzystości i bezpieczeństwa transakcji w łańcuchu dostaw,

4. Big Data – przetwarzanie dużych ilości danych w celu identyfikacji trendów i optymalizacji procesów,
5. robotyka i automatyzacja – automatyzacja magazynowania, kompletowania zamówień i transportu wewnętrznego,
6. druk 3D – produkcja elementów na żądanie, co redukuje konieczność utrzymywania zapasów,
7. cyfrowy bliźniak (Digital Twin) – tworzenie wirtualnych modeli fizycznych łańcuchów dostaw w celu symulacji i analizy,
8. Systemy do zarządzania produkcją i działalnością organizacji:
    - 8.1 planowanie zasobów przedsiębiorstwa (Enterprise Resource Planning – ERP),
    - 8.2 planowanie zapotrzebowania materiałowego (Material Requirements Planning – MRP),
    - 8.3 zarządzanie łańcuchem dostaw (Supply Chain Management – SCM),
    - 8.4 zarządzanie procesami biznesowymi (Business Process Management – BPM),
    - 8.5 zarządzanie relacjami w przedsiębiorstwie (Employee Relationship Management – ERM),
    - 8.6 zarządzanie relacjami z klientami (Customer Relationship Management – CRM).

6. Tworzenie systemów symulacji i testowania

Wdrożenie platform do testowania odporności systemów na różne scenariusze kryzysowe oraz wykorzystania foresightu technologicznego i predykcji przyszłych zdarzeń na postawie posiadanych danych. Ponadto testowe wykorzystanie technologii i eksperymentowanie przed podjęciem decyzji o jej wdrożeniu.

Kluczowe narzędzia i technologie:

1. modelowanie i symulacja procesów (Process Simulation Tools),
2. rozszerzona i wirtualna rzeczywistość (AR/VR),
3. narzędzia do symulacji scenariuszy awaryjnych – analiza skutków zagrożeń takich jak awarie technologiczne czy katastrofy naturalne,
4. systemy CAE (Computer-Aided Engineering) – symulacja zachowań produktów w środowisku wirtualnym przed ich produkcją,
5. systemy do symulacji i testowania w infrastrukturze IT – testowanie aplikacji, infrastruktury sieciowej i zabezpieczeń,
6. cyfrowy bliźniak (Digital Twin) – wykorzystanie do symulacji operacji i procesów w środowisku wirtualnym, zwłaszcza w obszarze produkcji i logistyki, przewidywania potencjalnych awarii i optymalizacji reakcji w sytuacjach kryzysowych. Cyfrowy bliźniak może także przewidywać, za pomocą analityki predykcyjnej, kiedy sprzęt lub procesy mogą ulec awarii, umożliwiając proaktywne serwisowanie. Może to pozwolić na skrócenie potencjalnych przestojów i zapobiegać zakłóceniom procesów produkcyjnych.

7. Monitorowanie procesu wdrażania technologii cyfrowych

Powodzenie implementacji strategii cyfryzacji w celu budowania odporności i poprzez podejmowanie działań prewencyjnych warunkuje kilka ważnych elementów, takich jak (Fałkowski i in. 2024):

1. przekazanie kompetencji menedżerowi projektu odpowiedzialnemu za proces wdrożenia zmian,
2. zachowanie równowagi pomiędzy czasem wdrażania technologii a utrzymaniem ciągłości procesów – zbyt długie przerwy w realizacji procesów biznesowych negatywnie wpłyną na ich efektywność, a w efekcie na wynik finansowy,
3. regularna aktualizacja oprogramowania,
4. kontrola dostępu i uprawnień – wdrażanie systemów zarządzania tożsamościami oraz regularne przeglądy dostępów,
5. szyfrowanie danych – zwłaszcza wrażliwych (np. dla bezpieczeństwa narodowego) oraz informacji biznesowych.

Kluczowe narzędzia i technologie:

1. systemy zarządzania projektami (Project Management Tools),
2. system ERP,
3. platformy BI (Business Intelligence),
4. systemy do monitorowania chmurowego – śledzenie wdrażania technologii opartych na chmurze,
5. platformy do automatyzacji i integracji (Robotic Process Automation – RPA i Integration Platform as a Service – iPaaS),
6. narzędzia DevOps do monitorowania wdrażania technologii IT w środowisku produkcyjnym,
7. specjalistyczne narzędzia IT do audytu wdrożeń.

8. Współpraca w ramach klastrów

Dodatkowe korzyści w podejmowaniu działań prewencyjnych wynikające z możliwości wymiany wiedzy i zasobów technologicznych, podejmowania wspólnych inicjatyw finansowania badań i projektów wdrożeniowych oraz organizowania warsztatów i konsultacji. Kluczowe narzędzia i technologie:

- platformy komunikacyjne i współpracy,
- systemy analizy danych i Business Intelligence,
- cyfrowe platformy współpracy klastrowej – np. ECCP,
- systemy GIS (Geographic Information Systems) – lokalizowanie i mapowanie potencjalnych zagrożeń środowiskowych i logistycznych,
- cyberbezpieczeństwo,
- Internet Rzeczy (IoT), Blockchain, sztuczna inteligencja i uczenie maszynowe (AI i ML), wirtualna rzeczywistość (VR).

9. Współpraca z agencjami bezpieczeństwa narodowego

Ustanowienie kanałów komunikacji z odpowiednimi organami rządowymi w celu wymiany informacji o aktualnych zagrożeniach. Zaleca się aktywną współpracę z instytucjami bezpieczeństwa narodowego w celu wymiany informacji na temat potencjalnych zagrożeń, a także skorzystania z ich eksperckiej wiedzy. Ponadto rekomenduje się wspieranie inicjatyw związanych z obowiązkowym i szybkim zgłaszaniem incydentów bezpieczeństwa narodowego w odpowiednich instytucjach oraz przestrzeganie standardów bezpieczeństwa narodowego (Fałkowski i in. 2024).

Kluczowe narzędzia i technologie:

1. bezpieczne platformy komunikacyjne i wymiany danych,
2. systemy analizy danych w czasie rzeczywistym,
3. narzędzia do monitorowania infrastruktury krytycznej,
4. AI i ML – predykcja zagrożeń, analiza ryzyka i wspieranie decyzji w działaniach prewencyjnych,
5. systemy GIS – wspomagają mapowanie i analizę geograficzną potencjalnych zagrożeń,
6. cyberbezpieczeństwo i systemy wykrywania zagrożeń,
7. platformy e-learningowe i szkoleniowe,
8. narzędzia do zarządzania incydentami (Incident Response Tools).

Permanentna realizacja powyższych działań prewencyjnych, przy wsparciu technologii cyfrowych, pozwoli przedsiębiorstwom nie tylko zmniejszyć ryzyko wystąpienia kryzysów, ale również skutecznie reagować na potencjalne zagrożenia, budując odporność i wzmacniając ich pozycję rynkową. Zdaniem autorów niniejszego raportu wybór, zaplanowanie i wdrożenie działań odpowiednich dla potrzeb danego przedsiębiorstwa, może stanowić istotny element działań prewencyjnych dla firm.

Zakończenie

Niniejszy raport miał na celu opracowanie dla przedsiębiorstw (głównie MŚP) katalogu działań prewencyjnych z wykorzystaniem technologii cyfrowych zapobiegających niekontrolowanej utracie ich potencjału konkurencyjnego wobec zagrożeń zewnętrznych, m.in. fizycznych, zdrowotnych czy geopolitycznych. Szczególną uwagę poświęcono roli klastrów we wsparciu działań prewencyjnych podejmowanych w procesie budowania odporności przedsiębiorstw i radzenia sobie z sytuacjami kryzysowymi.

Technologie cyfrowe odgrywają kluczową rolę w budowaniu odporności przedsiębiorstw. Narzędzia takie jak systemy wczesnego ostrzegania, platformy komunikacyjne, sztuczna inteligencja w zarządzaniu kryzysowym oraz cyberbezpieczeństwo są niezbędne zarówno na poziomie organizacji, jak i w ramach wsparcia ze strony państwa, wzmacniając zdolność firm do radzenia sobie z wyzwaniami i utrzymania konkurencyjności. Systemy wczesnego ostrzegania i cyfrowe platformy komunikacyjne wspierają reakcję na kryzysy, umożliwiając szybkie informowanie o zagrożeniach, takich jak klęski żywiołowe czy cyberataki, oraz sprawną wymianę danych między firmami a państwem. Sztuczna inteligencja i automatyzacja usprawniają zarządzanie kryzysowe poprzez analizę danych, monitorowanie sytuacji i wspieranie decyzji. W cyfrowym świecie cyberbezpieczeństwo stanowi fundament ochrony gospodarek i społeczeństw, zapewniając stabilność na poziomie lokalnym i międzynarodowym.

Skuteczne przeciwdziałanie zagrożeniom i wzmacnianie odporności przedsiębiorstw wymaga przemyślanego i systematycznego podejścia. Kluczowe kroki to poznanie możliwości technologii cyfrowych, przeprowadzenie audytu w celu określenia potrzeb, opracowanie szczegółowego planu wdrożenia oraz implementacja rozwiązań wraz z ich stałym monitorowaniem i ulepszaniem. Ważną rolę w tym procesie odgrywają klastry, które wspierają firmy, zapewniając dostęp do wiedzy eksperckiej, zasobów technologicznych oraz ułatwiając współpracę między podmiotami.

Dla przedsiębiorstw rekomendowane są działania prewencyjnie z wykorzystaniem technologii cyfrowych obejmujące następujące procesy i inicjatywy:

1. monitorowanie zagrożeń i predykcję ryzyka,
2. wdrażanie systemów cyberbezpieczeństwa,
3. organizację szkoleń i budowanie świadomości pracowników,
4. tworzenie kopii zapasowych i planów odzyskiwania danych,
5. tworzenie inteligentnych łańcuchów dostaw,
6. tworzenie systemów symulacji i testowania,
7. monitorowanie procesu wdrażania technologii cyfrowych,
8. współpracę w ramach klastrów,
9. współpracę z agencjami bezpieczeństwa narodowego.

Aby zapobiegać ryzyku niskiej odporności w obliczu kryzysu kluczowe jest wkomponowanie tych działań na rzecz budowania odporności w codzienną działalność przedsiębiorstw. Pozwala to również na zmniejszanie wysokiego ryzyka niekontrolowanej utraty potencjału konkurencyjnego w dobie obecnych zagrożeń zewnętrznych.

Bibliografia

1. Arroyabe M. F., Arranz C. F. A., De Arroyabe I. F., de Arroyabe J. C. F. (2024), Revealing the realities of cybercrime in small and medium enterprises: understanding fear and taxonomic perspectives, https://www.sciencedirect.com/science/article/pii/S0167404824001275
2. Asseco Data Systems (2024), https://www.assecods.pl/
3. Balkan N. (2022), Barriers to digitally transform SMEs in Europe, https://www.digitalsme.eu/barriers-to-digitally-transform-smes-in-europe/
4. BCSC (2024) https://www.ciberseguridad.eus/empresa-segura
5. CCfCS (2024), https://www.cyber.gc.ca/en/about-cyber-centre
6. CCTX (2024), https://cctx.ca/about-cctx/
7. CDC (2024), https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world
8. CI (2017), https://www.ipa.go.jp/en/about/activities/security-action.html
9. CISA (2012) Data Backup Options, 2012, https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
10. ComCERT (2024), https://www.comcert.pl/
11. CSJ (2021), https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou--en.pdf
12. Cyfrowa Polska (2022), Cyberbezpieczeństwo urządzeń końcowych po 2022 roku.
13. CyManII (2024), https://cymanii.org/about-us/
14. Delloite (2023). Tech Trends 2023. https://www2.deloitte.com/content/dam/insights/articles/us175897_tech-trends-2023/DI_tech-trends-2023.pdf
15. Drążek Z., Komorowski T.M. (red). (2021), Informatyka i zarządzanie. Problemy i wyzwania gospodarki cyfrowej. Wydawnictwo TNOiK Toruń.
16. DTS (2024), https://www.digitalsupercluster.ca/projects/
17. Easterly J. (2023), The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years,
18. ECSO (2024), https://ecs-org.eu/who-we-are/
19. ECT (2024), https://itl.ee/en/cybertech/#our-offerings
20. Eisenmann T.R., Parker G., Van Alstyne M. (2006). Strategies for Two-Sided Markets. Harvard Business Review
21. ENISA (2024), https://www.enisa.europa.eu/
22. ENISA (2024a), https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/
23. ENISA (2024b), https://www.enisa.europa.eu/publications/example-bcp-template
24. ENISA (2024c), https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management
25. Fałkowski A., Gorynia M., Kuczewska J., Pietrusewicz K. (2024), Identyfikacja luki cyfrowej oraz zagrożeń wynikających z wprowadzania technologii cyfrowych do przedsiębiorstw Przegląd międzynarodowy i krajowy, https://przemyslprzyszlosci.gov.pl/uploads/2024/06/2024_1_Identyfikacja-luki-cyfrowej-oraz-zagrozen-1.pdf
26. Fałkowski A., Gorynia M., Kuczewska J., Pietrusewicz K. (2024a), Zagrożenia dla przedsiębiorstw sektora MŚP i interesu narodowego w erze cyfryzacji Rekomendacje i dobre praktyki, https://przemyslprzyszlosci.gov.pl/uploads/2024/06/2024_2-Zagrozenia-dla-przedsiebiorstw-sektora-MSP-i-interesu-narodowego-1.pdf
27. Frankowicz K. (2017),WannaCry Ransomware, https://cert.pl/posts/2017/05/wannacry-ransomware/
28. Gartner (2023). Gartner Top 10 Strategic Technology Trends for 2023. https://

www.gartner.com/en/articles/gartner-top-10-strategic-technology-trends-for-2023
29. GDPR.pl (2017). WannaCry – najbardziej spektakularny atak w historii. https://gdpr.pl/wannacry-najbardziej-spektakularny-atak-w-historii
30. Gorynia M., Jankowska B. (2013). The Influence of Poland's Accession to the Euro Zone on the International Competitiveness and Internationalisation of Polish Companies. Wydawnictwo Difin.
31. Gorynia M., Jankowska B., Owczarzak R., Bartosik-Purgat M. (2005). Strategie firm polskich wobec ekspansji inwestorów zagranicznych. Organizacja i Kierowanie, 3(121), 9–26.
32. Gorynia M., Jankowska, B. (2008). Klastry a międzynarodowa konkurencyjność i internacjonalizacja przedsiębiorstwa. Wydawnictwo Difin.
33. Gorynia, M. (red.) (2002). Luka konkurencyjna na poziomie przedsiębiorstwa a przystąpienie Polski do Unii Europejskiej. Wydawnictwo Akademii Ekonomicznej w Poznaniu.
34. GovTech (2024), https://www.gov.pl/web/govtech/o-nas
35. https://hub4industry.pl/
36. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
37. ICSCoE (2024), https://www.ipa.go.jp/en/about/org/icscoe/index.html
38. Komisja Europejska (2020). Kształtowanie cyfrowej przyszłości Europy.https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020DC0067&qid=1700320178383
39. Komisja Europejska (2021). Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021DC0118&qid=1700318511296.
40. Komisja Europejska (2022) Dyrektywa NIS2 https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive
41. KPMG & Microsoft (2024), Monitor Transformacji Cyfrowej Biznesu. Odkrywanie nieznanych ścieżek w cyfrowym świecie, https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/04/pl-Monitor-Transformacji-Cyfrowej-Biznesu-Edycja-2024-KPMG-Microsoft.pdf
42. KSC (2024), https://www.kri.or.jp/en/
43. Kuczewska J. (2020). Benchmarking jako metoda diagnozy konkurencyjności przedsiębiorstw. Wydawnictwo Uniwersytetu Gdańskiego.
44. Łożykowski A., Sarnowski J. (2019), GovTech, czyli nowe technologie w sektorze publicznym, Polski Instytut Ekonomiczny, Warszawa. https://www.gov.pl/web/govtech/o-nas
45. McKinsey (2023). Technology Trends Outlook 2023. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech
46. MSWiA (2024), https://www.gov.pl/web/mswia/regionalny-system-ostrzegania
47. Palmen L., Baron M. (2016), Przewodnik dla animatorów inicjatyw klastrowych. Polska Agencja Rozwoju Przedsiębiorczości.
48. Poszytek P., Lis M., Jefmański B., Fila J., Jeżowski M., Kotelska J. (2024). Transformacja cyfrowa przedsiębiorstw w dobie Przemysłu 4.0. Wydawnictwo Akademia WSB
49. SAFe (2024), https://www.safecluster.com/offre-de-service/
50. Sienkiewicz-Małyjurek K. (2024). Możliwości i problemy zastosowania sztucznej inteligencji w zarządzaniu kryzysowym. Bezpieczeństwo Teoria i Praktyka, 1 (LIV), 43-60.
51. SMiL (2024), https://securitymadein.lu/
52. SS (2024), https://silicon-saxony.de/en/services/
53. Wood 2023, Wood K., 2023, Cybersecurity Policy Responses to the Colonial Pi-

peline Ransomware Attack, https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/

54. Wyzwania i możliwości. Polska, Europa, Świat, https://cyfrowapolska.org/wp-content/uploads/2023/09/Raport_Cyberbezpieczenstwo-urzadzen-koncowych_2023.pdf
55. Zoleński W.(2005). Systemy wczesnego ostrzegania w przedsiębiorstwie. Zeszyty Naukowe Politechniki Śląskiej, 27 (1681), 361–378.

Spis tabel: