

AKADEMIA SZTUKI WOJENNEJ



**AKADEMICKIE CENTRUM
ANALIZ STRATEGICZNYCH**

MYŚL STRATEGICZNA

Nr 2 (2) 2025

Warszawa 2025

Rada Naukowa

prof. dr hab. Mirosław Karpiuk (Uniwersytet Warmińsko-Mazurski w Olsztynie) –
przewodniczący
dr hab. Dominik Bierecki, prof. UP (Uniwersytet Pomorski w Słupsku)
dr hab. Małgorzata Czuryk, prof. UWM (Uniwersytet Warmińsko-Mazurski w Olsztynie)
dr hab. Krzysztof Drabik, prof. UwS (Uniwersytet w Siedlcach)
gen. bryg. dr hab. inż. Mariusz Fryc, prof. ASzWoj (Akademia Sztuki Wojennej w Warszawie)
Eriks Jekabsons, PhD (Maria Curie-Skłodowska University, University of Latvia, Latvia)
Gediminas Kazėnas, PhD (Mykolas Romeris University, Vilnius, Lithuania)
dr hab. Marek Klimek, prof. UKEN (Uniwersytet Komisji Edukacji Narodowej w Krakowie)
dr hab. Justyna Kurek-Sobieraj, prof. ASzWoj (Akademia Sztuki Wojennej w Warszawie)
prof. dr hab. Andrzej Pieczywok (Uniwersytet Kazimierza Wielkiego w Bydgoszczy)
dr hab. Michał Polak, prof. PK (Politechnika Koszalińska)
Prof. Dmytro Shevchuk (The National University of Ostroh Academy, Ukraine)
George Soroka, PhD (Harvard University, USA)
Prof. Vaja Vardidze (Sulkhan-Saba Orbeliani University, Tbilisi, Georgia)

Redakcja

Redaktor naczelny: prof. dr hab. Adam Jelonek
Sekretarz: dr Krzysztof Kaczmarek
Członkowie: dr Justyna Olędzka, dr Maciej Gurtowski

Projekt okładki: Krzysztof Fryc

ISSN 3071-9305

Adres wydawcy/redakcji

Akademickie Centrum Analiz Strategicznych
Akademia Sztuki Wojennej w Warszawie
Al. gen. A. Chruściela „Montera” 103
00-910 Warszawa

Spis treści

Tomasz Gergelewicz	
Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT	5
Mirosław Karpiuk	
Monitorowanie zagrożeń cyberbezpieczeństwa oraz incydentów na poziomie krajowym przez CSIRT NASK i CSIRT GOV	33
Dorota Sylwia Majewicz	
Linguistic Nuances in Crisis Communication: Advancing Conflict Mediation and Defense Education in Poland.....	44
Mariusz Domżański	
Fakultatywne zwolnienie ze służby funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego	58
Dariusz Andrzej Magierek	
Ciągłość działania w przedsiębiorstwie z punktu widzenia bezpieczeństwa	77
Kazimierz Pawelec	
Wyjaśnienia oskarżonych i podejrzanych a ich wpływ na bezpieczeństwo prawne.....	101

Tomasz Gergelewicz

Ministerstwo Obrony Narodowej

ORCID: 0000-0002-9145-5099

t.gergelewicz@wp.pl

Wykorzystanie potencjału sztucznej inteligencji w siłach zbrojnych – wywiad z Chatem GPT

Streszczenie

Wdrożenie systemów opartych na sztucznej inteligencji do obszarów funkcjonowania sił zbrojnych tworzy nowe zdolności, które w dużym stopniu odciążają dotychczas wykorzystywane mechanizmy. Wskazano szanse dla sił zbrojnych wynikające z użycia sztucznej inteligencji, jednocześnie podkreślono wyzwania, jakie tworzy użycie tej zaawansowanej technologii. Celem artykułu jest przedstawienie potencjału implementacji sztucznej inteligencji na potrzeby wojska i zestawienie go z treścią wygenerowaną podczas wywiadu przez Chat GPT, w odpowiedzi na pytania dotyczące różnych obszarów wykorzystania sztucznej inteligencji na potrzeby wojska.

Ponadto autor zaproponował skalę autonomii sztucznej inteligencji, a także zdefiniował trzy zasadnicze obszary, które należy opanować, żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko jej niepożądanego działania.

Wykorzystano metodę analityczną do wyodrębnienia obszarów zastosowania sztucznej inteligencji na potrzeby armii i wskazania potencjalnych kierunki jej wdrożenia. Zastosowano syntezę, żeby zaproponować skalę autonomiczności systemu względem decyzji człowieka. Posłużono się metodą wywiadu eksperckiego do zbadania jak sztuczna inteligencja ocenia własny potencjał do wykorzystania na potrzeby wojska.

We wnioskach wskazano, że treści generowane przez sztuczną inteligencję względem swojego własnego zastosowania w obszarze funkcjonowania wojska są zaawansowane, a Chat GPT może stanowić wartościowe narzędzie informacyjne, jako jedno z istotnych źródeł budowania świadomości sytuacyjnej.

Słowa kluczowe

Analiza przeprowadzona przez autora, a także wskazania samej sztucznej inteligencji świadczą o wielu korzyściach implementacji sztucznej inteligencji w siłach zbrojnych. Jednocześnie należy mieć świadomość wielu zagrożeń z tym związanych, ze względu na podatności, jakie to rozwiązanie obecnie tworzy.

sztuczna inteligencja, siły zbrojne, bezpieczeństwo, systemy autonomiczne, Chat GPT

Wstęp

Siły zbrojne jako wysoce wykwalifikowany instrument obrony państwa potrzebują nowoczesnych technologii, żeby sprostać coraz to nowym wyzwaniom i zagrożeniom. Sztuczna inteligencja jest technologicznym kołem napędowym naszych czasów, ale jej dwubiegowość skłania do głębszej refleksji nad jej dalszym rozwojem. Atrakcyjność wykorzystania sztucznej inteligencji jest ściśle związana z jej zdolnością do adaptacji i samouczenia się, możliwościami analitycznymi i predykcyjnymi, które umożliwiają tworzenie zaawansowanych i inteligentnych systemów. Jedną z najważniejszych zalet sztucznej inteligencji jest możliwość operowania ogromną ilością danych i podejmowanie na ich podstawie określonych działań: „Algorytmy stanowiące część AI mogą podejmować autonomiczne decyzje w oparciu o analizę dużych zbiorów danych, samodzielnie korygować błędy i podejmować decyzje w oparciu o wcześniejsze doświadczenie. Biorąc to pod uwagę, można je stosować tam, gdzie konieczna jest szybka analiza informacji i identyfikacja wzorców i współzależności. Pozwala to AI znaleźć optymalne rozwiązania danego problemu w nieporównywalnie krótszym czasie niż byłby potrzebny człowiekowi”¹. Świat sztucznej inteligencji doświadczył niezwyklej ewolucji, zwłaszcza w dziedzinie przetwarzania języka naturalnego. Duże modele językowe² takie,

- 1 K. Kaczmarek, M. Karpiuk, U. Soler, *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo E Società” 2024, t. 20, nr 2, s. 142.
- 2 Large Language Models (LLM) – duże modele językowe. To modele głębokiego uczenia, które są wstępnie trenowane na ogromnych ilościach danych. Podstawowym elementem jest zestaw sieci neuronowych, które wyodrębniają znaczenia z sekwencji tekstu i rozumieją relacje między słowami i frazami. Zob. *What is LLM (Large Language Model)?*, <https://aws.amazon.com/what-is/large-language-model/> [dostęp: 20.12.2024].

jak: Chat GPT firmy OpenAI, Bard firmy Google czy Claude firmy Anthropic, są najlepszymi przykładami ewolucji tej nowoczesnej technologii. Modele te są katalizatorami interakcji pomiędzy ludźmi a platformami cyfrowymi³. Jednakże rozwiązania wykorzystujące sztuczną inteligencję nie są doskonałe, są bowiem obarczone niedoskonałością człowieka, który ją tworzy, oraz możliwościami ingerencji w jej działanie przez wrogich aktorów. Ponadto istnieje prawdopodobieństwo wytworzenia przez sztuczną inteligencję informacji nieprawdziwej, co z zastosowaniem śmiertelnej broni może okazać się tragiczne w skutkach.

Celem artykułu jest przedstawienie potencjału wykorzystania sztucznej inteligencji na potrzeby wojska i zestawienie go z treścią wygenerowaną przez Chat GPT⁴ w odpowiedzi na pytania dotyczące różnych obszarów wdrożenia sztucznej inteligencji na potrzeby armii. Autor wykorzystał metodę analityczną, żeby wyodrębnić obszary zastosowania sztucznej inteligencji na potrzeby sił zbrojnych, a także wnioskuje, żeby wskazać potencjalne kierunki jej implementacji. Wykorzystał także metodę wywiadu eksperckiego⁵ do przeprowadzenia wywiadu ze sztuczną inteligencją. Ponadto zastosował syntezę, żeby zaproponować skalę autonomii systemu względem człowieka, a także zdefiniował trzy podstawowe obszary, które należy opanować, żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko jej niepożądanego działania.

Autonomia a całkowita samodzielność sztucznej inteligencji

Jednym z głównych powodów wykorzystania sztucznej inteligencji w przypadku systemów uzbrojenia jest dążenie do samodzielności systemu w wykonaniu zadania. Docelowo ta samodzielność ma dotyczyć wszystkich etapów

- 3 *Comparative Analysis between OpenAI ChatGPT, Google Bard, Anthropic Claude, and Google Gemini*, <https://medium.com/@DigitalQuill.ai/comparative-analysis-between-chatgpt-bard-claude-and-gemini-ai-llms-30b7a4488c5d> [dostęp: 13.11.2024].
- 4 Chat GPT (Generative Pre-Trained Transformer) to program sztucznej inteligencji, który generuje naturalny dialog. Wykorzystuje algorytm uczenia maszynowego do przetwarzania i analizowania dużych ilości danych w celu opracowania odpowiedzi na zapytania użytkowników. Poprzez przetwarzanie języka jest w stanie zrozumieć język ludzki w jego naturalnym środowisku, tj. używany przez ludzi w sposób naturalny. Zob. *Chat GPT: What is it?*, <https://uca.edu/cetal/chat-gpt> [dostęp: 13.11.2024].
- 5 Autor 21 marca 2025 r. przeprowadził wywiad z darmową wersją Chat GPT-4-turbo dla system operacyjnego iOS.

realizacji misji, od zaplanowania operacji, zebrania i analizy danych, po podjęcie decyzji na polu walki. Dlatego należy wyjaśnić pojęcia „samodzielność” i „autonomiczność”. Według słownika języka polskiego autonomia to: „samodzielność i niezależność w decydowaniu o sobie [...] niezależność od norm etycznych zewnętrznych, innych niż własne sumienie”⁶. Portal polszczyzna.pl podaje, że „[...] w odniesieniu do człowieka autonomia to samodzielność i niezależność, która przejawia się swobodą działania i posiadaniem możliwości decydowania o sobie i rządzeniu się własnymi prawami, bez narzucania ich przez inne osoby”⁷. Według publikacji Komisji Europejskiej pt. „The Assessment List For Trustworthy Artificial Intelligence” autonomiczny system sztucznej inteligencji to system, który wykonuje zachowania lub zadania z dużym stopniem autonomii, czyli bez zewnętrznego wpływu (np. bez udziału człowieka)⁸. Autorzy encyklopedii zarządzania stwierdzają, że „[...] autonomia odnosi się do stopnia, w jakim pracownicy mają możliwość podejmowania decyzji i działania samodzielnie, bez nadzoru i kontroli ze strony przełożonych” i uszczegóławia, że „[...] ważne jest jednak zrozumienie, że autonomia nie oznacza całkowitego braku nadzoru. Chociaż autonomia daje pracownikom większą swobodę w podejmowaniu decyzji, nadal istnieje potrzeba monitorowania ich działań i zapewnienia, że decyzje podejmowane są zgodne z celami organizacji. W związku z tym, ważne jest ustalenie granic autonomii i jasne zdefiniowanie zakresu decyzji, które pracownicy mogą podejmować samodzielnie”⁹. Rafał Rejmانيak podkreśla, że autonomiczność systemów sztucznej inteligencji należy rozumieć jako „[...] zdolność do samodzielnego działania bez ingerencji człowieka”¹⁰. Autor uważa, że najbardziej trafna definicja została zaproponowana w encyklopedii zarządzania. Pomimo samodzielności ważny jest nadzór i monitorowanie osiągniętych celów.

6 *Autonomia*, <https://sjp.pwn.pl/sjp/autonomia;2551312.html> [dostęp: 20.03.2025].

7 *Autonomia – co to jest? Definicja, synonimy, przykłady użycia*, <https://polszczyzna.pl/autonomia-co-to-jest-definicja-synonimy-przyklady-uzycia> [dostęp: 20.03.2025].

8 *The Assessment List For Trustworthy Artificial Intelligence (ALTAI)*, Glossary, Independent High-Level Expert Group On Artificial Intelligence, Bruksela, 2020, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> [dostęp: 3.02.2025].

9 *Autonomia*, <https://mfiles.pl/pl/index.php/Autonomia> [dostęp: 20.03.2025].

10 R. Rejmانيak, *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Rocznik Nauk Prawnych” 2021, t. 31, nr 3, s. 98.

Autor uważa, że cel sztucznej inteligencji z punktu widzenia jej autonomiczności może być wskazany bezpośrednio przed zadaniem lub pośrednio przy wprowadzaniu danych wejściowych¹¹.

Bezpośrednio polega na wskazaniu celu dla systemu, np. usunięcia przeszkody na drodze. System podejmuje decyzję, jakimi dostępnymi środkami wykona zadanie, a zadanie kończy się z chwilą usunięcia przeszkody. Można ogólnie stwierdzić, że system wykonał zadanie autonomicznie, tj. nie był sterowany przez człowieka i nie pytał człowieka o zgodę na wykorzystanie konkretnych środków, w tym sposobu ich użycia.

Pośrednio polega na wprowadzeniu poleceń na poziomie programowania i nasycania systemu danymi wejściowymi. Odnosząc się do wyżej zaproponowanego przykładu usunięcia przeszkody, polecenie wprowadzone podczas nasycenia danymi wejściowymi może dotyczyć usuwania wszystkich przeszkód, które np. uniemożliwiają kontynuowanie przemieszczania po wyznaczonej trasie. Jeżeli system napotka przeszkodę, to usuwa ją zgodnie z wcześniej określonymi celami. Można zatem ogólnie stwierdzić, że wykonał zadanie autonomicznie.

Autor obecnie nie dostrzega merytorycznych przesłanek do implementacji systemu całkowicie autonomicznego. Oznaczałoby to, że system inicjuje działanie, np. bojowe, bez żadnego udziału człowieka. Jeżeli nawet system będzie w stanie samodzielnie określić cele taktyczne lub operacyjne i sposób ich osiągnięcia, to nadrzędna struktura celów polityczno-strategicznych jest nadal definiowana przez człowieka. Autor twierdzi, że w momencie przekazania systemowi samodzielności nad określaniem celów polityczno-strategicznych lub nadania rzeczywistej i całkowitej autonomii systemowi opartemu na sztucznej inteligencji będzie to oznaczało wyparcie człowieka z cyklu decyzyjnego, jego marginalizację i alienację z funkcji kreatora środowiska własnego funkcjonowania.

11 Dane wejściowe – dane dostarczone do systemu AI lub bezpośrednio przez niego pozyskiwane, na podstawie których system generuje wynik. Zob. *Rozporządzenie 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektywy 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)*, Dz. Urz. UE 2024, L 1689, art. 3, pkt 33.

Autor proponuje skalę autonomii sztucznej inteligencji uwzględniającą poziom zaangażowania systemu i poziom zaangażowania człowieka w decyzyjność i sprawczość.

Tabela 1. Skala autonomii sztucznej inteligencji

Poziom autonomii sztucznej inteligencji	Charakterystyka zaangażowania systemu i człowieka	
	system	człowiek
Wykonawczy	brak autonomii; system wykonuje polecenia człowieka, wykorzystując swoje możliwości technologiczne	człowiek inicjuje działanie, decyduje o sposobie jego wykonania i zakończeniu; wspomaga się technologicznymi możliwościami systemu
Towarzyszący	wykonuje polecenia człowieka, wspomaga realizację zadań zgodnie ze swoimi możliwościami technologicznymi, wykazuje inicjatywę w ramach postawionych zadań, potrafi np. samodzielnie zaproponować różne warianty wykonania zadania czy samodzielnie zrealizować część misji zgodnie z postawionym celem	inicjuje działanie, decyduje o jego wykonaniu i zakończeniu, współpracuje z systemem z wykorzystaniem jego możliwości technologicznych, korzysta z inicjatywy systemu w sposobie realizacji zadań
Dominujący	otrzymuje od człowieka cel do osiągnięcia, sam dobiera sposób wykonania zadań i decyduje kiedy zostaną zakończone, a cel osiągnięty	stawia systemowi cel; cel może być określany bezpośrednio przed zadaniem lub w ramach danych wejściowych, na podstawie których system sam określi sposób wykonania; człowiek nie dobiera środków, a system sam decyduje, czy cel został osiągnięty

Źródło: Opracowanie własne.

Militarny potencjał sztucznej inteligencji

Sztuczna inteligencja jest technologią, w którą inwestuje coraz więcej armii, ponieważ przewaga w wyścigu technologicznym oznacza przewagę na polu walki. Jest wdrażana do rodzajów sił zbrojnych wielu państw, a jej zastosowanie wspomaga działanie armii na wielu płaszczyznach. Wykorzystanie sztucznej inteligencji może mieć zastosowanie w budowaniu świadomości operacyjnej,

logistyce i efektywności bojowej. Ahmed Banafa w publikacji pt. „Artificial Intelligence (AI) in Modern Military Applications” wymienia niektóre obszary i konkretne systemy, w których już zastosowano rozwiązania oparte na sztucznej inteligencji. Są to m.in. bezzałogowe platformy lądowe, które mogą wykonywać zadania rozpoznawcze, transportowe lub prowadzić działania bojowe z minimalnym udziałem człowieka. Jak wskazano na Platformie Przemysłu Przyszłości: „Pojazdy autonomiczne i bezzałogowe to systemy transportowe, które mogą poruszać się samodzielnie bez potrzeby bezpośredniego sterowania przez człowieka. Wykorzystują zaawansowane technologie, takie jak sztuczna inteligencja, czujniki i systemy nawigacyjne, aby samodzielnie analizować otoczenie, podejmować decyzje i przemieszczać się w środowisku. Tego rodzaju pojazdy mają szerokie zastosowanie w transporcie, logistyce, rolnictwie, wojsku i eksploracji”¹². Jednym z przykładów wykorzystania zaawansowanej technologii może być użycie robotycznego muła¹³, który w wojsku jest przeznaczony przede wszystkim do przenoszenia ciężkich ładunków, co z kolei odciąża żołnierzy wykonujących np. działania patrolowe¹⁴. Z kolei Firma BAE Systems Australia zaprezentowała autonomiczny opancerzony lekki system taktyczny ATLAS CCV (Autonomous Tactical Light Armour System Collaborative Combat Variant)¹⁵, sterujący pojazdem, który będzie pozwalał unikać przeszkód, planować trasę i podejmować decyzje taktyczne¹⁶. W logistyce warto podkreślić wykorzystanie sztucznej inteligencji w utrzymaniu predykcyjnym. Polega ono na zbieraniu danych o stanie maszyn i przebiegu procesów eksploatacyjnych. Na podstawie danych są tworzone modele pozwalające przewidywać wystąpienie awarii i określać stan urządzenia, np. stopień jego zużycia. Modele sztucznej inteligencji potrafią w czasie rzeczywistym określać ryzyko niesprawności i alarmować o możliwych problemach. Dzięki

12 *Pojazdy autonomiczne/bezzałogowe*, <https://przemyslprzyszlosci.gov.pl/technologie/cyfrowe/robotyzacja/pojazdy-autonomiczne-bezzałogowe> [dostęp: 3.03.2025].

13 *LS3: Legged Squad Support System*, <https://www.darpa.mil/research/programs/legged-squad-support-system> [dostęp: 3.03.2025].

14 *Testy LS3*, <https://www.youtube.com/watch?v=IIbtwn8jwwc&t=62s> [dostęp: 3.03.2025].

15 *Zob. Autonomous Tactical Light Armour System Collaborative Combat Variant (ATLAS CCV), Australia*, <https://www.army-technology.com/projects/atlas-ccv-australia> [dostęp: 3.03.2025].

16 *Bezzałogowy pojazd bojowy nowej generacji ATLAS CCV, 2024*, <https://tacgear.pl/2024/09/bezzałogowy-pojazd-bojowy-nowej-generacji-atlas-ccv> [dostęp: 23.02.2025].

wdrożeniu strategii utrzymania predykcyjnego można zmniejszyć koszty serwisu, ograniczyć czas przestojów, jednocześnie wydłużyć czas działania urządzeń i zwiększyć bezpieczeństwo¹⁷. Zastosowanie sztucznej inteligencji wspomaga także zdolności żołnierzy, dlatego że monitoruje dane dotyczące ich stanu zdrowia, żeby poprawiać proces szkolenia, a docelowo zwiększyć efektywność bojową. Jednym z elementów tego procesu może być *neurofeedback*, który jest nowym podejściem do przygotowania psychofizycznego żołnierzy i stanowi zaawansowaną metodę pozwalającą na świadomą regulację aktywności mózgowej¹⁸. Sztuczna inteligencja może także wesprzeć działania marynarki wojennej w prowadzeniu operacji morskich, np. poprzez realizację misji patrolowych, bojowych czy zbieranie danych wywiadowczych. Ponadto algorytmy sztucznej inteligencji przetwarzają dane z sonarów, żeby wykryć i śledzić pojazdy podwodne bardziej efektywnie niż człowiek. W przypadku sił powietrznych i kosmicznych sztuczna inteligencja może wspomagać zadania związane z wykorzystaniem dronów, wspierać pilotów czy monitorować ruch lotniczy. Dodatkowo algorytmy optymalizują pracę satelitów i mogą przewidywać potencjalną ich kolizję. W rzeczywistości cyberwojny sztuczna inteligencja jest narzędziem niezbędnym do wykrycia zagrożenia i reakcji na nie, a także ochrony sieci wojskowych przed atakami. Wykorzystanie sztucznej inteligencji pozwala prowadzić ofensywne operacje cybernetyczne poprzez identyfikację podatności wrogich systemów i automatyzację ataku¹⁹. W kwestii zagrożenia pociskami balistycznymi należy podkreślić, że z pomocą sztucznej inteligencji można wykryć nadlatujący pocisk balistyczny, próbować przewidzieć trajektorię jego lotu i w rezultacie spróbować zakłócić sygnał sterujący pociskiem lub przejąć na nim kontrolę. Przykładem niebojowego wykorzystania może być użycie oprogramowania do tłumaczenia i transkrypcji, które potrafi w czasie rzeczywistym wykonać tłumaczenie i transkrypcję wielu długich tekstów jednocześnie, na wiele języków. W obszarze szkolenia,

17 *Predictive Maintenance (Utrzymanie predykcyjne)*, <https://www.statsoft.pl/rozwiwania/zastosowania-technologiczne/predictive-maintenance> [dostęp: 23.02.2025].

18 A. Nowacka, *Zastosowanie neurofeedbacku w optymalizacji wydolności psychofizycznej żołnierzy*, <https://www.ezaf.pl/wpisy/zastosowanie-neurofeedbacku-w-optymalizacji-wydolnosc-psychofizycznej-zolnierzy,1842> [dostęp: 7.02.2025].

19 A. Banafa, *Artificial Intelligence (AI) in Modern Military Applications*, <https://www.linkedin.com/pulse/artificial-intelligence-ai-modern-military-prof-ahmed-banafa-e9sxc> [dostęp: 23.01.2025].

sztuczna inteligencja może być wykorzystana w symulatorach i тренаżerach, żeby jak najdokładniej odwzorować rzeczywiste pole walki. Szkolenie może być także prowadzone przez inteligentnego asystenta, np. chatbot, który w przeciwieństwie do podręczników będzie zawsze dysponował uaktualnianą bazą danych. Atutem użycia sztucznej inteligencji na potrzeby armii może być brak typowo ludzkich dylematów moralnych podczas podejmowania decyzji. Warto wspomnieć, że prowadzone są prace nad tym, żeby sztuczna inteligencja uczyła się samodzielnie, co ma ograniczyć udział człowieka i zmniejszyć koszty nasycania algorytmów danymi wejściowymi²⁰. Jak wskazano w projekcie Komisji Europejskiej „Horizon 2020”, żeby usprawnić proces uczenia się sztucznej inteligencji, zostało opracowanych kilka nowych technologii mogących prowadzić własne badania. Wskazano, że algorytmy „[...] mogą to robić automatycznie, konsultując się z zasobami internetowymi, na przykład bazami Google i Wikipedii, a także dzięki nowemu matematycznemu podejściu do uczenia się geometrii obiektów na podstawie obrazów i filmów bez konieczności korzystania z zewnętrznego źródła nadzoru”²¹. Kolejnym obszarem, w którym można wykorzystać sztuczną inteligencję, może być przeciwdziałanie wrogim operacjom informacyjnym, w tym procesowi dezinformacji. Autor wskazuje trzy filary dezinformacji, które są wykorzystywane do wprowadzenia w błąd użytkownika przestrzeni informacyjnej:

- manipulacja faktami,
- tworzenie fake-newsów,
- szum informacyjny²².

Sztuczna inteligencja jest w tym obszarze wykorzystywana do identyfikacji, analizy i monitorowania treści i tendencji w procesach dezinformacyjnych, daje np. możliwość przygotowania narracji informacyjnej w przypadku zaistnienia sytuacji kryzysowej lub możliwość określania kierunków komunikacji proaktywnej.

20 *Artificial Intelligence in Electronic Warfare*, <https://www.te.com/en/industries/defense-military/insights/ai-in-warfare-and-military-applications.html> [dostęp: 3.02.2025].

21 *Uczenie sztucznej inteligencji, jak ma się sama uczyć*, Europejska Rada ds. Badań Naukowych, <https://cordis.europa.eu/article/id/435616-teaching-ai-to-teach-itself/pl> [dostęp: 10.03.2025].

22 Zob. T. Gergelewicz, *Countering Disinformation Concept for building social resilience in times of cognitive warfare*, „Przegląd Nauk o Obronności. Defence Science Review” 2024, nr 20, s. 34.

Podsumowując, implementacja sztucznej inteligencji na potrzeby sił zbrojnych może bezpośrednio wpłynąć po poprawienie wydajności sił zbrojnych, a także na przyspieszenie procesów decyzyjnych. To z kolei może przejawiać się m.in. w takich obszarach, jak:

- podejmowanie decyzji – możliwość przetwarzania dużej ilości danych i dostarczanie dowódcom szybkich rekomendacji na podstawie konkretnych informacji. Ponadto warto zaznaczyć, że czas oszczędzony na wykonanie zadania wspartego sztuczną inteligencją to czas, który może być wykorzystany do opracowania bardziej kompletnych planów działania z większą liczbą wariantów²³,
- świadomość sytuacyjna – czujniki i narzędzia analityczne dają dokładniejszy obraz pola walki,
- ryzyko strat w ludziach – automatyczne systemy mogą wykonywać niebezpieczne zadania, potencjalnie ratować życie żołnierzy,
- wydajność zasobów – optymalizacja logistyki, utrzymanie i przemieszczanie zasobów, obniżanie kosztów i poprawa skuteczności realizacji zadań,
- czas reakcji – możliwość reagowania na zagrożenia w krótszym czasie niż operatorzy-żołnierze, potencjalnie zapewniać przewagę w krytycznych momentach,
- wydłużona gotowość do działania – możliwość działania nieprzerwanie bez zmęczenia, utrzymanie stałej gotowości,
- obliczenia kwantowe – potencjał dużej mocy przetwarzania danych i możliwości rozwiązywania złożonych problemów obliczeniowych,
- analiza predykcyjna wydarzeń geopolitycznych – prawdopodobieństwo przewidywania konfliktów²⁴.

Jak podkreślono w „Artificial Intelligence and National Security U.S.”, rozwój możliwości nowoczesnych technologii opartych na sztucznej inteligencji prawdopodobnie umożliwi przejście z misji bojowych załogowych na bezzałogowe i tym samym bardziej autonomiczne wsparcie żołnierzy przez roboty²⁵.

23 M. Zequeira, *U.S. Army, Artificial Intelligence as a Combat Multiplier, Using AI to Unburden Army Staffs*, Military Review Online Exclusive, 2024, <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier> [dostęp: 18.01.2025].

24 A. Banafa, op. cit.

25 G. Allen, T. Chan, *Artificial Intelligence and National Security U.S. Intelligence Advanced Research Projects Activity (IARPA)*, Harvard Cennedy School – Belfer Center for Science and International Affairs, 2017, <https://www.belfercenter.org/sites/default/>

Rozwój sztucznej inteligencji na potrzeby wojska w ujęciu ogólnym zmierza w stronę samodzielnego nasycenia się danymi, możliwości autonomicznej analizy informacji i podjęcia suwerennej decyzji.

Militarny potencjał sztucznej inteligencji – wyzwania

Ciągły postęp w dziedzinie sztucznej inteligencji generuje coraz większe wyzwania dotyczące m.in. określenia podstaw prawnych i moralnych jej tworzenia oraz wykorzystywania. Wydaje się, że obecnie jednym z głównych problemów w tym zakresie jest zdefiniowanie zasad odpowiedzialności za potencjalne szkody, które mogą zostać wyrządzone w wyniku działania sztucznej inteligencji. Robert Weissman i Savannah Wooten w publikacji pt. „A.I. Joe: The Dangers of Artificial Intelligence and the U.S. Military” wyliczają wyzwania, z którymi należy się mierzyć podczas wdrażania sztucznej inteligencji na potrzeby wojska:

- etyka – użycie broni autonomicznej wywołuje pytania natury moralnej dotyczące roli człowieka w podejmowaniu decyzji na polu walki. Sztuczna inteligencja może mieć trudności w podejmowaniu decyzji, które wymagają empatii, zrozumienia kulturowego lub złożonych rozważań etycznych,

- rzetelność i nieprzewidywalność – systemy mogą działać w sposób nieprzewidywalny w złożonych, rzeczywistych scenariuszach, co może prowadzić do niezamierzonych rezultatów,

- podatność na wrogie przejęcie – systemy mogą zostać przejęte przez przeciwników, potencjalnie obracając broń przeciwko własnym operatorom.

Leonel Garciga²⁶ przestrzegął personel wojskowy i propagatorów sztucznej inteligencji, że „narzędzia sztucznej inteligencji zostały szeroko przyjęte ze względu na ich wysoką wydajność i łatwość użytkowania. Jednak stanowią one również wyjątkowe wyzwania pod względem prywatności danych,

files/2024-10/Artificial%20Intelligence%20and%20National%20Security.pdf [dostęp: 28.02.2025].

26 Szef ds. Informacji w Dowództwie Wojsk Lądowych Armii Stanów Zjednoczonych. Zob. Leonel Garciga on Army's Unified Network Operations Initiative, <https://executive.gov.com/2025/02/leonel-garciga-army-unified-network-operations-initiative> [dostęp: 2.02.2025].

bezpieczeństwa i kontroli nad generowaną treścią. Dlatego ich stosowanie powinno być starannie oceniane i monitorowane²⁷.

1. Zależność od danych. Do skutecznego działania systemy oparte na sztucznej inteligencji wymagają dużych ilości wysokiej jakości danych, które nie zawsze mogą być dostępne w sytuacjach bojowych.

Rozmieszczanie śmiertelnej broni opartej na sztucznej inteligencji w środowisku pola walki oznacza użytkowanie jej w warunkach, do których nie została zaprogramowana. Potencjalne problemy z wiarygodnymi danymi szkoleniowymi lub nieprawdziwymi danymi wywiadowczymi mogą skutkować błędną identyfikacją celów i niezamierzonym atakiem.

2. Ryzyko eskalacji. Efektywność działań bojowych z zastosowaniem sztucznej inteligencji może prowadzić do szybkiej eskalacji konfliktów, potencjalnie zwiększać ryzyko pełnoskalowej wojny. Ponadto dostęp do sztucznej inteligencji jest coraz bardziej powszechny, co zwiększa prawdopodobieństwo, że wpadnie w ręce aktorów niepaństwowych lub państw-agresorów.

3. Niejednoznaczność prawna. Wykorzystanie systemów autonomicznych powoduje pytania natury prawnej dotyczące odpowiedzialności i zgodności z prawem²⁸.

Kwestię odpowiedzialności prawnej za użycie sztucznej inteligencji podjął Rafał Rejmank w publikacji „Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego”. Zazaczył, że wraz ze wzrostem poziomu autonomiczności systemów sztucznej inteligencji rosną trudności ze wskazaniem odpowiedzialnego za ewentualne szkody w mieniu czy za narażenie zdrowia lub życia. Z reguły odpowiedzialność ponosi ten, który ostatecznie podejmuje decyzję o rozpoczęciu lub zaniechaniu działania. Natomiast jeżeli rola człowieka sprowadza się do nadzorującego system, to zarzutem nie jest to, że skutek wywołał, ale to, że mu nie zapobiegł, znając jego konsekwencje. Problemy ze wskazaniem odpowiedzialnego karnie za skutki powodowane przez systemy

27 Cyt. za: M. Easley, *Army implements generative AI platform to cArmy cloud environment*, 2024 <https://defensescoop.com/2024/09/10/army-generative-ai-capability-carmy-cloud> [dostęp: 2.02.2025].

28 R. Weissman, S. Wooten, *A.I. Joe: The Dangers of Artificial Intelligence and the U.S. Military*, 2024, s. 8–17, <https://www.citizen.org/article/ai-joe-report/> [dostęp: 13.01.2025].

w pełni autonomiczne wydają się wyzwaniem ze względu na brak związku pomiędzy wolą i świadomością człowieka a działaniem systemu²⁹.

Ponadto należy podkreślić, że przykładem nieprawidłowego działania sztucznej inteligencji mogą być tzw. halucynacje sztucznej inteligencji, które pojawiają się, gdy system regularnie generuje nieprawidłowe odpowiedzi i przedstawia je z dużą pewnością jako prawdziwe. Błędy te mogą być spowodowane m.in. przez niewystarczające dane szkoleniowe (na których sztuczna inteligencja się uczy), nieprawidłowe założenia przyjęte przez model lub błędy w danych wykorzystywanych do szkolenia³⁰.

Reasumując, autor definiuje trzy zasadnicze obszary, które należy opanować, żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko niepożądanego działania.

1. Awary – niedające się przewidzieć awary powodowane przez wadliwe elementy, co może prowadzić do zaniechania lub błędnego wykonania zadania.

2. Przejęcie – prawdopodobieństwo przejęcia systemów przez strony nieposiadające autoryzowanego dostępu, co mogłoby zostać wykorzystane do celów niezwiązanych z wolą i zamiarem właściwego operatora.

3. Autonomia – całkowita autonomia systemów opartych na sztucznej inteligencji, w perspektywie jej śmiertelności potencjału, może stanowić poważne zagrożenie w przypadku braku kontroli ze strony człowieka. Pełna decyzyjność po stronie systemu może być tragiczna w skutkach.

Wywiad z Chatem GPT

Prowadząc rozważania na temat wykorzystania sztucznej inteligencji na potrzeby sił zbrojnych, warto posłkować się głosem eksperckim. Autor zakłada, że eksperckie stanowisko może przedstawić sama sztuczna inteligencja, dlatego przeprowadził wywiad z tą technologią, która w tym przypadku jest reprezentowana przez Chat GPT.

²⁹ R. Rejmaniak, op. cit., s. 108.

³⁰ Na podstawie: T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas” 2024, nr 2, s. 71–94.

1. Jakie obszary w wojsku są kluczowe do zastosowania sztucznej inteligencji?

„W wojsku sztuczna inteligencja (SI) może być zastosowana w wielu obszarach, a jej wdrożenie może znacząco zwiększyć efektywność operacji, poprawić bezpieczeństwo i zredukować ryzyko. Kluczowe obszary zastosowania SI w wojsku to:

1. Zautomatyzowane systemy rozpoznania i analizy danych: SI może analizować ogromne ilości danych z różnych źródeł (np. zdjęć satelitarnych, dronów, monitoringu) w celu wykrywania zagrożeń, identyfikowania celów lub monitorowania ruchów wroga.

2. Drony i roboty bojowe: Wykorzystanie SI do autonomicznych systemów bojowych (np. dronów, robotów naziemnych), które mogą prowadzić misje zwiadowcze, dostarczać zaopatrzenie, czy nawet przeprowadzać ataki precyzyjne.

3. Wspomaganie decyzji w dowodzeniu: Algorytmy SI mogą analizować dane strategiczne, prognozować możliwe scenariusze konfliktów i sugerować optymalne decyzje dowódcom, wspomagając procesy planowania i decyzyjne.

4. Cyberbezpieczeństwo i obrona przed atakami: SI jest kluczowym narzędziem w walce z cyberzagrożeniami, w tym w wykrywaniu ataków hakerskich, analizowaniu zachowań podejrzanych użytkowników i zabezpieczaniu systemów wojskowych.

5. Symulacje i treningi wojskowe: SI może służyć do tworzenia realistycznych symulacji, które pozwalają na doskonalenie umiejętności żołnierzy i sztabów wojskowych w bezpiecznym, wirtualnym środowisku.

6. Logistyka i zaopatrzenie: Optymalizacja procesów logistycznych za pomocą SI, w tym zarządzanie zaopatrzeniem, transportem, magazynowaniem i dystrybucją zasobów w trudnych warunkach wojennych.

7. Przewidywanie i zarządzanie zasobami: SI może pomóc w przewidywaniu potrzeb w zakresie personelu, sprzętu czy amunicji, umożliwiając bardziej efektywne planowanie zasobów i zmniejszając marnotrawstwo.

8. Medycyna wojskowa: Zastosowanie SI w diagnostyce medycznej, zdalnym monitorowaniu zdrowia żołnierzy oraz robotach medycznych do pomocy w terenie, zwłaszcza w sytuacjach wymagających natychmiastowej interwencji.

9. Zarządzanie komunikacją i koordynacją: SI może wspomagać systemy komunikacyjne, zapewniając szybkie, bezpieczne i efektywne przesyłanie

informacji w czasie rzeczywistym, co jest kluczowe w dynamicznych warunkach pola walki.

Implementacja sztucznej inteligencji w tych obszarach może poprawić szybkość, precyzję i bezpieczeństwo działań wojskowych, a także umożliwić lepsze wykorzystanie zasobów i wsparcie dla żołnierzy w trudnych warunkach”.

Chat trafnie wymienił i scharakteryzował większość zasadniczych obszarów wykorzystujących i potencjalnie wykorzystujących sztuczną inteligencję na potrzeby wojska. Należy zwrócić uwagę, że zadane pytanie nie zawierało oczekiwania uzasadnienia, ale Chat z własnej inicjatywy ogólnie scharakteryzował przedstawione obszary. Dodatkowo dokonał krótkiego podsumowania, w którym wskazał zalety wykorzystania sztucznej inteligencji na potrzeby wojska.

2. Które państwo obecnie może wykorzystać sztuczną inteligencję do prowadzenia działań agresywnych?

„Wykorzystanie sztucznej inteligencji (SI) do prowadzenia agresywnych działań wojskowych staje się coraz bardziej realne i jest rozwijane przez kilka państw. Wśród krajów, które inwestują i rozwijają technologie związane z SI w kontekście obronności i wojskowości, wyróżniają się przede wszystkim:

1. Stany Zjednoczone: USA są jednym z liderów w zastosowaniu SI w wojskowości. Amerykańska armia intensywnie inwestuje w rozwój autonomicznych systemów bojowych, dronów, cyberbezpieczeństwa oraz analityki danych opartej na SI. Dodatkowo, Stany Zjednoczone pracują nad rozwojem systemów wspierających decyzje dowódcze i automatycznych broni opartej na SI. Sztuczna inteligencja jest także wykorzystywana w cyberwojnie, co pozwala na ofensywne działania w sieci.

2. Chiny: Chiny są jednym z najbardziej zaawansowanych krajów w zakresie zastosowania sztucznej inteligencji w wojskowości. Chińska armia inwestuje w rozwój autonomicznych systemów takich, jak: drony bojowe, roboty czy technologie w zakresie wojny cybernetycznej. Chińska strategia wojskowa w dużym stopniu opiera się na »wojnie informacyjnej« i wykorzystaniu SI do przeprowadzania operacji wywiadowczych, analizie danych i atakach w cyberprzestrzeni.

3. Rosja: Rosja również rozwija technologie sztucznej inteligencji w kontekście działań wojskowych, szczególnie w zakresie dronów bojowych, autonomicznych systemów naziemnych i cyberbezpieczeństwa. Istnieją doniesienia

o wykorzystaniu SI w rosyjskich działaniach ofensywnych w cyberprzestrzeni, a także w analizie danych wywiadowczych oraz planowaniu operacji wojskowych.

4. Izrael: Izrael jest jednym z liderów w dziedzinie technologii obronnych, w tym sztucznej inteligencji. Kraj ten jest znany z zaawansowanych systemów obrony powietrznej, dronów oraz innych autonomicznych systemów, które mogą być wykorzystywane w ofensywnych operacjach wojskowych. Izrael również inwestuje w rozwój cyberwojny opartej na sztucznej inteligencji.

5. Zjednoczone Emiraty Arabskie: ZEA rozwijają autonomiczne systemy bojowe i inwestują w SI jako część swojej strategii obronnej. Drony i roboty bojowe są wykorzystywane zarówno w obronie, jak i do przeprowadzania ofensywnych działań.

6. Indie: Indie, choć na mniejszą skalę niż inne mocarstwa, również inwestują w sztuczną inteligencję w kontekście obronności, szczególnie w zakresie autonomicznych systemów, dronów, analityki danych oraz cyberbezpieczeństwa.

Sztuczna inteligencja w kontekście agresywnych działań wojskowych wiąże się z wieloma wyzwaniem etycznymi, prawnymi i technologicznymi. Wiele z tych państw bada kwestie związane z autonomią broni, analizą danych wywiadowczych oraz cyberatakami, co może mieć poważne konsekwencje w przypadku wykorzystania tych technologii w konfliktach zbrojnych. Oczekuje się, że w najbliższych latach konkurencja w tej dziedzinie będzie intensyfikować się, a rozwój SI będzie kluczowym elementem strategii obronnych w wielu państwach”.

Chat komplementarnie odpowiada na pytanie, rozwija swoją odpowiedź o szczegóły dotyczące konkretnych wskazanych państw. Na uwagę zasługuje obszar cyberwojny i cyberbezpieczeństwa. Jak wskazuje Chat:

- „Dodatkowo, Stany Zjednoczone pracują nad rozwojem systemów wspierających decyzje dowódcze i automatycznych broni opartej na SI. Sztuczna inteligencja jest także wykorzystywana w cyberwojnie, co pozwala na ofensywne działania w sieci”.

- „Chińska armia inwestuje w rozwój autonomicznych systemów, takich jak drony bojowe, roboty czy technologie w zakresie wojny cybernetycznej”.

- „Rosja: Istnieją doniesienia o wykorzystaniu SI w rosyjskich działaniach ofensywnych w cyberprzestrzeni”.

- „Izrael również inwestuje w rozwój cyberwojny opartej na sztucznej inteligencji”.

Należy zwrócić uwagę na charakterystykę Federacji Rosyjskiej. W przypadku np. Stanów Zjednoczonych Ameryki, Chin czy Izraela Chat jednoznacznie stwierdza wykorzystanie sztucznej inteligencji w obszarze cyberwojny. Jeżeli chodzi o Federację Rosyjską, to wskazuje jedynie na „doniesienia”. W rzeczywistości wielokrotnie dowiedziono, że Moskwa prowadzi działania ofensywne w cyberprzestrzeni, w tym z wykorzystaniem sztucznej inteligencji.

3. Czy obecny etap rozwoju sztucznej inteligencji w Polsce daje szanse na jej skuteczne zastosowanie na potrzeby wojska?

„W Polsce rozwój sztucznej inteligencji (SI) w kontekście wojskowym jest na wczesnym etapie, ale kraj podejmuje kroki w celu zbudowania podstaw do jej skutecznego zastosowania w obronności. Obecny etap rozwoju SI w Polsce daje pewne szanse na jej przyszłe zastosowanie w wojsku, ale także stawia wyzwania, które będą wymagały dalszych inwestycji, rozwoju technologii i współpracy międzynarodowej. Oto kilka kluczowych aspektów, które należy uwzględnić:

1. Inwestycje w rozwój technologii i infrastruktury. Polska stawia na rozwój sektora technologii, w tym sztucznej inteligencji, poprzez różne inicjatywy, takie jak Program Inteligentnego Rozwoju czy wsparcie dla start-upów technologicznych. Zostały również uruchomione projekty badawcze w dziedzinie sztucznej inteligencji, które mogą z czasem przyczynić się do rozwoju rozwiązań wojskowych, w szczególności współpraca między uczelniami, ośrodkami badawczo-rozwojowymi i przemysłem obronnym jest kluczowa, aby stworzyć technologie odpowiadające specyficznym wymaganiom sektora obronności.

2. Współpraca międzynarodowa. Polska jest członkiem NATO, a współpraca z sojusznikami, w szczególności z krajami takimi jak Stany Zjednoczone, Wielka Brytania czy Niemcy, może pomóc w przyspieszeniu wdrożenia SI w wojsku. Dzięki tej współpracy Polska może uzyskać dostęp do nowoczesnych technologii i wiedzy, a także uczestniczyć w międzynarodowych programach badawczo-rozwojowych.

3. Wykorzystanie sztucznej inteligencji w cyberbezpieczeństwie. Jednym z bardziej rozwiniętych obszarów w Polsce, w którym sztuczna inteligencja może mieć szybki i efektywny wpływ, jest cyberbezpieczeństwo. Siły zbrojne i agencje rządowe, takie jak Polska Agencja Kosmiczna czy Agencja Bezpieczeństwa Wewnętrznego, już pracują nad wdrożeniem SI do monitorowania

zagrożeń w cyberprzestrzeni. W tym zakresie Polska ma szansę na skuteczne wykorzystanie SI do ochrony infrastruktury krytycznej oraz obrony przed cyberatakami.

4. Autonomiczne systemy bojowe. Polska armia posiada już pewne autonomiczne technologie, jak bezzałogowe statki powietrzne (drony) wykorzystywane do celów zwiadowczych. Przyszłość w rozwoju autonomicznych systemów bojowych (np. drony bojowe, roboty naziemne) może również przynieść korzyści w zakresie zwiększenia efektywności działań wojskowych, a w Polsce trwają prace nad rozwojem takich systemów. Jednak pełne wdrożenie zaawansowanych autonomicznych systemów wymagających SI w Polsce wymagałoby znacznych inwestycji w badania, rozwój technologii oraz infrastrukturę.

5. Edukacja i rozwój kompetencji. Polska już teraz inwestuje w rozwój kompetencji w dziedzinie sztucznej inteligencji, co jest kluczowe dla dalszego rozwoju technologii obronnych. Wprowadzenie specjalistycznych kursów, szkoleń oraz współpraca z międzynarodowymi ośrodkami naukowymi może zbudować bazę wiedzy niezbędną do wdrożenia SI w wojsku.

6. Wyzwania związane z regulacjami i etyką. Sztuczna inteligencja w wojskowości wiąże się z licznymi wyzwaniami etycznymi i prawnymi, zwłaszcza w kontekście autonomicznych systemów bojowych. Polska, podobnie jak inne kraje, będzie musiała zmierzyć się z kwestiami regulacyjnymi dotyczącymi użycia SI w wojskowości, takimi jak odpowiedzialność za działania maszyn, a także przestrzeganie międzynarodowych norm prawnych dotyczących użycia broni.

7. Potrzebna jest większa integracja z przemysłem obronnym. Choć w Polsce istnieją firmy, które rozwijają technologie sztucznej inteligencji, ich integracja z przemysłem obronnym może być kluczowa dla skutecznego wdrożenia SI w wojsku. Wymaga to długofalowych inwestycji w badania, rozwój i współpracę z sektorem zbrojeniowym.

Podsumowanie: Obecny etap rozwoju sztucznej inteligencji w Polsce daje podstawy do przyszłego wykorzystania tej technologii w wojsku, szczególnie w zakresie cyberbezpieczeństwa, autonomicznych systemów bojowych oraz wsparcia w analizie danych. Jednak pełne wykorzystanie SI w obronności wymaga dalszych inwestycji w badania, rozwój, współpracę międzynarodową i budowanie odpowiedniej infrastruktury technologicznej. Polska ma szansę

na skuteczne zastosowanie sztucznej inteligencji w wojsku, ale potrzebne są dalsze wysiłki w tych obszarach”.

Chat trafnie, na dużym poziomie ogólności, opisuje zaawansowanie Polski w implementację sztucznej inteligencji na potrzeby wojska. Wymienia konkretne obszary wykorzystania oraz potencjalnego wykorzystania tej technologii, które w dużej mierze są spójne z obszarami wskazanymi w odpowiedzi na pytanie pierwsze. Niewskazywanym wcześniej elementem, a zarazem sugestią Chatu są obszary współpracy międzynarodowej i rozwoju przemysłu obronnego. Należy uznać te wskazania jako istotne, ponieważ *de facto* są to podstawowe obszary rozwoju zdolności sił zbrojnych.

Ponadto autor zwraca uwagę, że Chat nie wspomina, że 3 marca 2025 roku kierownictwo Ministerstwa Obrony Narodowej ogłosiło powstanie Centrum Implementacji Sztucznej Inteligencji w Wojskach Obrony Cyberprzestrzeni³¹, a 14 marca tegoż roku ogłoszono powstanie kolejnej instytucji związanej z tym obszarem, tj. fabryki sztucznej inteligencji w Poznaniu³².

4. Czy możliwe jest, że wojskowe systemy autonomiczne wykorzystywane w wojsku mogą działać przeciwko wojskom własnym?

„Tak, istnieje ryzyko, że wojskowe systemy autonomiczne mogą działać przeciwko własnym wojskom, jeśli nie będą odpowiednio zaprojektowane, kontrolowane i monitorowane. Takie scenariusze, choć wciąż rzadkie, są powodem do niepokoju i są brane pod uwagę przez ekspertów w dziedzinie sztucznej inteligencji, etyki wojskowej oraz prawa międzynarodowego. Potencjalne ryzyka:

- 31 Centrum Implementacji Sztucznej Inteligencji ma za zadanie wspieranie rozwoju Sił Zbrojnych RP m.in. poprzez wykorzystanie sztucznej inteligencji do analizy informacji wywiadowczo-rozpoznawczych, działania autonomicznych systemów bojowych czy wsparcia procesu decyzyjnego. Zob. *W Wojsku Polskim powstaje Centrum Implementacji Sztucznej Inteligencji*, <https://www.gov.pl/web/obrona-narodowa/w-wojsku-polskim-powstaje-centrum-implementacji-sztucznej-inteligencji> [dostęp: 1.03.2025].
- 32 Poznańska fabryka ma wspierać innowacje w takich sektorach, jak: zdrowie, cyberbezpieczeństwo, technologie kwantowe, robotyka i zrównoważony rozwój. Zob. *W Poznaniu powstanie fabryka sztucznej inteligencji*, <https://naukawpolsce.pl/aktualnosci/news%2C107049%2Cw-poznaniu-powstanie-fabryka-sztucznej-inteligencji.html> [dostęp: 23.03.2025].

1. Błędy w algorytmach: Autonomiczne systemy wojskowe, takie jak drony czy roboty bojowe, opierają się na algorytmach, które mogą popełniać błędy w analizie sytuacji na polu walki. Błędy w rozpoznawaniu celów (np. identyfikowanie własnych jednostek jako wroga) mogą prowadzić do ataków na siły własne. Nawet małe błędy w oprogramowaniu lub błędne interpretacje danych wywiadowczych mogą skutkować tragicznymi konsekwencjami.

2. Ataki cybernetyczne: Autonomiczne systemy wojskowe są podatne na ataki cybernetyczne. Złośliwe oprogramowanie lub hakowanie tych systemów może prowadzić do ich przejęcia przez wroga, co może skutkować ich skierowaniem do ataku na własne siły. Przykładem może być przejęcie kontroli nad dronem lub robotem bojowym i wykorzystanie go przeciwko własnym oddziałom.

3. Problemy z systemami rozpoznawania: Autonomiczne systemy wojskowe często korzystają z systemów rozpoznawania obrazu (np. kamery, sensory, lidar³³) do identyfikowania celów. Jeśli te systemy nie będą wystarczająco dokładne lub jeżeli wystąpią problemy z ich kalibracją, mogą błędnie rozpoznać własne jednostki jako wroga.

4. Brak elastyczności w podejmowaniu decyzji: Autonomiczne systemy mogą działać zgodnie z zaprogramowanymi procedurami, ale w sytuacjach niestandardowych, gdzie wymagana jest ocena kontekstu, mogą nie być w stanie podjąć właściwej decyzji. Na przykład, w trudnych warunkach konfliktu, gdzie wroga jednostkę można pomylić z własną, systemy autonomiczne mogą podjąć błędne decyzje, prowadzące do ataku na jednostki przyjazne.

5. Błąd ludzki w programowaniu i kontrolowaniu systemów: Nawet jeśli systemy autonomiczne są zaprojektowane tak, by unikać takich sytuacji, błędy popełnione przez programistów, techników czy dowódców mogą wpłynąć na ich działanie. Niewłaściwa konfiguracja, nieaktualne dane rozpoznawcze lub brak odpowiedniego nadzoru mogą prowadzić do błędów, które będą skutkować atakiem na własne wojska.

33 Dane pomiarowe LIDAR (ang. Light Detection and Ranging). Zob. *Dane pomiarowe LIDAR (LIDAR)*, <https://www.geoportal.gov.pl/pl/dane/dane-pomiarowe-lidar-lidar/> [dostęp: 23.03.2025].

Rozwiązania minimalizujące ryzyko

Aby zapobiec takim sytuacjom, należy wdrożyć szereg środków ochronnych i kontrolnych:

1. Testowanie i walidacja systemów autonomicznych: Systemy autonomiczne muszą przejść skomplikowane testy w różnych warunkach, aby upewnić się, że działają zgodnie z założeniami i nie będą stanowiły zagrożenia dla sił własnych.

2. Reguły angażowania systemów autonomicznych: Wiele armii pracuje nad stworzeniem zasad użycia systemów autonomicznych, które zapewnią, że będą one używane tylko w określonych, kontrolowanych warunkach i nie podejmą działań przeciwko własnym wojskom.

3. Mechanizmy awaryjne i nadzór ludzki: Nawet w przypadku autonomicznych systemów wojskowych, powinny istnieć mechanizmy awaryjne pozwalające na przejęcie kontroli przez człowieka w sytuacjach kryzysowych. Powinna istnieć możliwość zatrzymania systemu w przypadku wykrycia nieprawidłowego działania.

4. Szkolenia i procedury dla operatorów: Operatorzy systemów autonomicznych powinni być odpowiednio przeszkoleni i świadomi ryzyka, jakie niosą ze sobą błędy w działaniu takich systemów. Muszą wiedzieć, jak reagować w przypadku wykrycia problemów.

5. Zabezpieczenia przed atakami cybernetycznymi: Zabezpieczenie systemów autonomicznych przed cyberatakami jest kluczowe. Stosowanie zaawansowanych technik szyfrowania, systemów wykrywania intruzów i regularnych aktualizacji oprogramowania może zmniejszyć ryzyko przejęcia kontroli nad takimi systemami przez wroga.

Podsumowanie: Tak, istnieje ryzyko, że wojskowe systemy autonomiczne mogą działać przeciwko własnym wojskom, jeśli nie będą odpowiednio zaprojektowane, kontrolowane i monitorowane. Jednak poprzez odpowiednią kontrolę, testowanie, zabezpieczenia i nadzór ludzki, można minimalizować to ryzyko i zapewnić bezpieczne zastosowanie technologii autonomicznych w wojsku”.

Oprócz odpowiedzi na pytanie Chat wskazał „rozwiązania minimalizujące ryzyko”, które służą ograniczeniu możliwości zwrócenia się sztucznej inteligencji przeciwko wojskom własnym. Natomiast w odpowiedzi zawartej

w pkt 4 Chat rozszerza zawartą w pytaniu percepcję „wojsk własnych”, wzbogacając wypowiedzi o element wojsk przyjaznych:

„4. [...] Na przykład, w trudnych warunkach konfliktu, gdzie wroga jednostkę można pomylić z własną, systemy autonomiczne mogą podjąć błędne decyzje, prowadzące do ataku na jednostki przyjazne”.

Jako niecelowo zagrożonych aktorów działań zbrojnych Chat wskazuje nie tylko wojska własne, lecz także wojska sprzymierzone i strony neutralne.

5. Czy implementowanie sztucznej inteligencji to dobry kierunek inwestowania znacznych środków finansowych z budżetu na obronność?

„Implementowanie sztucznej inteligencji (SI) w obronności jest zdecydowanie jednym z najważniejszych i obiecujących kierunków inwestycyjnych na przyszłość, jednak wymaga dokładnej analizy i rozważenia zarówno korzyści, jak i wyzwań związanych z takim podejściem. Z perspektywy obronności, inwestowanie znacznych środków finansowych w SI ma wiele zalet, ale także wiąże się z pewnymi ryzykami, które należy wziąć pod uwagę. Korzyści z inwestowania w SI w obronności:

1. Zwiększenie efektywności operacyjnej:

- automatyzacja i autonomizacja: Wykorzystanie autonomicznych systemów bojowych, dronów czy robotów bojowych może zredukować konieczność angażowania ludzi w niebezpieczne operacje, jednocześnie zwiększając efektywność operacyjną i precyzję,

- zbieranie i analiza danych: SI może przetwarzać ogromne ilości danych w czasie rzeczywistym, co pozwala na lepsze monitorowanie sytuacji na polu walki, identyfikowanie zagrożeń oraz przewidywanie ruchów wroga. To daje przewagę strategiczną, a także przyspiesza podejmowanie decyzji.

2. Poprawa cyberbezpieczeństwa. Ochrona przed atakami: SI może pomóc w szybszym wykrywaniu i reagowaniu na cyberzagrożenia, chroniąc systemy obronne przed cyberatakami. W kontekście nowoczesnych konfliktów, gdzie wojna w cyberprzestrzeni staje się coraz bardziej istotna, inwestycje w SI mogą zapewnić przewagę w obronie przed cyberatakami.

3. Redukcja ryzyka i strat ludzkich. Zminimalizowanie zaangażowania żołnierzy w niebezpiecznych misjach: Drony, roboty bojowe i inne autonomiczne systemy mogą wykonywać misje zwiadowcze, transportowe, a nawet bojowe, zmniejszając ryzyko dla życia żołnierzy i umożliwiając wykonanie niebezpiecznych operacji z większą precyzją.

4. Długoterminowa przewaga technologiczna. Inwestycje w SI mogą zapewnić krajowi długoterminową przewagę technologiczno-wojskową. Z perspektywy rozwoju technologii, SI jest kluczowym elementem przyszłościowych systemów obronnych i może decydować o przewadze w konflikcie.

Wyzwania i ryzyka:

1. Koszty rozwoju i wdrożenia: Rozwój i implementacja sztucznej inteligencji wiąże się z wysokimi kosztami. Oprócz samego zakupu technologii, wymaga to również inwestycji w badania, rozwój, szkolenia oraz infrastrukturę technologiczną. Utrzymanie i aktualizacja tych systemów także wiąże się z długoterminowymi wydatkami.

2. Zależność od technologii: Zbyt duża zależność od autonomicznych systemów może stwarzać ryzyko w przypadku ich awarii, cyberataków czy błędów w działaniu. Istnieje ryzyko, że w sytuacji awarii systemów sztucznej inteligencji, armia może zostać narażona na poważne straty lub utratę kontroli nad działaniami.

3. Etyka i odpowiedzialność: Autonomiczne systemy bojowe, zwłaszcza te zdolne do podejmowania decyzji o użyciu siły, rodzą poważne pytania etyczne. Kwestie odpowiedzialności za decyzje podjęte przez maszyny w przypadku ofiar czy zniszczeń są nadal niejasne, a międzynarodowe prawo humanitarne w tej kwestii nie zostało jeszcze jednoznacznie opracowane.

4. Cyberzagrożenia: Autonomiczne systemy oparte na SI mogą być podatne na cyberataki. Przejęcie kontroli nad systemami obronnymi przez nieautoryzowane podmioty może mieć katastrofalne konsekwencje. Inwestycje w zabezpieczenia są więc niezbędne, co dodatkowo podnosi koszty.

5. Złożoność i trudności integracyjne: Wdrażanie sztucznej inteligencji w strukturach wojskowych, które już posiadają swoje ustalone procedury, może być trudne. Integracja nowych systemów z istniejącymi technologiami, infrastruktura i systemami operacyjnymi może być czasochłonna i kosztowna.

Podsumowanie: Inwestowanie w sztuczną inteligencję na potrzeby obronności jest zdecydowanie obiecującym kierunkiem, który może przynieść znaczące korzyści, takie, jak: zwiększenie efektywności, precyzji działań, ochrony cybernetycznej czy zmniejszenie ryzyka dla żołnierzy. Niemniej jednak wiąże się to także z wysokimi kosztami, ryzykami związanymi z bezpieczeństwem i etyką, a także z potrzebą zapewnienia odpowiednich mechanizmów kontroli i nadzoru. Decyzja o takim inwestowaniu powinna być dokładnie rozważona

i oparta na długoterminowej strategii obronnej, z uwzględnieniem zarówno korzyści, jak i ryzyk, jakie mogą wyniknąć z używania sztucznej inteligencji w wojsku. Inwestowanie w SI w obronności ma sens, ale musi być częścią kompleksowego planu modernizacji armii, uwzględniającego także inne aspekty technologiczne, edukacyjne i bezpieczeństwa”.

Chat wskazuje, że zasadne jest inwestowanie w implementację sztucznej inteligencji w obszarze obronności, nie wskazuje jednak jednoznacznie inwestowania „znaczących środków finansowych”. Warto zauważyć, że Chat wspomina o mechanizmie kontroli i nadzoru, które muszą być zapewnione przy wzbogacaniu obszaru obronności o możliwości oferowane przez sztuczną inteligencję. Wskazuje również, że jej wdrożenie powinno być sprzężone z modernizacją techniczną armii z uwzględnieniem innych ważnych aspektów dotyczących funkcjonowania wojska. Ponadto podkreśla zasadność funkcjonowania dotychczasowych systemów, nie dewaluując ich przydatności. Jednocześnie zaznacza potrzebę integracji i budowania interoperacyjności. Chat prezentuje podejście komplementarne, w którym wskazuje różnorodność czynników, jakie należy uwzględnić w ocenie wykonania zadania przez system oparty na sztucznej inteligencji.

Zakończenie

Analiza potencjału wdrożenia sztucznej inteligencji na potrzeby sił zbrojnych pokazuje duże możliwości, jakie daje jej zastosowanie. Wdrożenie tej nowoczesnej technologii tworzy nowe zdolności, które w dużym stopniu mogą usprawnić dotychczas wykorzystywane mechanizmy. Użycie sztucznej inteligencji na potrzeby armii należy rozpatrywać nie tylko z perspektywy misji bojowych i wsparcia, lecz także pod względem prowadzenia działań kinetycznych i niekinetycznych, co może w znacznym stopniu wpływać na operacje w wojnie hybrydowej. Rozwój zastosowania sztucznej inteligencji zmierza w kierunku jej całkowitej autonomii, która pozwoliłaby na samodzielne wskazywanie zadań i dobieranie środków do ich wykonania. Autor zaproponował „skalę autonomii sztucznej inteligencji” uwzględniającą poziom zaangażowania człowieka i systemu w decyzyjność i sprawczość.

Wydaje się, że państwa nie mają innej drogi jak inwestowanie w rozwój sztucznej inteligencji i jej wdrożenie na potrzeby wojska, gdyż pozostanie w tyle tego wyścigu zbrojeń sztucznej inteligencji nie daje szans na przetrwanie.

Należy zaznaczyć, że sztuczna inteligencja, z którą autor przeprowadził wywiad, trafnie rozpoznaje szanse i zagrożenia związane z wykorzystaniem jej potencjału w obszarze wojskowości. Treści generowane przez Chat GPT względem wykorzystania sztucznej inteligencji na potrzeby armii pokrywały się z analizą autora. Pomimo pojedynczych nieścisłości, należy uznać, że udzielone odpowiedzi mogą być cennym narzędziem wspomagającym świadomość sytuacyjną. Zdaniem autora zasadne jest, aby podobne narzędzia z zamkniętym systemem obiegu informacji (implikowanych pytań i generowanych treści) były powszechnie wykorzystywane w wojsku.

Komisja Europejska wskazuje, że wyzwaniem jest rozwój systemów opartych na sztucznej inteligencji, które będą wolne od wad i będzie można im ufać, gdyż „kluczowym wymogiem dla osiągnięcia godnych zaufania³⁴ systemów sztucznej inteligencji jest ich wiarygodność (zdolność do dostarczania usług, którym można zasadnie zaufać) i odporność (wiarygodność w obliczu zmian). Rzetelność techniczna wymaga, aby systemy sztucznej inteligencji były rozwijane z zapobiegawczym podejściem do ryzyka, żeby zachowywały się niezawodnie i zgodnie z przeznaczeniem, minimalizując niezamierzone i nieoczekiwane szkody, a także zapobiegając im, gdy jest to możliwe”³⁵. Jedynym z bardziej oczywistych rozwiązań wydaje się skuteczne prawodawstwo, które ograniczałoby rozwój tej technologii do bezpiecznego i akceptowalnego poziomu lub zakazywałoby rozwoju niektórych obszarów tej technologii, np. tworzenia całkowicie samodzielnych systemów bojowych. Komisja Europejska zatwierdziła rezolucję, w której wyrażono zaniepokojenie możliwymi negatywnymi konsekwencjami i wpływem autonomicznych systemów uzbrojenia na bezpieczeństwo globalne oraz stabilność regionalną i międzynarodową, w tym obawy o ryzyko pojawienia się wyścigu zbrojeń, obniżenia progu konfliktu i proliferacji, także w odniesieniu do podmiotów niepaństwowych³⁶. Jednocześnie jednym z podstawowych działań ograniczających potencjalną

34 „Godna zaufania sztuczna inteligencja” odnosi się do systemów sztucznej inteligencji, które są możliwe do wyjaśnienia, uczciwe, interpretowalne, solidne, przejrzyste, bezpieczne i pewne. Zob. *What is trustworthy AI?*, <https://www.ibm.com/think/topics/trustworthy-ai> [dostęp: 23.03.2025].

35 *The Assessment List for Trustworthy...*

36 Zgromadzenie Ogólne ONZ, *Siedemdziesiąta ósma sesja, 28. Spotkanie, GA/DIS/3731, 2023*, <https://docs.un.org/en/A/C.1/78/L.56> [dostęp: 23.02.2025].

agresywną autonomię sztucznej inteligencji i przestrzeni do jej wrogiego wykorzystania może być nadanie klauzuli niejawności grupom informacji dotyczących bezpieczeństwa. W związku z tym, że technologie oparte na sztucznej inteligencji potrzebują zasilania danymi, co stanowi o ich funkcjonalności, można ją ograniczyć poprzez hamowanie dostępu do treści wrażliwych i istotnych z punktu widzenia bezpieczeństwa państwa.

Żeby swobodnie posługiwać się sztuczną inteligencją bez obaw o ryzyko niepożądanego działania, autor definiuje trzy zasadnicze obszary, które należy opanować.

Według autora rozwój sztucznej inteligencji na potrzeby armii osiągnie poziom odstraszenia i potencjalnego czynnika rażenia porównywalnego ze skutkami z efektem nuklearnym. Powyższe należy rozumieć w kategorii możliwości oddziaływania na przeciwnika, niszczenia jego potencjału i ochrony potencjału własnego. Zanim aktorzy państwowi zrozumieją, że wyścig zbrojenia sztucznej inteligencji w rezultacie doprowadzi do tragicznych konsekwencji i zanim prawo skutecznie pozwoli usankcjonować wykorzystanie sztucznej inteligencji na potrzeby walki, część podmiotów będzie dysponowała potencjałem zdolnym do masowego autonomicznego rażenia.

Konieczne jest podjęcie otwartego i eksperckiego dyskursu na arenie międzynarodowej dotyczącego wdrożenia potencjału sztucznej inteligencji na potrzeby wojska w sposób, który zapewni jej bezawaryjność, odporność na manipulację i rzeczywisty nadzór człowieka nad jej działaniem.

Bibliografia

- Allen G., Chan T., *Artificial Intelligence and National Security U.S. Intelligence Advanced Research Projects Activity (IARPA)*, Harvard Cennedy School – Belfer Center for Science and International Affairs, 2017 <https://www.belfercenter.org/sites/default/files/2024-10/Artificial%20Intelligence%20and%20National%20Security.pdf> [dostęp: 28.02.2025].
- Artificial Intelligence in Electronic Warfare*, <https://www.te.com/en/industries/defense-military/insights/ai-in-warfare-and-military-applications.html> [dostęp: 3.02.2025].
- Assessment List For Trustworthy Artificial Intelligence (ALTAI)*, Glossary, Independent High-Level Expert Group On Artificial Intelligence, Bruksela, 2020, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment> [dostęp: 3.02.2025].

- Autonomia*, <https://mfiles.pl/pl/index.php/Autonomia> [dostęp: 20.03.2025].
- Autonomia*, <https://sjp.pwn.pl/sjp/autonomia;2551312.html> [dostęp: 20.03.2025].
- Autonomia – co to jest? Definicja, synonimy, przykłady użycia*, <https://polszczyzna.pl/autonomia-co-to-jest-definicja-synonimy-przyklady-uzycia> [dostęp: 20.03.2025].
- Banafa A., *Artificial Intelligence (AI) in Modern Military Applications*, <https://www.linkedin.com/pulse/artificial-intelligence-ai-modern-military-prof-ahmed-banafa-e9sxc> [dostęp: 23.01.2025].
- Bezzałogowy pojazd bojowy nowej generacji ATLAS CCV*, 2024, <https://tacgear.pl/2024/09/bezzałogowy-pojazd-bojowy-nowej-generacji-atlas-ccv> [dostęp: 23.02.2025].
- Chat GPT: What is it?*, <https://uca.edu/cetal/chat-gpt> [dostęp: 13.11.2024].
- Comparative Analysis between OpenAI ChatGPT, Google Bard, Anthropic Claude, and Google Gemini*, <https://medium.com/@DigitalQuill.ai/comparative-analysis-between-chatgpt-bard-claude-and-gemini-ai-llms-30b7a4488c5d> [dostęp: 13.11.2024].
- Easley M., *Army implements generative AI platform to cArmy cloud environment*, 2024 <https://defensescoop.com/2024/09/10/army-generative-ai-capability-carmy-cloud> [dostęp: 2.02.2025].
- Gergelewicz T., *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas” 2024, nr 2.
- Gergelewicz T., *Countering Disinformation Concept for building social resilience in times of cognitive warfare*, „Przegląd Nauk o Obronności. Defence Science Review” 2024, nr 20.
- Kaczmarek K., Karpiuk M., Soler U., *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo E Societa” 2024, t. 20, nr 2.
- LS3: Legged Squad Support System*, <https://www.darpa.mil/research/programs/legged-squad-support-system> [dostęp: 3.03.2025].
- Nowacka A., *Zastosowanie neurofeedbacku w optymalizacji wydolności psychofizycznej żołnierzy*, <https://www.ezaf.pl/wpisy/zastosowanie-neurofeedbacku-w-optymalizacji-wydolnoscii-psychofizycznej-zolnierzy,1842> [dostęp: 7.02.2025].
- Pojazdy autonomiczne/bezzałogowe*, <https://przemyslprzyszlosci.gov.pl/technologie/cyfrowe/robotyzacja/pojazdy-autonomiczne-bezzałogowe> [dostęp: 3.03.2025].
- Rejmaniak R., *Autonomiczność systemów sztucznej inteligencji jako wyzwanie dla prawa karnego*, „Rocznik Nauk Prawnych” 2021, t. 31, nr 3.
- Testy LS3*, <https://www.youtube.com/watch?v=Ilbtwn8jwwc&t=62s> [dostęp: 3.03.2025].
- Uczenie sztucznej inteligencji, jak ma się sama uczyć*, Europejska Rada ds. Badań Naukowych, <https://cordis.europa.eu/article/id/435616-teaching-ai-to-teach-itself/pl> [dostęp: 10.03.2025].
- Weissman R., Wooten S., *A.I. Joe: The Dangers of Artificial Intelligence and the U.S. Military*, 2024, <https://www.citizen.org/article/ai-joe-report/> [dostęp: 13.01.2025].
- What is LLM (Large Language Model)?*, <https://aws.amazon.com/what-is/large-language-model/> [dostęp: 20.12.2024].
- Zequeira M., *U.S. Army, Artificial Intelligence as a Combat Multiplier, Using AI to Unburden Army Staffs*, Military Review Online Exclusive, 2024, <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier> [dostęp: 18.01.2025].

The use of artificial intelligence potential in the armed forces – interview with Chat GPT

Abstract

The implementation of artificial intelligence-based systems into the armed forces creates new capabilities that significantly reduce the burden of previously used mechanisms. The opportunities for the armed forces are indicated, which result from the use of artificial intelligence. At the same time, the challenges posed by the use of this advanced technology are highlighted. The aim of the article is to present the potential of implementing artificial intelligence for military purposes and compare it with the content generated by Chat GPT during the interview, in response to questions about various areas of artificial intelligence absorption for military purposes.

In addition, the author proposed a scale of artificial intelligence autonomy and defined three fundamental areas, which have to be mastered in order to freely use artificial intelligence without worrying about the risk of undesirable action.

The analytical method was used to distinguish areas of application of artificial intelligence for the needs of the army and indicate potential directions of its implementation. Synthesis was employed to propose a scale of system autonomy in relation to human decisions. Expert interview method was applied to examine how artificial intelligence assesses its own potential for implementation for the needs of the army.

The analysis conducted by the author, as well as the indications of the artificial intelligence itself, point many benefits of implementing artificial intelligence into the armed forces. At the same time, one has to be aware of the many threats associated with the vulnerabilities this solution currently creates.

In conclusions it is indicated that the content generated by artificial intelligence during the interview, regarding its own use for the army, is advanced; and Chat GPT can be a valuable information tool, as one of the important sources in building situational awareness.

Keywords

artificial intelligence, armed forces, security, autonomous systems, Chat GPT

Mirosław Karpiuk

Wydział Prawa i Administracji

Uniwersytet Warmińsko-Mazurski w Olsztynie

ORCID: 0000-0001-7012-8999

miroslaw.karpiuk@uwm.edu.pl

Monitorowanie zagrożeń cyberbezpieczeństwa oraz incydentów na poziomie krajowym przez CSIRT NASK i CSIRT GOV

Streszczenie

W świecie cyfrowym znaczna część aktywności jest przeniesiona do sieci. Dotyczy to zarówno sfery prywatnej, jak i publicznej. Systemy teleinformatyczne odpowiadają dzisiaj za funkcjonowanie wielu sektorów, w tym mających istotne znaczenie dla gospodarki, a także zapewnienia bezpieczeństwa państwa. Wykonywanie zadań z wykorzystaniem cyberprzestrzeni musi być bezpieczne, dlatego zarówno na organach władzy publicznej, jak i na podmiotach prywatnych (operatorach usług kluczowych, dostawcach usług cyfrowych) ciąży obowiązek ochrony odpowiednich systemów teleinformatycznych przed cyberzagroženiami. Ważne jest też odpowiednie zabezpieczenie infrastruktury krytycznej, do której działania wykorzystywane są takie systemy.

Słowa kluczowe

cyberbezpieczeństwo, cyberzagrożenia, incydenty cyberbezpieczeństwa, phishing

Wstęp

Cyfryzacja poprzez implementację zaawansowanych technologii, w tym sztucznej inteligencji, przyczynia się do automatyzacji oraz optymalizacji procesów w różnych dziedzinach, od przemysłu po usługi publiczne. Tego rodzaju zmiany mają bezpośredni wpływ nie tylko na codzienne życie obywateli, lecz

także na efektywność funkcjonowania państw. Rozwój technologii komunikacyjnych, w tym szerokopasmowego dostępu do internetu, powoduje znoszenie barier geograficznych oraz społecznych, umożliwia tym samym większą integrację na poziomie międzynarodowym¹. Niesie on również za sobą różne zagrożenia, które wymagają stosowania nowoczesnych narzędzi.

Dokonująca się obecnie transformacja cyfrowa wymaga zaangażowania wielu podmiotów zarówno ze sfery publicznej, jak i prywatnej, w tym prowadzenia odpowiedniej polityki przez państwo, które odpowiada za jej przebieg, zwłaszcza w sferze administracyjnej. Należy też zwrócić uwagę, że procesy zachodzące podczas transformacji cyfrowej są determinowane przez uwarunkowania międzynarodowe, nie można zatem wprowadzać stosownych zmian w tym zakresie w oderwaniu od polityki międzynarodowej czy rozwiązań prawno-międzynarodowych. Nowe technologie nie są domeną jednego państwa bądź kilku państw, ich zasięg jest globalny. Oddziałują one zarówno na gospodarkę międzynarodową, jak i sektor publiczny, który też musi się liczyć z uwarunkowaniami międzynarodowymi². Ponieważ cyberprzestrzeń nie ogranicza się do jednego, konkretnego państwa, ale ma charakter globalny, zatem podejście do zagrożeń w niej występujących też musi mieć taki charakter. Inaczej działania nie będą tak skuteczne, żeby zapobiegać cyberatakom czy skutecznie je zwalczać.

Zagrożenia w cyberprzestrzeni powodują coraz częściej znaczne szkody (w tym w sferze publicznej), które mogą doprowadzić nawet do ograniczenia działania lub paraliżu ważnych dla bezpieczeństwa sektorów. Ustawodawca definiuje cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniem między nimi oraz relacjami z użytkownikami³. Cyberprzestrzeń to zbiór wszystkich fizycznych i technicznych środków pozwalających na elektroniczną relację, w tym użytkowników mających dostęp do jej zasobów. Całość tych zjawisk

- 1 T. Wojciechowski, *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas” 2024, nr 1, s. 84.
- 2 C. Gaie, M. Karpiuk, A. Spaziani, *New Technologies in Public Administration*, ibidem, nr 2, s. 50.
- 3 Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, t.j., Dz.U. 2022, poz. 2091, z późn. zm., art. 2, ust. 1b.

dzieje się w jednoczesnej przestrzeni stanowiącej nowe pole ludzkich działań, gdzie są przynoszone zachowania oraz rozwiązania stosowane w świecie realnym⁴.

W przypadku zarówno generowania cyberzagrożeń, jak i im przeciwdziałania należy zwrócić uwagę na sztuczną inteligencję. Z jednej strony może być ona używana jako narzędzie przeciwko społeczeństwom, stwarzające realne zagrożenia. Wrogie podmioty mogą wykorzystywać ją do prowadzenia operacji przestępczych, czyniąc je bardzo wydajnymi. Z drugiej, sztuczna inteligencja może stać się ważnym elementem obronnym, pełnić istotną funkcję analityczną, umożliwiać szybką identyfikację i zwalczanie zagrożeń⁵. Pomimo ogromnego potencjału sztucznej inteligencji i korzyści, jakie ona niesie, nie należy zapominać o zachowaniu równowagi między postępem technologicznym a ochroną prywatności i prawami człowieka. Wprowadzając ją, należy mieć na względzie aspekty etyczne i społeczne, żeby ta technologia służyła wspólnym interesom i nie naruszała podstawowych praw i wolności⁶.

Incydenty cyberbezpieczeństwa. Studium przypadku

Polski ustawodawca cyberbezpieczeństwo definiuje jako odporność systemów informacyjnych na działania, które naruszają poufność, integralność, dostępność oraz autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy⁷. Według prawodawcy Unii Europejskiej cyberbezpieczeństwo oznacza działania, które są niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów, a także innych osób przed cyberzagrozeniami. Cyberzagrożenie to z kolei wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę, spowodować zakłócenia bądź też w inny sposób niekorzystnie wpłynąć na

4 K. Chałubińska-Jentkiewicz, *Cyberprzestrzeń*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024, s. 90.

5 T. Gergelewicz, *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas” 2024, nr 2, s. 91.

6 K. Kaczmarek, M. Karpiuk, U. Soler, *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo e Società” 2024, nr 2, s. 149.

7 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2024, poz. 1077, z późn. zm., art. 2, pkt 4.

sieci i systemy informatyczne, użytkowników takich systemów oraz inne osoby⁸. Cyberbezpieczeństwo jest pojęciem związanym z zapewnieniem ochrony i przeciwdziałaniem zagrożeniom, które dotyczą samej cyberprzestrzeni, a także funkcjonowania w niej, co odnosi się do sektora zarówno publicznego, jak i prywatnego oraz ich wzajemnych relacji⁹.

Incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Definicja ta wynika z art. 2 pkt 5 ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (u.k.s.c.). Incydent nie jest tożsamy z zagrożeniem cyberbezpieczeństwa, gdyż to drugie pojęcie, według art. 2 pkt 17 u.k.s.c., oznacza potencjalną przyczynę wystąpienia incydentu.

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, który działa na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK) monitoruje w Polsce incydenty cyberbezpieczeństwa. Odpowiada za ich obsługę w sieciach publicznych¹⁰.

- 8 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylecia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz. Urz. UE 2019, L 151/15, art. 2, pkt 1, 8.
- 9 K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo*, [w:] *Leksykon...*, s. 63. Na temat cyberbezpieczeństwa zob. także: K. Kaczmarek, *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, „Cybersecurity and Law” 2023, nr 1, s. 212; M. Czuryk, *The legal status of digital service providers in the national cybersecurity system*, ibidem 2024, nr 1, s. 39–46; M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity management – current state and directions of change*, „International Journal of Legal Studies” 2023, nr 2, s. 646; K. Kaczmarek, *Nordic countries in the face of digital threats*, „Cybersecurity and Law” 2024, nr 1, s. 152; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia” 2022, nr 3, s. 31–43; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law” 2020, nr 2, s. 57–72; K. Kaczmarek, *Vulnerability to cyber threats: a qualitative analysis from societal and institutional perspectives*, ibidem 2024, nr 2, s. 108–109; E.M. Włodyka, K. Kaczmarek, *Cyber Security of Electrical Grids – A Contribution to Research*, ibidem, nr 2, s. 262–263; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia” 2023, nr 5, s. 43–52; A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law” 2023, nr 1, s. 82–94.
- 10 F. Radoniewicz, CSIRT NASK, [w:] *Leksykon...*, s. 49.

Tabela 1. Incydenty cyberbezpieczeństwa zarejestrowane w latach 2019–2023 przez CSIRT NASK

2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6 484

Źródło: *Raport roczny z działalności CERT Polska, Warszawa 2024, s. 102.*

W 2023 roku najczęściej występującym typem incydentów zarejestrowanych były strony phishingowe. Od lat phishing zajmuje pierwsze miejsce na liście incydentów cyberbezpieczeństwa. CSIRT NASK zarejestrował 41 423 tego typu incydenty, i stanowiły one 51,61% wszystkich obsługiwanych incydentów. Najgroźniejsze kampanie phishingowe wykorzystywały wizerunek serwisu aukcyjnego Allegro – 11 161 zgłoszonych incydentów, serwisu społecznościowego Facebook – 5308 incydentów, oraz serwisu sprzedażowego OLX – 4753 przypadki. Następne w kolejności były oszustwa komputerowe – 34 304 przypadki, które stanowiły ponad 42% wszystkich zarejestrowanych incydentów. Wśród nich odnotowano fałszywe sklepy internetowe, a także oszustwa finansowe związane z podszywaniem się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy oraz instytucje. Trzecim typem incydentów, które według CSIRT NASK występowały najczęściej w 2023 roku, było szkodliwe oprogramowanie. Tego typu incydentów zarejestrowano 1650. Było to o połowę mniej niż w roku poprzednim. Ten rodzaj incydentów obejmował nie tylko infekcje oprogramowaniem ransomware, ale też kampanie spamowe, które dystrybuowały oprogramowanie Remcos i Agent Tesla¹¹.

CSIRT NASK obsłużył 40 incydentów, które uznano za poważne¹². Incydent poważny, według art. 2 pkt 7 u.k.s.c., to ten, który powoduje lub może spowodować poważne obniżenie jakości bądź przerwanie ciągłości świadczenia usługi kluczowej.

W 2023 roku CSIRT NASK obsłużył 2184 incydenty, które dotyczyły podmiotów publicznych. Najczęściej rejestrowane incydenty, które uznano jako incydenty w podmiocie publicznym, miały miejsce w sektorze administracji publicznej – 1206, w sektorze oświaty i wychowania – 282, oraz w ochronie zdrowia – 231¹³.

11 *Raport roczny z działalności CERT Polska, Warszawa 2024, s. 102.*

12 *Ibidem, s. 103.*

13 *Ibidem, s. 104.*

Tabela 2. Najczęstsze cele phishingu w 2023 roku według CSIRT NASK

Poz.	Cel phishingu	Liczba domen 2023 r.	Liczba domen 2022 r.
1	Inwestycje	20 609	2 443
2	Allegro	11 015	643
3	Baltic Pipe	6 971	583
4	Facebook	6 638	7 186
5	OLX	4 564	1 656
6	InPost	2 770	6 728
7	PGNiG	2 764	309
8	Tesla	2 758	2 647
9	Netflix	1 495	1 231
10	Webmail	1 325	562

Źródło: Raport..., s. 88.

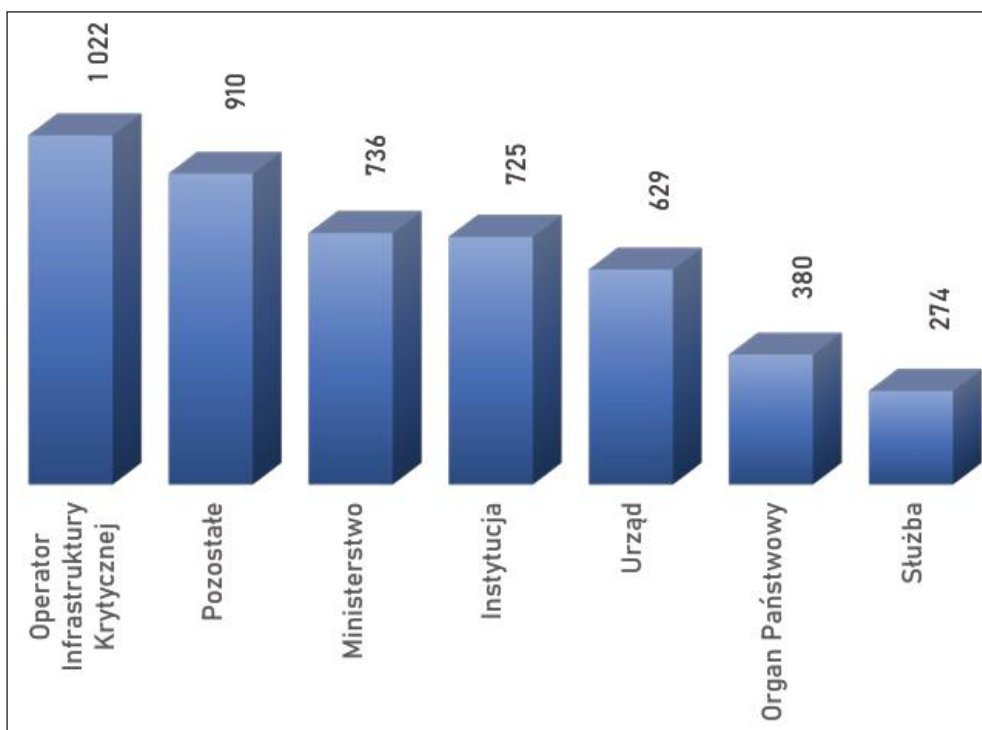
Incydent w podmiocie publicznym, według art. 2 pkt 9 u.k.s.c., to ten, który powoduje bądź też może spowodować obniżenie jakości lub przerwanie wykonania zadania publicznego przez podmiot publiczny.

Tabela 3. Incydenty cyberbezpieczeństwa zarejestrowane w 2023 roku przez CSIRT NASK z podziałem na sektory gospodarki

Sektor gospodarki	Liczba incydentów	Procent wszystkich
Handel hurtowy i detaliczny	19 253	23,99
Infrastruktura rynków finansowych	18 943	23,61
Media	10 191	12,70
Energetyka	9 196	11,46
Poczta i usługi kurierskie	5 319	6,63
Infrastruktura cyfrowa	5 101	6,35
Bankowość	2 481	3,09
Produkcja	2 353	2,93
Administracja publiczna	2 234	2,78
Osoby fizyczne	2 105	2,62
Usługi inne	902	1,12
Transport	492	0,61
Inne	451	0,56
Ochrona zdrowia	405	0,50
Oświata i wychowanie	354	0,44
Hotele, restauracje, catering	153	0,19

Źródło: Raport..., s. 102.

W Polsce zespołem reagowania na incydenty bezpieczeństwa komputerowego, prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego, jest CSIRT GOV. Jest to zespół koordynujący obsługę incydentów, które są zgłaszane przez podmioty należące do administracji rządowej, Narodowy Bank Polski, Bank Gospodarstwa Krajowego. CSIRT GOV odpowiada za rozpoznawanie, zapobieganie oraz wykrywanie zagrożeń godzących w bezpieczeństwo systemów teleinformatycznych należących do organów administracji publicznej lub systemów i sieci teleinformatycznych, które wchodzą w skład infrastruktury krytycznej¹⁴.

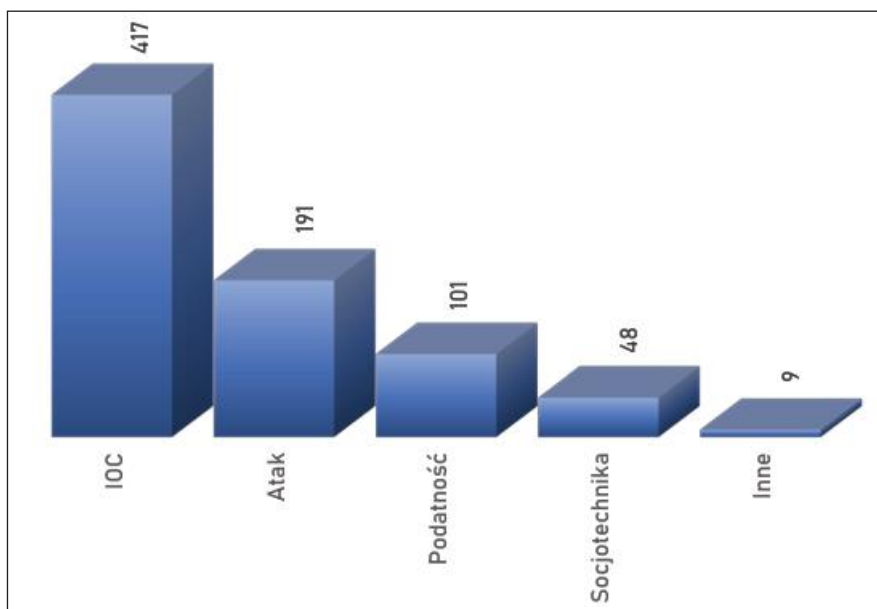


Źródło: *Raport...*, s. 13.

Wykres 1. Liczba incydentów zgłoszonych do CSIRT GOV w 2023 roku z podziałem na sektory

14 F. Radoniewicz, *CSIRT GOV*, [w:] *Leksykon...*, s. 47.

W art. 26 ust. 3 pkt 1 i 4 u.k.s.c. prawodawca wyraźnie wskazuje, że do zadań zespołów CSIRT, w tym CSIRT GOV, należy monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, a także wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Zadania te CSIRT GOV wykonuje m.in. przez wydawanie ostrzeżeń.



Źródło: *Raport...*, s. 15.

Wykres 2. Ostrzeżenia wydane przez CSIRT GOV z podziałem na kategorie

Wydawanie przez CSIRT GOV ostrzeżeń dotyczących incydentów cyberbezpieczeństwa ma charakter prewencyjny. Ma na celu ograniczać ich występowanie, a także edukować osoby korzystające z internetu z zachowania zasad cyberhigieny.

Zakończenie

W związku z szybko postępującą transformacją cyfrową oraz siecią wzajemnych połączeń w społeczeństwie, w tym w zakresie wymiany transgranicznej, sieci i systemy informatyczne stały się podstawowym elementem codziennego życia. Doprowadziło to do ewolucji krajobrazu cyberzagrożeń, ale i przyniosło nowe wyzwania wymagające dostosowanych, skoordynowanych, a także

innowacyjnych reakcji we wszystkich państwach członkowskich Unii Europejskiej. Liczba, zasięg, zaawansowanie, a także częstotliwość oraz wpływ incydentów cyberbezpieczeństwa stają się coraz większe, a przy tym poważnie zagrażają funkcjonowaniu sieci i systemów informatycznych. W efekcie mogą one utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników, a także powodować poważne szkody dla gospodarki i społeczeństwa. W związku z powyższym gotowość oraz skuteczność w sferze cyberbezpieczeństwa są coraz ważniejsze dla prawidłowego funkcjonowania rynku wewnętrznego. W wielu sektorach krytycznych cyberbezpieczeństwo należy do podstawowych czynników umożliwiających udany przebieg transformacji cyfrowej oraz pełne wykorzystanie zarówno ekonomicznych, jak i społecznych korzyści wynikających z cyfryzacji¹⁵.

Należy pamiętać że każda nowa technologia stanowi nie tylko ułatwienie, lecz także niesie za sobą zagrożenia. Współcześnie, w dobie kulturowych przemian społecznych, napływu najnowszych technologii oraz wszechobecnej sieci, bez internetu bardzo trudno byłoby funkcjonować. Należy podkreślić, że brak ostrożności w korzystaniu z niego powoduje ryzyko cyberataku, cyberprzemocy, wykorzystania wizerunku czy też phishingu. Zainfekowana sieć może wyłączyć z użytku serwery i podłączone do nich komputery. Dostępność internetu to zachęta dla przestępców do szpiegostwa przemysłowego czy wykradania danych. Atrakcyjność wirtualnego świata powoduje, że bardzo dużym problemem jest uzależnienie od internetu, które skutkuje rozpadem więzi społecznych, chorobami, a także dysfunkcją społeczną¹⁶.

Niektóre systemy teleinformatyczne odpowiadają za stabilność państwa i jego gospodarki, dlatego muszą być należycie chronione¹⁷. Ochrona ta powinna zabezpieczać przed nieuprawnioną ingerencją ograniczającą ich funkcjonowanie, ponieważ może poważnie zagrażać bezpieczeństwu państwa,

15 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz. Urz. UE 2022, L 333/80, motyw 3.

16 B. Grabowski, *Cyfrowe zagrożenia – zarys problemu*, „Ius et Securitas” 2024, nr 1, s. 103.

17 A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, s. 89–90.

a także powodować duże szkody w gospodarce. Szczególna ochrona powinna obejmować systemy, które odpowiadają za funkcjonowanie infrastruktury krytycznej zabezpieczającej podstawowe sektory decydujące o stabilności państwa.

Bibliografia

- Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law” 2023, nr 1.
- Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.
- Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.
- Chałubińska-Jentkiewicz K., *Cyberprzestrzeń*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.
- Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia” 2023, nr 5.
- Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia” 2022, nr 3.
- Czuryk M., *The legal status of digital service providers in the national cybersecurity system*, „Cybersecurity and Law” 2024, nr 1.
- Gaie C., Karpiuk M., Spaziani A., *New Technologies in Public Administration*, „Ius et Securitas” 2024, nr 2.
- Gergelewicz T., *Bipolarity of Artificial Intelligence – Chances and Threats*, „Ius et Securitas” 2024, nr 2.
- Grabowski B., *Cyfrowe zagrożenia – zarys problemu*, „Ius et Securitas” 2024, nr 1.
- Kaczmarek K., *Finland in the light of cyber threats in the context of Russia’s aggression against Ukraine*, „Cybersecurity and Law” 2023, nr 1.
- Kaczmarek K., Karpiuk M., Soler U., *The Potential Use of Artificial Intelligence in Crisis Management*, „Sicurezza, Terrorismo e Società” 2024, nr 2.
- Kaczmarek K., *Nordic countries in the face of digital threats*, „Cybersecurity and Law” 2024, nr 1.
- Kaczmarek K., *Vulnerability to cyber threats: a qualitative analysis from societal and institutional perspectives*, „Cybersecurity and Law” 2024, nr 2.
- Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity management – current state and directions of change*, „International Journal of Legal Studies” 2023, nr 2.
- Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law” 2020, nr 2.
- Radoniewicz F., *CSIRT GOV*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.

Radoniewicz F., *CSIRT NASK*, [w:] *Leksykon cyberbezpieczeństwa*, red. K. Chałubińska-Jentkiewicz, Warszawa 2024.

Włodyka E.M., Kaczmarek K., *Cyber Security of Electrical Grids – A Contribution to Research*, „Cybersecurity and Law” 2024, nr 2.

Wojciechowski T., *Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego*, „Ius et Securitas” 2024, nr 1.

Monitoring Cybersecurity Threats and Incidents at the National Level by CSIRT NASK and CSIRT GOV

Abstract

In the digital world, a significant part of the activity is transferred to the network. This applies to both the private and public spheres. Today, IT systems are responsible for the functioning of many sectors, including those that are of significant importance to the economy and ensuring state security. Performing tasks using cyberspace must be safe, which is why both public authorities and private entities (operators of key services, digital service providers) are obliged to protect the appropriate IT systems from cyber threats. It is also important to properly secure the critical infrastructure for which such systems are used.

Keywords

cybersecurity, cyber threats, cybersecurity incidents, phishing

Dorota Sylwia Majewicz
Politechnika Koszalińska
ORCID: 0000-0003-4568-3549
e-mail: dorota.majewicz@gmail.com

Linguistic Nuances in Crisis Communication: Advancing Conflict Mediation and Defense Education in Poland

Abstract

This article explores the significance of linguistic nuances in crisis communication within the context of defense education in Poland. The author highlights the pivotal role of syntax, semantics, and cultural connotations in effectively conveying information during crisis situations. Emphasis is placed on the importance of cultural sensitivity and mediation competencies, as well as their integration within the legal frameworks applicable in Poland. An interdisciplinary approach is adopted, combining insights from linguistics, crisis management, and higher education. As a result, contextually sensitive communication strategies are proposed for Polish institutions of higher education.

Keywords

crisis communication, defense education, mediation, linguistic sensitivity, Poland

Introduction

Crisis communication has emerged as a crucial aspect of defense education, particularly in the context of Poland's unique socio-political landscape. Effective communication during crises is not merely a matter of relaying information; it involves an intricate interplay of linguistic nuances that can significantly influence the clarity, trust, and overall efficacy of emergency

responses. As highlighted in contemporary research, the adaptation of communication strategies to cater to diverse linguistic and cultural contexts is essential, with particular attention to the roles of syntax, semantics, and cultural connotations¹. In the context of Polish higher education, where the risks of miscommunication can have dire consequences in crisis scenarios, the call for context-sensitive frameworks becomes increasingly urgent. This paper aims to explore the critical importance of linguistic sensitivity and cultural adaptation in enhancing mediation strategies within defense education, positing that miscommunication not only undermines response efforts but also jeopardizes the safety and well-being of students and faculty alike. Mediation and crisis communication strategies in Poland operate within a robust legal framework. Articles 183(1)–183(15) of the Polish Civil Code² provide formal guidelines for mediation, while the Act on Mediation and Conciliation in Collective Disputes ensures its adaptability across sectors, including education. Together, these laws form a foundation for integrating mediation into defense education. By examining effective tools and frameworks, such as infographics, which have been shown to improve understanding and engagement in global studies³, this study will offer concrete recommendations for Polish universities to incorporate linguistically nuanced strategies into their crisis communication training. Ultimately, bridging the fields of linguistics, mediation, and crisis management can create safer academic environments, fostering resilience and preparedness in the face of emergencies. Grounded in Art. 68 and 54 of the Constitution of the Republic of Poland⁴, linguistically sensitive and transparent communication frameworks uphold the fundamental rights to safety and expression, fostering trust and resilience in academic communities.

- 1 G. Georgakopoulos, B. O'Dwyer, *Processes of auditability in sustainability assurance – the case of materiality construction*, „Accounting and Business Research” 2019, vol. 49, no. 1; C. Menkel-Meadow, A.K. Schneider, *International Conflict Resolution Processes*, SSRN Working Paper 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5168799 [access: 2.03.2025].
- 2 Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego, Dz.U. 2024, item. 1568, as amended, Art. 183¹–183¹⁵.
- 3 R.W. Setyaningrum, S. Anam, *Translanguaging as a scaffolded practice in a primary school CLIL context during the COVID-19 pandemic*, „European Journal of Educational Research” 2022, vol. 11, no. 4.
- 4 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, no. 78, item. 483, as amended, Art. 68, 54.

Linguistic Sensitivity in Crisis Communication

In crisis communication, the subtle interplay between syntax and semantics significantly shapes the strategies employed by organizations to manage and resolve crises. The framing of messages, whether emotional or rational, directly influences public perception and organizational reputation during crises, as evidenced by studies on the impact of such framing techniques⁵. This is particularly crucial when considering the semantic fields and neural binding processes involved in crafting effective crisis communication strategies that resonate with the audience⁶. Understanding the semantics of „crisis” itself, from a cognitive perspective, helps in identifying central semantic problems that may arise, thereby improving the overall efficacy of crisis management strategies⁷. To optimize these strategies, it is essential for organizations to integrate a nuanced understanding of syntax and semantics into their communication efforts, ensuring messages are not only clear but also contextually relevant. This approach can greatly enhance the alignment of messages with the intended audience, ultimately leading to more effective crisis resolution and management⁸. Therefore, a comprehensive incorporation of syntax and semantics into crisis communication strategies is imperative for organizations looking to navigate crises successfully.

In the context of emergency response communication, cultural connotations play a pivotal role in shaping the effectiveness of the messages conveyed to diverse communities. The research emphasizes the importance of cultural literacy and humility, which are crucial for developing communication strategies that resonate with the cultural contexts of different communities⁹.

- 5 A. Claeys, V. Cauberghe, *What makes crisis response strategies work? The impact of crisis involvement and message framing*, „Journal of Business Research” 2014, vol. 67, no. 2.
- 6 M. Conoscenti, *The Deepwater Horizon Crisis: A Linguistic and Cognitive Analysis of BP Communicative Strategy*, 2012, <https://iris.unito.it/handle/2318/110597> [access: 19.01.2025].
- 7 *Discourse in crisis: critical perspectives*, red. A. De Rycker, Z. Mohd Don, 2013, <https://www.degruyter.com/document/doi/10.1075/dapsac.52.01der/html> [access: 19.01.2025].
- 8 M. Sigala, *Social media and crisis management in tourism: Applications and implications for research*, „Current Issues in Tourism” 2011, vol. 22, no. 5.
- 9 T. Vandrevalla et al., *Strengthening the relationship between community resilience and health emergency communication: a systematic review*, „BMC Public Health”

Integrating cultural sensitivities into emergency planning is not just a best practice, but a necessity for building genuinely responsive and resilient systems. When communication strategies reflect the lived realities and cultural values of local communities, messages are more likely to resonate and prompt action. More importantly, when community members are treated not just as recipients but as contributors in the planning process, they become active participants in shaping outcomes. This collaborative approach enhances both the legitimacy and long-term impact of emergency responses. A model that values inclusivity, encourages reflection, and acknowledges the insights of non-experts helps shift the dynamic toward shared responsibility and mutual trust. Ultimately, these strategies highlight the need for continuous learning and adaptation, ensuring that communication efforts are culturally sensitive and tailored to meet the unique needs of each community.

In adapting communication strategies to diverse linguistic contexts, it is essential to consider the interplay between local practices and global methodologies like Communicative Language Teaching (CLT) and Task-Based Language Teaching (TBLT). These approaches, when adapted to the local environments, can address specific conceptual, classroom-level, and societal-institutional constraints, ensuring that language education is both effective and culturally relevant. Moreover, the adoption of innovative or decentralized language-in-education policies can offer additional avenues for adapting these strategies, allowing for flexibility and creativity in multilingual settings¹⁰. The integration of English as a Lingua Franca (ELF) can also play a critical role by enhancing collaborative communication, thus bridging gaps between speakers of different linguistic backgrounds and developing mutual understanding – an approach that not only facilitates improved communication but also encourages the valuing of diverse linguistic resources, which can be crucial in corporate or institutional settings striving for inclusivity. Emphasizing the adaptability of communication strategies, particularly in environments characterized by linguistic super-diversity, calls for „an enhanced focus on languaging” – a phenomenon that supports multilingual practices and encourages speakers

2024, no. 2, <https://link.springer.com/article/10.1186/s44263-024-00112-y> [access: 19.01.2025].

10 Y.G. Butler., *The Implementation of Communicative and Task-Based Language Teaching in the Asia-Pacific Region*, Cambridge 2016.

to utilize their entire linguistic repertoire to effectively convey and interpret messages¹¹. To achieve this, interventions should focus on creating policies and educational frameworks that are flexible, context-aware, and inclusive of the linguistic diversity present in various regions.

Importance of Cultural Adaptation in Defense Education

Cultural adaptation plays a crucial role in Polish higher education as it aligns with the increasing demands of the global job market, where intercultural competencies are becoming indispensable. Higher education institutions bear the responsibility of preparing students not only in their respective disciplines but also in navigating culturally diverse contexts with competence. In today's interconnected world, the ability to work across cultural lines has shifted from a desirable trait to a professional imperative. As organizations increasingly operate on a global scale, effectively engaging with cultural diversity is now seen as a key driver of innovation and strategic success. Thus, universities need to integrate opportunities that help students build cultural awareness and adaptability throughout their academic development¹². By developing these competencies, Polish higher education institutions can better prepare graduates for the complexities of a multicultural workforce, ensuring they possess the skills required to succeed in a diverse and interconnected world.

In academic environments, the risks of miscommunication during crisis scenarios are profound, often resulting from the failure to establish and maintain effective communication channels prior to emergencies. When institutions fail to cultivate and test communication strategies outside of crisis situations, their ability to convey essential information under pressure can be significantly compromised. In such cases, the lack of structured, two-way communication between university leadership and the student body often results in a disconnect – leaving student needs misunderstood and response measures poorly aligned with lived experiences, particularly during events

11 A. Cogo, *ELF and super-diversity: a case study of ELF multilingual practices from a business context*, „Journal of English as a Lingua Franca” 2012, vol. 1, no. 2.

12 A. Knap-Stefaniuk, Ł. Burkiewicz, *Rozwój systemu komunikacji kryzysowej w Polsce*, „Ius Novum” 2023, <https://bibliotekanauki.pl/articles/1597280.pdf> [access: 19.01.2025].

like forced relocations. Additionally, when vital support systems are not clearly and proactively communicated, students may be unaware of available resources, heightening their risk and undermining their resilience in times of emergency¹³. These interconnected challenges highlight the necessity for proactive measures, including the establishment of clear, consistent, and transparent communication practices well in advance of any crisis. By doing so, academic institutions can enhance their preparedness and responsiveness, ultimately safeguarding the well-being and trust of their stakeholders.

Building on the concept of empowerment and inclusion in emergency response communication, cultural adaptation emerges as a pivotal factor in enhancing the effectiveness of mediation strategies. By fostering cultural intelligence (CQ), individuals can significantly improve social performance, which is essential for effective mediation¹⁴. Incorporating linguistically nuanced mediation strategies aligns with Art. 267 of the Act on Higher Education and Science¹⁵, which empowers universities to develop autonomous safety and crisis response protocols. This approach ensures both legal compliance and effective conflict resolution. This enhanced social performance not only facilitates innovation but also strengthens the capability to manage and resolve conflicts effectively; furthermore, individuals with high CQ are adept at understanding and appreciating diverse cultural perspectives, which is crucial in maintaining harmony and relationships among parties involved in mediation¹⁶. Such cultural awareness helps overcome divisions and reduce conflicts, creating the foundation for stronger social unity – an essential element in effective mediation. Therefore, integrating cultural adaptation into mediation strategies is vital for achieving effective and sustainable conflict resolution, necessitating deliberate efforts to cultivate cultural intelligence and adaptive capacities in mediators.

- 13 H. Wu, *Mass email risk communication: Lessons learned from COVID-19-triggered campus-wide evictions in Canada and the United States*, PLOS ONE 2023, <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0289117> [access: 19.01.2025].
- 14 U. Awan, A. Kraslawski, J. Huiskonen, *The impact of relational governance on performance improvement in export manufacturing firms*, „Journal of Industrial Engineering and Management” 2018, vol. 11, no. 3.
- 15 Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, Dz.U. 2018, item. 1668, as amended, Art. 267.
- 16 U. Awan, A. Kraslawski, J. Huiskonen, op. cit.

Tools and Frameworks for Effective Communication

In recommending context-sensitive frameworks for Polish universities, it is crucial to adopt methodologies that align with both the specific educational needs and cultural contexts of Poland. The development of a comprehensive framework that includes context-sensitive approaches is essential for Polish universities to enhance their educational offerings and research outputs¹⁷. This involves integrating techniques from existing frameworks that have been effectively utilized in different contexts, such as context-sensitive explorations and implications drawn from diverse sectors like Mobile Commerce and public good frameworks¹⁸. By doing so, Polish universities can create environments that are not only sensitive to local needs but also adaptive to global academic standards, ultimately contributing to the broader educational landscape. To achieve this, ongoing evaluations and adaptations of these frameworks will be necessary, ensuring that they remain responsive to the evolving educational and socio-cultural dynamics.

In the realm of global crisis communication, infographics have emerged as a vital tool for effectively disseminating complex data and facilitating a comprehensive understanding among diverse audiences. The integration of strategic communication and visual design is pivotal during global crises, as infographics can bridge cultural and linguistic divides, ensuring that critical information is conveyed efficiently across different communities¹⁹. Notably, infographics serve not only as connectors of data but also as collective calls to action, which can galvanize public response to crises. This dual

17 C. Atkinson, P. Bostan, T. Butter, *SALSA—A Framework for Context-Sensitive Service Discovery in Mobile Commerce Applications*, <https://journals.riverpublishers.com> [access: 19.01.2025].

18 M. Krzyżanowski, *Ethnography and critical discourse analysis: towards a problem-oriented research dialogue*, „Critical Discourse Studies” 2011, <https://www.tandfonline.com/doi/full/10.1080/17405904.2011.601630> [access: 19.01.2025]; E. Brewis, S. Marginson, *Introduction to the special issue: 'The public good of higher education: A comparative study'*, „Higher Education” 2024, <https://link.springer.com/article/10.1007/s10734-024-01346-3> [access: 19.01.2025].

19 V. Diwanji, J. Cortese, P. Merle, *Fighting a Global Pandemic in the Digital Age: Use of Infographics to 'Flatten the Curve' in the US and India*, „Journal of International Communication” 2023, <https://www.tandfonline.com/doi/abs/10.1080/1553118X.2023.2231409> [access: 19.01.2025].

function highlights their ability to both inform and motivate action, thereby enhancing their effectiveness in crisis scenarios²⁰. Moreover, the use of visual-based infographics, particularly when aligned with appropriate framing techniques, can significantly enhance message retention and engagement compared to text-based communication alone²¹. Therefore, it is imperative for crisis communication teams to harness the full potential of infographics by integrating them strategically within their communication frameworks, thereby optimizing their impact in managing and resolving crises.

Improving the clarity and credibility of emergency responses requires the integration of tools that facilitate both communication and cooperation. Digital platforms, in particular, can optimize how information flows within response teams, reducing administrative burdens and enabling a stronger focus on mission-critical activities. These technologies support the timely and accurate delivery of essential updates, which is vital for maintaining transparency and trust across teams and with external partners. Additionally, by creating a culture that values feedback and continuous learning, organizations can evolve their strategic approach to emergency coordination—strengthening both internal alignment and public confidence²². By adopting these integrated tools and practices, emergency response teams can achieve a more cohesive understanding of situations, thereby improving the overall effectiveness of their actions.

Recommendations for Polish Universities

In the context of Polish defense education, implementing linguistically nuanced strategies requires a multifaceted approach that acknowledges the

- 20 D. Kaviani, N. Salehi, *Bridging action frames: Instagram infographics in US ethnic movements*, [w:] *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW1, New York 2022, <https://dl.acm.org/doi/abs/10.1145/3512926> [access: 19.01.2025].
- 21 S. Lee, J. Kim, Y. Sung, *When infographics work better: The interplay between temporal frame and message format in e-health communication*, „Psychology & Health” 2021, <https://www.tandfonline.com/doi/abs/10.1080/08870446.2021.1912342> [access: 19.01.2025].
- 22 M. Ohrling, K. Solberg Carlsson, M. Brommels, *No man is an island: management of the emergency response to the SARS-CoV-2 (COVID-19) outbreak in a large public decentralised service delivery organisation*, „BMC Health Services Research” 2022, <https://link.springer.com/article/10.1186/s12913-022-07716-w> [access: 19.01.2025].

complex interplay between language, culture, and policy. Language policies within the education system should not be confined to minimal linguistic rights but rather should embrace linguistic diversity to foster a more inclusive educational environment²³. This inclusivity can be achieved by integrating authentic reading and listening texts that highlight the nuances of different languages, thus aiding in preventing linguistic fossilization and enhancing students' linguistic competence²⁴. Furthermore, the strategic use of discursive strategies can facilitate a deeper understanding of the cultural and historical contexts of defense education, thereby enabling students to grasp the nuanced meanings of policies and narratives related to national security²⁵. By employing these strategies, Polish defense education can cultivate a more comprehensive understanding of national identity and security, while also promoting critical thinking and empathy among students. Such an educational framework not only prepares students for complex geopolitical challenges but also nurtures a generation that values linguistic and cultural diversity as a strength rather than a barrier.

The integration of linguistics into crisis management holds great potential for creating safer academic environments by enhancing communication and understanding during emergencies. Effective crisis management requires clear, concise, and culturally sensitive communication, which can be achieved by understanding and utilizing the nuances of language in emergency scenarios. By maintaining a personalized language approach in crisis response, institutions can foster a sense of safety and community, which is vital in ensuring effective communication during emergencies²⁶. Effective crisis communication strategies must align with Art. 115–128 of the Polish Penal

23 N. Albury, K. Aye, *Malaysia's national language policy in international theoretical context*, <https://www.duo.uio.no/handle/10852/58857> [access: 19.01.2025].

24 M. Ehrman, *Understanding the learner at the Superior-Distinguished threshold*, Washington 2007.

25 M. Krzyżanowski, *Ethnography and critical discourse analysis: towards a problem-oriented research dialogue*, „Critical Discourse Studies” 2011, vol. 8, no. 4.

26 S. Veil, T. Buehner, *A work-in-process literature review: Incorporating social media in risk and crisis communication*, „Journal of Contingencies and Crisis Management” 2015, vol. 19, no. 2.

Code²⁷, which mandate the safeguarding of public safety in scenarios involving terrorism or mass endangerment. Such alignment enhances institutional preparedness and response efficacy. Interorganizational communication and decision-making are also crucial components of crisis management in academic settings, which can be significantly improved by incorporating linguistics into communication strategies²⁸. Moreover, the use of language skills in crisis management not only facilitates the dissemination of vital information but also aids in bridging the gap between institutional protocols and individual understanding, thus ensuring that all stakeholders are on the same page²⁹. This multidisciplinary approach not only supports the efficient management of crises but also contributes to a more resilient and cohesive academic community. To implement these strategies effectively, educational institutions must prioritize training and development programs that focus on enhancing linguistic competencies in crisis communication, thereby fostering an environment where safety and understanding are paramount.

Incorporating mediation strategies into crisis communication training requires a multifaceted approach that emphasizes the need for strategic anticipation and the integration of diverse expertise. A key step involves understanding the interplay between different crisis types and the respective communication strategies that can effectively address them³⁰. This understanding necessitates the adoption of a holistic framework that draws from multiple disciplines, including strategic management and mediation, as these fields offer valuable insights into the complexities of crisis scenarios³¹. Mediation skills are crucial in this context for those involved in crisis communication, as it equips them to manage disputes and foster constructive conversations between affected parties. To build these

27 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 1997, no. 88, item. 553, as amended, Art. 115–128.

28 N. Kapucu, *Interagency communication networks during emergencies: Boundary spanners in multiagency coordination*, „Public Administration Review” 2006, no. 36.

29 H. Eshach, *Bridging in-school and out-of-school learning: Formal, non-formal, and informal education*, „Journal of Science Education and Technology” 2006, no. 2.

30 S. Utz, F. Schultz, S. Glocka., *Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster*, „Public Relations Review” 2013, no. 39.

31 J. Bundy, M. Pfarrer, C. Short, *Crises and crisis management: Integration, interpretation, and research development*, „Journal of Management” 2016, vol. 43, no. 6.

competencies, educational and training initiatives should emphasize hands-on scenarios where participants can practice mediation strategies in controlled, crisis-like environments. Such experiential learning reinforces their capacity to respond effectively when confronted with real-life emergencies.

The findings of this research paper illuminate the profound impact of linguistic nuances on crisis communication, particularly within the context of Poland's defense education and conflict mediation strategies. By emphasizing the relationship between syntax, semantics, and effective message framing, this study aligns with existing literature that advocates for a more refined understanding of communication dynamics during crises. The cognitive interpretation of „crisis” as highlighted in the paper underscores the necessity for organizations to adopt a more nuanced approach, integrating linguistic insights into their communication strategies. This is particularly relevant in Poland, where diverse cultural connotations can greatly influence public perception and response. However, while the paper advocates for the integration of local practices with global methodologies, it also raises important questions about the scalability and adaptability of these strategies across varying linguistic contexts. Future research should explore the effectiveness of these communication strategies in different crisis scenarios and among diverse populations. Additionally, the discussion on the risks of miscommunication in academic settings prompts a critical examination of existing communication frameworks, suggesting a need for proactive measures that enhance preparedness and responsiveness in crisis situations. The recommendation for context-sensitive frameworks in Polish universities is particularly timely, as educational institutions strive to align their offerings with both local and global standards. Yet, the study may benefit from a more detailed exploration of the specific challenges faced by educators in implementing these strategies. As the research underscores the intersection of linguistic diversity and cultural adaptation, it opens avenues for further investigation into the role of English as a Lingua Franca (ELF) in facilitating effective communication among multilingual populations. Overall, the paper advocates for a holistic approach to crisis management that incorporates linguistic and cultural sensitivity, thereby contributing valuable insights to the ongoing discourse on effective crisis communication and management within the context of Poland's evolving socio-political landscape.

Bibliography

- Albury N., Aye K., *Malaysia's national language policy in international theoretical context*, <https://www.duo.uio.no/handle/10852/58857> [access: 19.01.2025].
- Atkinson C., P Bostan., Butter T., *SALSA–A Framework for Context-Sensitive Service Discovery in Mobile Commerce Applications*, <https://journals.riverpublishers.com> [access: 19.01.2025].
- Awan U., Kraslawski A., Huiskonen J., *The impact of relational governance on performance improvement in export manufacturing firms*, „Journal of Industrial Engineering and Management” 2018, vol. 11, no. 3.
- Brewis E., Marginson S., *Introduction to the special issue: 'The public good of higher education: A comparative study'*, „Higher Education” 2024, <https://link.springer.com/article/10.1007/s10734-024-01346-3> [access: 19.01.2025].
- Bundy J., M Pfarrer., Short C., *Crises and crisis management: Integration, interpretation, and research development*, „Journal of Management” 2016, vol. 43, no. 6.
- Butler Y.G., *The Implementation of Communicative and Task-Based Language Teaching in the Asia-Pacific Region*, Cambridge 2016.
- Claeys A., Cauberghe V., *What makes crisis response strategies work? The impact of crisis involvement and message framing*, „Journal of Business Research” 2014, vol. 67, no. 2.
- Cogo A., *ELF and super-diversity: a case study of ELF multilingual practices from a business context*, „Journal of English as a Lingua Franca” 2012, vol. 1, no. 2.
- Conoscenti M., *The Deepwater Horizon Crisis: A Linguistic and Cognitive Analysis of BP Communicative Strategy*, 2012, <https://iris.unito.it/handle/2318/110597> [access: 19.01.2025].
- Discourse in crisis: critical perspectives*, red. A. De Rycker, Z. Mohd Don, 2013, <https://www.degruyter.com/document/doi/10.1075/dapsac.52.01der/html> [access: 19.01.2025].
- Diwanji V., Cortese J., Merle P., *Fighting a Global Pandemic in the Digital Age: Use of Infographics to 'Flatten the Curve' in the US and India*, „Journal of International Communication” 2023, <https://www.tandfonline.com/doi/abs/10.1080/1553118X.2023.2231409> [access: 19.01.2025].
- Ehrman M., *Understanding the learner at the Superior-Distinguished threshold*, Washington 2007.
- Eshach H., *Bridging in-school and out-of-school learning: Formal, non-formal, and informal education*, „Journal of Science Education and Technology” 2006, no. 2.
- Georgakopoulos G., O'Dwyer B., *Processes of auditability in sustainability assurance – the case of materiality construction*, „Accounting and Business Research” 2019, vol. 49, no. 1.
- Kapucu N., *Interagency communication networks during emergencies: Boundary spanners in multiagency coordination*, „Public Administration Review” 2006, no. 36.

- Kaviani D., N. Salehi, *Bridging action frames: Instagram infographics in US ethnic movements*, [w:] *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW1, New York 2022.
- Knap-Stefaniuk A., Burkiewicz Ł., *Rozwój systemu komunikacji kryzysowej w Polsce*, „Ius Novum” 2023, <https://bibliotekanauki.pl/articles/1597280.pdf> [access: 19.01.2025].
- Krzyżanowski M., *Ethnography and critical discourse analysis: towards a problem-oriented research dialogue*, „Critical Discourse Studies” 2011, vol. 8, no. 4.
- Lee S., Kim J., Sung Y., *When infographics work better: The interplay between temporal frame and message format in e-health communication*, „Psychology & Health” 2021, <https://www.tandfonline.com/doi/abs/10.1080/08870446.2021.1912342> [access: 19.01.2025].
- Menkel-Meadow C., Schneider A.K., *International Conflict Resolution Processes*, SSRN Working Paper 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5168799 [access: 2.03.2025].
- Ohrling M., Solberg Carlsson K., Brommels M., *No man is an island: management of the emergency response to the SARS-CoV-2 (COVID-19) outbreak in a large public decentralised service delivery organisation*, „BMC Health Services Research” 2022, <https://link.springer.com/article/10.1186/s12913-022-07716-w> [access: 19.01.2025].
- Setyaningrum R.W., Anam S., *Translanguaging as a scaffolded practice in a primary school CLIL context during the COVID-19 pandemic*, „European Journal of Educational Research” 2022, vol. 11, no. 4.
- Sigala M., *Social media and crisis management in tourism: Applications and implications for research*, „Current Issues in Tourism” 2011, vol. 22, no. 5.
- Utz S., F. Schultz., Glocka S., *Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster*, „Public Relations Review” 2013, no. 39.
- Vandrevala T. et al., *Strengthening the relationship between community resilience and health emergency communication: a systematic review*, „BMC Public Health” 2024, <https://link.springer.com/article/10.1186/s44263-024-00112-y> [access: 19.01.2025].
- Veil S., T Buehner., *A work-in-process literature review: Incorporating social media in risk and crisis communication*, „Journal of Contingencies and Crisis Management” 2015, vol. 19, no. 2.
- Wu H., *Mass email risk communication: Lessons learned from COVID-19-triggered campus-wide evictions in Canada and the United States*, PLOS ONE 2023, <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0289117> [access: 19.01.2025].

Językowe niuansy w komunikacji kryzysowej: rozwój mediacji i edukacji obronnej w Polsce

Streszczenie

W artykule omówiono znaczenie niuansów językowych w komunikacji kryzysowej w kontekście edukacji obronnej w Polsce. Autorka wskazuje ważną rolę składni, semantyki i konotacji kulturowych w skutecznym przekazywaniu informacji w sytuacjach kryzysowych. Podkreślono znaczenie wrażliwości kulturowej i kompetencji mediacyjnych oraz ich integracji z aktami prawnymi obowiązującymi w Polsce. Zastosowano podejście interdyscyplinarne, które łączy lingwistykę, zarządzanie kryzysowe i edukację wyższą. W efekcie zaproponowano kontekstowo wrażliwe strategie komunikacyjne dla polskich uczelni wyższych.

Słowa kluczowe

komunikacja kryzysowa, edukacja obronna, mediacja, wrażliwość językowa, Polska

mjr dr Mariusz Domżański

Dowództwo 18 Dywizji Zmechanizowanej im. gen. broni Tadeusza Buka

ORCID: 0000-0002-7749-2598

mail: mariuszdomzanski89@gmail.com

Fakultatywne zwolnienie ze służby funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego

Streszczenie

Ustawodawca utworzył Służbę Kontrwywiadu Wojskowego jako służbę specjalną, właściwą w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej. Służba Wywiadu Wojskowego, jako służba specjalna, jest właściwa w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej. W związku z tym, że zadania obu tych służb mają bardzo duże znaczenia dla obronności kraju ważny jest też status funkcjonariuszy tych służb, a szczególnie stabilność służby.

Słowa kluczowe

służby mundurowe, zwolnienie, stosunek służbowy

Wstęp

Stosunek służbowy funkcjonariuszy służb mundurowych ma wiele swoistych cech, które odróżniają go od stosunku pracy. Najważniejsze cechy to: publicznoprawny charakter zatrudnienia i wynikająca z tego nierównorzędność stron, jednostronny tryb zwolnienia ze służby, wzmożona dyspozycyjność i podporządkowanie, szczególny charakter obowiązków, trwałość zatrudnienia.

Ustawy regulujące stosunki służbowe zawierają zamknięte katalogi stanów faktycznych, których wystąpienie umożliwia zwolnienie funkcjonariusza ze służby. Ustawa z 9 czerwca 2006 roku o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego¹ wyróżnia przyoczyny obligatoryjne oraz fakultatywne zwolnienia ze służby. Mając na względzie ograniczenia objętościowe artykułu, autor skupił się na przedmiotowych regulacjach dotyczących wyłącznie przesłanek fakultatywnych.

**Niewywiązywanie się z obowiązków służbowych w czasie odbywania
służby stałej, stwierdzone w dwóch kolejnych opiniach,
między którymi upłynęło co najmniej 6 miesięcy
(art. 19 ust. 2 pkt 1 ustawy)**

Pierwszą przesłanką, której wystąpienie powoduje fakultatywne zwolnienie funkcjonariusza ze służby, jest uzyskanie przez niego negatywnej opinii służbowej.

Istotny w przypadku wystąpienia tej przesłanki jest rodzaj służby pełnionej przez funkcjonariusza. Funkcjonariusz zostaje mianowany na stałe po upływie okresu służby przygotowawczej trwającej 3 lata i uzyskaniu pozytywnej oceny ogólnej w opinii służbowej. W przypadkach uzasadnionych szczególnymi kwalifikacjami szef SKW (SWW) może skrócić okres jego służby przygotowawczej albo zwolnić funkcjonariusza od jej odbywania.

Funkcjonariusz podlega okresowemu opiniowaniu służbowemu przeprowadzanemu w służbie stałej raz na 2 lata.

Aktem prawnym określającym szczegółowe zasady i tryb okresowego opiniowania służbowego funkcjonariuszy SKW jest rozporządzenie Ministra Obrony Narodowej z 21 marca 2022 roku w sprawie opiniowania służbowego funkcjonariuszy służby Kontrwywiadu Wojskowego², dla funkcjonariuszy SWW – rozporządzenie Ministra Obrony Narodowej z 10 lutego 2017 roku

- 1 Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego, t.j., Dz.U. 2023, poz. 2098, z późn. zm.
- 2 Rozporządzenie Ministra Obrony Narodowej z dnia 21 marca 2022 r. w sprawie opiniowania służbowego funkcjonariuszy służby Kontrwywiadu Wojskowego, Dz.U. 2022, poz. 780.

w sprawie opiniowania służbowego funkcjonariuszy Służby Kontrwywiadu Wojskowego³.

Celem opiniowania służbowego jest zweryfikowanie dalszej przydatności funkcjonariusza do służby⁴. Niewątpliwie jest to najodpowiedniejsza i najskuteczniejsza forma korygowania niewłaściwego i utrwalania pożądanego sposobu wypełniania obowiązków służbowych przez funkcjonariuszy⁵. Przyczynia się również do optymalizacji sposobu wykonywania obowiązków służbowych przez opiniowanego. Istotą opiniowania służbowego jest ustalenie celów i zasad oraz kryteriów, podmiotu i przedmiotu oraz terminów oceniania⁶.

Niewątpliwie opinia służbowa ma pewne cechy uznaniowości oraz subiektywizmu, nie może jednak nosić znamion dowolności. Opiniujący powinien dokonać wszechstronnej oceny konkretnego funkcjonariusza, z uwzględnieniem w procesie opiniowania zarówno pozytywów, jak i negatywów dotyczących opiniowanego⁷.

Instytucją mającą na celu ochronę funkcjonariusza przed nierzetelnym i stronniczym opiniowaniem służbowym jest możliwość odwołania się od otrzymanej opinii do wyższego przełożonego⁸.

Opiniowany może wnieść odwołanie od opinii, za pośrednictwem ją wydającego, w terminie 30 dni od dnia zapoznania się z nią. Możliwe jest uwzględnienie opinii przez wydającego ją i wydanie nowej. Odwołanie, które wydający opinię uzna za nieuzasadnione, przesyła w terminie 14 dni (w przypadku SWW) lub 7 dni (w przypadku SKW) od dnia jego otrzymania przełożonemu właściwemu do rozpatrzenia odwołania, wraz z opinią i pisemnym uzasadnieniem swojego stanowiska w sprawie, a także z kompletem materiałów będących podstawą wydania opinii.

- 3 Rozporządzenie Ministra Obrony Narodowej z dnia 10 lutego 2017 r. w sprawie opiniowania służbowego funkcjonariuszy Służby Kontrwywiadu Wojskowego, Dz.U. 2017, poz. 507.
- 4 B. Jaworski, *System opiniowania funkcjonariuszy służb mundurowych*, „Acta Universitatis Lodziensis” 2019, t. 87, s. 105–117.
- 5 Z. Ścibiorek, *Personel w organizacjach zhierarchizowanych*, Szczytno 2012, s. 179.
- 6 A. Pocztowski, *Zarządzanie zasobami ludzkimi. Strategie, procesy, metody*, Warszawa 2008, s. 264.
- 7 M. Domżałski, *Przyczyny obligatoryjnego rozwiązania stosunku służbowego w wybranych służbach mundurowych*, „Prawo i Polityka” 2023, t. 11, s. 41.
- 8 Wyrok NSA z dnia 1 grudnia 2016 r., I OSK 2365/15, LEX nr 2190274.

W przypadku funkcjonariuszy SKW przełożony właściwy do rozpatrzenia odwołania po zapoznaniu się ze sprawozdaniem komisji utrzymuje w mocy zaskarżoną opinię, zmienia ją bądź uzupełnia albo uchyla zaskarżoną opinię i wydaje nową. W razie braku podstaw prawnych do sporządzenia opinii służbowej opinia jest uchylana. Natomiast w przypadku funkcjonariuszy SWW przełożony właściwy do rozpatrzenia odwołania może uchylić zaskarżoną opinię służbową i poleca wydanie nowej opinii, wskazuje okoliczności, które należy wziąć pod uwagę przy jej wydawaniu, lub utrzymuje w mocy zaskarżoną opinię.

Funkcjonariusz SKW ma prawo w terminie 14 dni od dnia zawiadomienia go o nieuwzględnieniu w całości lub w części odwołania złożyć wnioszek o ponowne rozpatrzenie jego odwołania do szefa SKW. Podobnie wygląda sytuacja w przypadku funkcjonariusza SWW, z tym zastrzeżeniem, że możliwość ta istnieje wyłącznie wówczas, gdy w dwóch kolejnych opiniach służbowych, między którymi upłynęło co najmniej 6 miesięcy, stwierdzono niewywiązywanie się z obowiązków służbowych na zajmowanym stanowisku służbowym. Co istotne, rozstrzygnięcie szefów SKW bądź SWW wyczerpuje tryb rozpatrywania odwołania.

Rozstrzygnięcie wyższego przełożonego bądź szefa odpowiedniej służby nie podlega kontroli sądu administracyjnego⁹. Opinia służbowa jest aktem wydawanym w ramach podległości służbowej między przełożonym a podwładnym¹⁰. Ten zakres władzy służbowej pozostaje poza kontrolą sądową¹¹. Procedura administracyjna nie ma zastosowania do prowadzonego procesu opiniowania służbowego¹². Wydaje się, że jest trafny pogląd, że opinia służbowa nie posiada cech niezbędnych do tego, żeby konkretny akt organu był decyzją administracyjną¹³.

Z analizy rozwiązań systemowych wynika, że sądy administracyjne nie mają podstaw do merytorycznego badania zarówno trafności ocen zawartych

- 9 Uchwała NSA w składzie 7 sędziów z dnia 5 grudnia 2011 r., I OPS 3/11, LEX nr 1089623.
- 10 Wyrok NSA z dnia 10 kwietnia 2003 r., II SA 1434/02, LEX nr 142367.
- 11 Postanowienie WSA w Rzeszowie z dnia 5 listopada 2014 r., II SA/Rz 1214/14, LEX nr 1534310.
- 12 Wyrok WSA w Warszawie z dnia 12 kwietnia 2007 r., II SA/Wa 2225/06, LEX nr 338209.
- 13 Postanowienie NSA z dnia 16 grudnia 2014 r., I OSK 3114/14, LEX nr 1591024.

w opinii służbowej, jak i sposobu opiniowania¹⁴. Sprawa opiniowania nie jest sprawą administracyjną, a opinia służbowa nie ma cech rozstrzygnięcia sprawy administracyjnej ani w znaczeniu procesowym, ani materialnym¹⁵.

**Skazanie prawomocnym wyrokiem za przestępstwo,
które nie jest przestępstwem umyślnym ściganym z urzędu
(art. 19 ust. 2 pkt 2 ustawy)**

Kolejną przesłanką warunkującą fakultatywne zwolnienie ze służby jest skazanie funkcjonariusza prawomocnym wyrokiem sądu za przestępstwo, które nie jest przestępstwem ściganym z urzędu.

Niekaralność jest jednym z podstawowych kryteriów mających znaczenie podczas procedowania kandydata do służby i jest to atrybut funkcjonariusza niezbędny przez cały okres jego pozostawania w służbie. Ma to być gwarantem tego, że odpowiedzialną służbę na rzecz społeczeństwa będą pełnili wyłącznie starannie dobrani i wyselekcjonowani funkcjonariusze.

Dla zwolnienia funkcjonariusza na podstawie omawianej przesłanki bez znaczenia jest to, że w tej samej sprawie toczyło się postępowanie dyscyplinarne, niezakończony w momencie wydania decyzji w sprawie zwolnienia ze służby¹⁶.

W obecnym stanie prawnym większość przestępstw to przestępstwa publicznoskargowe, co oznacza, że ich ściganiem zajmuje się oskarżyciel publiczny (prokurator) działający w imieniu państwa¹⁷. Drugim trybem ścigania jest tryb prywatnoskargowy, który przewiduje przestępstwa z oskarżenia prywatnego (w trybie prywatnoskargowym). Z przepisów ustawy karnej musi wprost wynikać, jaki jest zakres ścigania określonego w niej przestępstwa.

Popelnienie przez funkcjonariusza przestępstwa uniemożliwia pozostawienie go w służbie ze względu na to, że podjęte przez funkcjonariusza działania godzą w społeczny wizerunek danej formacji mundurowej, przyczyniają

14 Wyrok NSA z dnia 20 grudnia 2013 r., I OSK 2732/12, LEX nr 1529035.

15 Postanowienie NSA z dnia 12 kwietnia 2013 r., I OSK 302/13, LEX nr 1320436.

16 Wyrok WSA w Bydgoszczy z dnia 18 października 2005 r., II SA/Bd 601/05, LEX nr 866193.

17 L. Gardocki, *Prawo karne*, Warszawa 1999, s. 58.

się do obniżenia zaufania społecznego do tej instytucji¹⁸. Wiąże się to zarówno z faktem samego skazania, jak i dopuszczenia się przestępstwa. Funkcjonariusze służb mundurowych, z racji ich szczególnego statusu prawnego oraz celu pełnionej służby, są zobowiązani do zachowania szczególnie wysokich standardów zawodowych i moralnych. Popełnienie przestępstwa w oczywisty sposób koliduje z tymi standardami oraz interesem społecznym.

Przeciwdziałanie negatywnym zachowaniom funkcjonariuszy ma również za zadanie budowę pozytywnego wizerunku tych służb i zapobieganie jego pogorszeniu¹⁹. Oczywiście jest, że każdy funkcjonariusz służby mundurowej powinien cechować się nienaganną postawą moralno-etyczną. Musi mieć świadomość, że niegodne zachowanie zarówno w służbie, jak i poza nią negatywnie wpływa na odbiór społeczny całej formacji, w której pełni on służbę²⁰.

Wykładnia celowościowa przepisu jednoznacznie wskazuje, że jeżeli przyczyną zwolnienia jest popełnienie przestępstwa, to nie ma znaczenia prawnego, kiedy zostało ono popełnione²¹.

Dla prawidłowości zastosowania analizowanej przesłanki bez znaczenia jest, czy rozstrzygnięcie zostało oparte na kopii wyroku czy na podstawie informacji uzyskanej z sądu. Istotne jest, że w obrocie prawnym funkcjonuje wyrok sądu, który daje podstawę do zastosowania wymienionej przesłanki zwolnienia ze służby²².

Nieobecność funkcjonariusza w służbie przez okres powyżej 3 miesięcy z powodu tymczasowego aresztowania (art. 19 ust. 2 pkt 3 ustawy)

Zgodnie z art. 258 § 1 kodeksu postępowania karnego tymczasowe aresztowanie można zastosować, jeżeli zachodzi:

- 18 Wyrok WSA w Szczecinie z dnia 1 lipca 2009 r., II SA/Sz 245/09, LEX nr 553211.
- 19 Wyrok TK z dnia 8 października 2002 r., K 36/00, LEX nr 56627; B. Opaliński, *Postępowanie dyscyplinarne funkcjonariuszy służb mundurowych w orzecznictwie Trybunału Konstytucyjnego. Zagadnienia wybrane*, [w:] *Funkcjonowanie służb mundurowych i żołnierzy zawodowych w polskim systemie prawnym. Zagadnienia wybrane*, red. B. Opaliński, P. Szustakiewicz, Warszawa 2015, s. 34.
- 20 Wyrok NSA z dnia 23 kwietnia 2014 r., I OSK 927/13, LEX nr 1480912.
- 21 Wyrok NSA z dnia 20 czerwca 2007 r., I OSK 1243/06, LEX nr 377351.
- 22 Wyrok WSA w Warszawie z dnia 12 kwietnia 2017 r., II SA/Wa 985/16, LEX nr 2296409.

1) uzasadniona obawa ucieczki lub ukrycia się oskarżonego, zwłaszcza wtedy, kiedy nie można ustalić jego tożsamości albo nie ma on w kraju stałego miejsca pobytu,

2) uzasadniona obawa, że oskarżony będzie nakłaniał do składania fałszywych zeznań lub wyjaśnień albo w inny bezprawny sposób utrudniał postępowanie karne²³.

Do przyjęcia przesłanek umożliwiających zastosowanie tymczasowego aresztowania nie jest konieczne dokonanie ustaleń, z których wynikałoby, że oskarżony z całą pewnością podejmie próbę takich działań, wystarczająca jest w tym zakresie uzasadniona obawa nastąpienia takich działań²⁴. Przykładem sytuacji uzasadniającej obawę ukrycia się oskarżonego jest nieodbieranie wezwań oraz niestawiennictwo przed organem procesowym²⁵.

Rozwiązanie stosunku służbowego ze względu na nieobecność w służbie przez okres powyżej 3 miesięcy z powodu tymczasowego aresztowania ma na celu usunięcie ze służby funkcjonariuszy, których zachowanie godzi w autorytet wykonywanej służby. Leży to zarówno w interesie SKW/SWW, jak i państwa, na którego autorytet funkcjonariusze tych formacji mogą powoływać się podczas wykonywaniu obowiązków służbowych²⁶.

Objęcie kierowniczego stanowiska państwowego albo objęcie funkcji z wyboru w organach samorządu terytorialnego (art. 19 ust. 2 pkt 4 ustawy)

Zarówno powołanie, jak i objęcie funkcji w organach samorządu terytorialnego powoduje dla funkcjonariusza powstanie nowych zadań, których wykonywanie mogłoby uniemożliwić mu należyte wykonywanie obowiązków

23 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, t.j., Dz.U. 2025, poz. 46.

24 Postanowienie SN z dnia 11 maja 2017 r., WZ 6/17, LEX nr 2309633.

25 Postanowienie SA w Katowicach z dnia 15 kwietnia 2009 r., II AKz 256/09, LEX nr 512063.

26 Wyrok WSA w Białymstoku z dnia 21 czerwca 2016 r., II SA/Bk 181/16, LEX nr 2099502.

służbowych²⁷. Taka sytuacja może być negatywnie odbierana przez społeczeństwo oraz godzi w dobre imię służby.

Katalog „kierowniczych stanowisk państwowych” zawiera art. 2 ustawy z 31 lipca 1981 roku o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe²⁸. Są to: Prezydent Rzeczypospolitej Polskiej, marszałkowie Sejmu i Senatu, Prezes Rady Ministrów, wicemarszałkowie Sejmu, Senatu, wiceprezes Rady Ministrów, prezes Najwyższej Izby Kontroli, minister, prezes Narodowego Banku Polskiego, rzecznicy: Praw Obywatelskich, Praw Dziecka, Finansowy, Małych i Średnich Przedsiębiorców, prezes Urzędu Ochrony Danych Osobowych, prezes Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, przewodniczący Krajowej Rady Radiofonii i Telewizji, wiceprezes Najwyższej Izby Kontroli, szefowie kancelarii Sejmu i Senatu, zastępcy szefów kancelarii Sejmu i Senatu, szef Kancelarii Prezesa Rady Ministrów, szefa Służby Cywilnej, Główny Inspektor Pracy, zastępca Głównego Inspektora Pracy, kierownik Krajowego Biura Wyborczego, minister stanu, szef Kancelarii Prezydenta, zastępca szefa Kancelarii Prezydenta, zastępca Prokuratora Generalnego; prezes Polskiej Akademii Nauk, sekretarz stanu, członek Państwowej Komisji do spraw wyjaśniania przypadków czynności skierowanych przeciwko wolności seksualnej i obyczajności wobec małoletniego poniżej lat 15, członek Krajowej Rady Radiofonii i Telewizji, pierwszy zastępca prezesa Narodowego Banku Polskiego, podsekretarz stanu (wiceminister), wiceprezes Narodowego Banku Polskiego, zastępcy rzecznika: Praw Obywatelskich, Praw Dziecka, Finansowego, Małych i Średnich Przedsiębiorców, zastępca prezesa Urzędu Ochrony Danych Osobowych, kierownik urzędu centralnego, wiceprezes Polskiej Akademii Nauk, wojewoda, zastępcy kierownika urzędu centralnego, wicewojewodowie.

27 E. Mazurczak-Jasińska, *Ustanie stosunku służbowego*, [w:] *System prawa administracyjnego. Stosunek służbowy*, t. 11, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2011, s. 337–338.

28 Ustawa z dnia 31 lipca 1981 r. o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe, t.j., Dz.U. 2022, poz. 1215, z późn. zm.

Zgodnie z ustawami samorządowymi organami wykonawczymi samorządu terytorialnego są: wójt (burmistrz, prezydent miasta)²⁹, zarząd powiatu³⁰ oraz zarząd województwa³¹.

Celem zakazu pełnienia określonych stanowisk jest likwidacja uwikłania funkcjonariuszy w ramach stosunków służbowych oraz zapobieżenie powstaniu stosunków podległości i odpowiedzialności wobec innego zwierzchnika. Niepołączalność mandatu przedstawicielskiego zapewnia przejrzystość podejmowania decyzji i jest wyrazem racjonalnego zarządzania zasobami ludzkimi³².

W opinii autora przepis jest wadliwie skonstruowany, gdyż umożliwia dalsze pełnienie służby w przypadku wyboru na posła lub senatora, co stoi w sprzeczności z wykładnią celowościową analizowanego przepisu.

Nabycie prawa do emerytury w pełnym wymiarze, określonego w przepisach odrębnych (art. 19 ust. 2 pkt 5 ustawy)

Zgodnie z art. 12 ust. 1 ustawy z 18 lutego 1994 roku o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin emerytura przysługuje funkcjonariuszowi, który w dniu zwolnienia ma 15 lat służby w Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, Centralnym Biurze Antykorupcyjnym, Straży Granicznej, Straży Marszałkowskiej, Służbie Ochrony Państwa, Państwowej Straży Pożarnej, Służbie Celnej, Służbie Celno-Skarbowej lub w Służbie Więziennej, z wyjątkiem funkcjonariusza, który ma ustalone

29 Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, t.j., Dz.U. 2024, poz. 1465, z późn. zm., art. 26.

30 Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym, t.j., ibidem, poz. 107, z późn. zm., art. 26.

31 Ustawa z dnia 5 czerwca 1998 o samorządzie województwa, t.j., ibidem, poz. 566, z późn. zm., art. 31, ust. 1.

32 M. Zubik, *Ustrojowe założenia niepołączalności mandatu parlamentarnego*, „Przegląd Sejmowy” 2008, nr 4, s. 107.

prawo do emerytury określonej w ustawie o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, obliczonej z uwzględnieniem okresów służby i okresów z nią równorzędnych³³. Zgodnie z art. 18 ust. 1 przywołanej ustawy o zaopatrzeniu emerytalnym kwota emerytury, bez uwzględnienia dodatków, zasiłków i świadczeń pieniężnych, o których mowa w art. 25 tejże ustawy, nie może przekroczyć 75% podstawy wymiaru.

Nabycie prawa do emerytury w pełnym wymiarze jest jedyną przesłanką, od której ustawodawca uzależnił możliwość zwolnienia funkcjonariusza na tej podstawie prawnej³⁴.

Analizowana przesłanka umożliwiająca zwolnienie funkcjonariusza ze służby ma na celu odpowiednie i optymalne prowadzenie przez szefa SKW/SWW polityki kadrowej pozwalającej na skuteczne i sprawne wykonywanie zadań postawionych przez ustawodawcę całej formacji. Specyfika służby w formacji mundurowej wymaga, żeby funkcjonariusz po stosunkowo długim okresie służby przeszedł na emeryturę, a ustawodawca może wprowadzić pewne ograniczenia, z czego powinien zdawać sobie sprawę funkcjonariusz, który decyduje się świadomie na podjęcie służby³⁵.

W tym miejscu należy zwrócić uwagę na dyrektywę Rady Unii Europejskiej 2000/78/WE z 27 listopada 2000 roku ustanawiającą ogólne warunki równego traktowania w zakresie zatrudnienia i pracy³⁶. W art. 6 ust. 1 rzeczownego dokumentu stwierdzono, że odmienne traktowanie ze względu na wiek jest dozwolone, jeżeli w ramach prawa krajowego zostanie to obiektywnie i racjonalnie uzasadnione zgodnym z przepisami celem i jeżeli środki służące osiągnięciu tego celu są właściwe i konieczne. Uznać należy, że ze względu na operacyjność SKW/SWW oraz szczególne zadania, jakie przed nimi są

- 33 Ustawa z dnia 18 lutego 1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin, t.j., Dz.U. 2024, poz. 1121.
- 34 Wyrok WSA w Warszawie z dnia 31 stycznia 2020 r., II SA/Wa 1457/19, LEX nr 3010668.
- 35 Wyrok WSA w Warszawie z dnia 16 maja 2024 r., II SA/Wa 2168/23, LEX nr 3765153.
- 36 Dyrektywa Rady Unii Europejskiej 2000/78/WE z dnia 27 listopada 2000 r. ustanawiająca ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy, Dz. Urz. UE 2000, L 303/16.

stawiane, wskazują na możliwość zwolnienia funkcjonariusza z powodu osiągniętego przez niego wieku bądź odpowiednio długiego okresu służby, i nie mają przy tym znamion dyskryminacji.

Ważny interes służby (art. 19 ust. 2 pkt 6 ustawy)

Konieczność zwolnienia funkcjonariusza ze względu na ważny interes służby może wynikać z różnych okoliczności i zdarzeń świadczących o tym, że dalsze pozostawienie go w służbie jest bezcelowe. Warto zauważyć, że brak jest konieczności powiązania tej przesłanki wyłącznie z przypadkiem naruszenia obowiązków służbowych przez funkcjonariusza. Może to być również uzasadnione każdym innym zachowaniem funkcjonariusza, które uniemożliwia kontynuowanie służby bez uszczerbku dla jej ważnych interesów³⁷. Przykładem takiego stanu faktycznego będzie np. cofnięcie posiadanego przez funkcjonariusza poświadczenia bezpieczeństwa³⁸.

Pomimo że pojęcie „ważny interes służby” jest nieostre, użycie go znajduje swoje uzasadnienie w aspekcie praktycznej działalności organu kadrowego odpowiedniej służby. Umożliwia to zastosowanie analizowanego przepisu do różnych stanów faktycznych i pozwala właściwym organom na ich odpowiednią ocenę, która w konsekwencji może zdecydować o dalszym trwaniu stosunku służbowego funkcjonariusza. Ustawodawca dostrzega potrzebę ochrony interesu społecznego będącego w tym momencie tożsamym z interesem danej formacji, daje jednocześnie możliwość oceny każdego indywidualnego przypadku przez odpowiednie organy³⁹. Istotne w odczytywaniu treści zwrotu „ważny interes służby” jest również sięgnięcie do celów i zadań SKW/SWW, które to służby są właściwe w sprawach ochrony przed zagrożeniami wewnętrznymi (SKW) i zewnętrznymi (SWW) dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej. Interes danej formacji jest nadrzędny wobec interesu funkcjonariusza, a zatem funkcjonariusz ten dla dobra macierzystej formacji, z przyczyn

37 Wyrok NSA z dnia 21 kwietnia 1999 r., II SA 426/99, LEX nr 77389.

38 Wyrok WSA w Warszawie z dnia 26 marca 2010 r., II SA/Wa 15/10, LEX nr 667168.

39 Wyrok NSA z dnia 10 lutego 2023 r., III OSK 6627/21, LEX nr 3514794.

pozamerytorycznych, nie powinien kontynuować służby⁴⁰. Oczywiście jest to, że przesłanka „ważny interes służby” powinna być w każdej indywidualnej sprawie należycie skonkretyzowana przez wskazanie okoliczności faktycznych składających się na taką ocenę.

**Likwidacja jednostki organizacyjnej SKW albo SWW
lub jej reorganizacja połączona ze zmniejszeniem obsady etatowej,
jeżeli przeniesienie funkcjonariusza odpowiednio do innej jednostki
organizacyjnej SKW albo SWW lub na niższe stanowisko służbowe
nie jest możliwe (art. 19 ust. 2 pkt 7 ustawy)**

Kolejną przesłanką zwolnienia ze służby jest likwidacja jednostki organizacyjnej SKW/SWW lub jej reorganizacja połączona ze zmniejszeniem obsady etatowej, jeżeli przeniesienie funkcjonariusza do innej jednostki lub na niższe stanowisko służbowe nie jest możliwe. Zwolnienie funkcjonariusza ze względu na likwidację jednostki organizacyjnej, w której dotychczas pełnił służbę lub jej reorganizacja, połączona ze zmniejszeniem stanów osobowych, jest możliwe wyłącznie wtedy, kiedy nie ma możliwości przeniesienia funkcjonariusza do innej jednostki organizacyjnej lub na niższe stanowisko służbowe. Niezbędna w takim przypadku jest wszechstronna analiza ewentualnego wykorzystania funkcjonariusza w innej jednostce lub na innym stanowisku. Działanie organów kadrowych musi zmierzać do znalezienia nowego stanowiska służbowego, a na organie spoczywa obowiązek zbadania wszystkich możliwości dalszego pozostania funkcjonariusza w służbie.

Ważne jest to, że organ kadrowy sam dokonuje analizy konkretnego stanowiska służbowego na podstawie posiadanych przez funkcjonariusza kwalifikacji. Bez znaczenia są przyczyny niewyznaczenia funkcjonariusza na inne stanowisko służbowe, o ile organ dokonał analizy możliwości wyznaczenia funkcjonariusza na inne stanowisko służbowe⁴¹. Analiza sytuacji kadrowej następuje w postępowaniu poprzedzającym wszczęcie procedury zwolnieniowej i jest ona wszechstronnie i dogłębnie przeprowadzona, ponieważ odpowiedni

⁴⁰ Wyrok NSA z dnia 7 marca 2019 r., I OSK 1484/17, LEX nr 2665638.

⁴¹ Wyrok WSA w Warszawie z dnia 8 sierpnia 2017 r., II SA/Wa 2181/16, LEX nr 2358574.

dobór kadr jest istotnym elementem wpływającym na poprawne wykonywanie zadań postawionych SKW/SWW⁴².

Organ nie ma obowiązku wyjaśnienia powodów braku wyznaczenia funkcjonariusza na stanowisko. Ocena przydatności funkcjonariusza do dalszej służby należy do wyłącznej kompetencji organów kadrowych⁴³. Innymi słowy, właściwe organy posiadają wyłączne uprawnienia do kształtowania – w ramach przyznanych kompetencji – polityki kadrowej, zgodnie z potrzebami danej służby⁴⁴.

W przypadku sprzeczności pomiędzy interesem SKW/SWW a indywidualnym interesem funkcjonariusza przełożeni powinni dążyć do wyważenia obu wskazanych interesów⁴⁵, jednakże w razie braku możliwości ich wyważenia słuszny interes funkcjonariusza może mieć prymat wyłącznie wtedy, kiedy równoważy on interes służbowy⁴⁶.

Upływ 12 miesięcy od dnia zaprzestania służby z powodu choroby (art. 19 ust. 2 pkt 7a ustawy)

Przesłanką umożliwiającą zwolnienie funkcjonariusza ze służby jest upływ 12 miesięcy od dnia zaprzestania służby z powodu choroby.

Przy podjęciu decyzji o zwolnieniu funkcjonariusza konieczne jest spełnienie równocześnie trzech przesłanek: zaprzestanie służby, choroba powodująca to zaprzestanie oraz upływ 12 miesięcy. Przepis wymaga koniunkcji tych trzech przesłanek, które muszą być interpretowane wąsko⁴⁷.

Do spełnienia tej przesłanki istotne jest to, że przyczyną niepodjęcia służby po okresie zwolnienia lekarskiego była choroba. Brak przedstawienia zaświadczenia lub orzeczenia potwierdzającego zdolność do wykonywania obowiązków służbowych należy traktować jako okoliczność „z powodu choroby”. Użyte sformułowanie „z powodu choroby” nie oznacza, że funkcjonariusz musi być chory. Choroba jako powód uzasadniający przesłankę upływu

42 Wyrok NSA z dnia 15 marca 2013 r., I OSK 1312/12, LEX nr 1339581.

43 Wyrok NSA z dnia 25 lutego 2009 r., I OSK 487/08, LEX nr 544926.

44 Wyrok NSA z dnia 14 listopada 2013 r., I OSK 3088/12, LEX nr 1612109.

45 Wyrok SN z dnia 18 listopada 1993 r., III ARN 49/93, OSNC 1994, nr 9, poz. 181.

46 Wyrok WSA w Warszawie z dnia 3 lutego 2017 r., II SA/Wa 1453/16, LEX nr 2253600.

47 Wyrok NSA z dnia 29 stycznia 2016 r., I OSK 1188/14, LEX nr 2032699.

12 miesięcy od dnia zaprzestania służby nie musi być potwierdzona wyłącznie zaświadczeniem lekarskim⁴⁸. Po upływie 12 miesięcy dopuszczalne jest już rozwiązywanie stosunku służbowego, i to niezależnie od tego, czy funkcjonariusz jest nadal chory czy deklaruje on chęć powrotu do służby⁴⁹.

Na gruncie orzecznictwa wskazano, że przerwanie okresu 12 miesięcy może nastąpić jedynie wówczas, gdy funkcjonariusz po zakończeniu leczenia, ale przed upływem 12 miesięcy od zaprzestania świadczenia służby z powodu choroby stawia się do służby i zostanie dopuszczony do wykonywania obowiązków służbowych⁵⁰. Gotowość do podjęcia służby w sytuacji, gdy brak jest stosownego obligatoryjnego zaświadczenia lekarskiego, że ustała przyczyna zaprzestania służby z powodu choroby, nie stanowi podstawy przerwania biegu okresu 12 miesięcy⁵¹. Bez znaczenia jest również to, że po upływie 12 miesięcy od zaprzestania służby z powodu choroby stan zdrowia pozwala mu na podjęcie służby⁵².

Na gruncie analizowanego przepisu należy wskazać, że konkretna choroba, która stała się przyczyną zaprzestania służby, trwała przez cały okres ochronny. Wystarczające jest, żeby funkcjonariusz nieprzerwanie korzystał ze zwolnienia lekarskiego w ciągu 12 miesięcy. Bez znaczenia, czy leczył się na jedną jednostkę chorobową czy w tym czasie były wydawane zwolnienia lekarskie w związku z leczeniem innych dolegliwości. Nieobecności spowodowane różnymi jednostkami chorobowymi, ale następującymi po sobie w kolejnych okresach czasu należy zsumować⁵³.

- 48 Wyrok WSA w Kielcach z dnia 25 marca 2021 r., II SA/Ke 790/20, LEX nr 3185395.
49 Wyrok WSA w Gliwicach z dnia 13 lutego 2018 r., IV SA/Gl 1040/17, LEX nr 2465000.
50 Wyrok NSA z dnia 23 maja 2019 r., I OSK 499/18, LEX nr 2730687.
51 Wyrok NSA z dnia 24 lutego 2010 r., I OSK 1188/99, LEX nr 591219.
52 Wyrok WSA we Wrocławiu z dnia 21 listopada 2019 r., IV SA/Wr 365/19, LEX nr 2757011.
53 Wyrok NSA z dnia 27 marca 2008 r., I OSK 537/07, LEX nr 494859.

Dwukrotne nieusprawiedliwione niestawienie się na badania zlecone przez komisję lekarską lub niepoddanie się im albo w przypadku dwukrotnego nieusprawiedliwionego niestawienia się na obserwację w podmiocie leczniczym w przypadku wyrażenia zgody przez funkcjonariusza, chyba że skierowanie do komisji lekarskiej nastąpiło na wniosek funkcjonariusza (art. 19 ust. 2 pkt 8 ustawy)

Funkcjonariusz jest obowiązany poddać się badaniom zleconym przez komisję lekarską, w tym również badaniom specjalistycznym, psychologicznym i dodatkowym.

Stawiennictwo na badanie przed komisją lekarską nie jest obowiązkiem który wpisywałby się w pojęcie „zajęcia służbowe”. Konieczność zbadania stanu zdrowia funkcjonariusza nie wynika z zajmowanego stanowiska służbowego. Każdy funkcjonariusz musi posiadać stan zdrowia umożliwiający mu pełnienie służby. Zwolnienie lekarskie usprawiedliwia wyłącznie nieobecność na zajęciach służbowych przewidzianych w jego zakresie obowiązków.

W skierowaniu do komisji lekarskiej organ uprawniony ustala konkretny termin i miejsce stawienia się funkcjonariusza przed właściwą komisją. W razie zaistnienia okoliczności, które uniemożliwiają stawiennictwo w ustalonym terminie, organ powinien zmienić termin wcześniej ustalony. Funkcjonariusz jest zobligowany do stawiennictwa przed komisją lekarską w terminie wskazanym w skierowaniu.

Stawienie się przed komisją rozpoczyna drugi, odrębny etap postępowania toczącego się już przed komisją i wówczas to komisja określa badania, termin ich wykonania, dokumenty, jakie należy przedłożyć itp.

Zwolnienie lekarskie obejmujące swym zakresem termin zgłoszenia się na badania przed komisją lekarską nie usprawiedliwia niestawienia się przed komisją⁵⁴. Określenie „nieusprawiedliwione” użyte w ustawie pragmatycznej dotyczy niewątpliwie także przesłanki „niepoddania się badaniom”, następującej po spójniku „lub” wyrażającym możliwość wymienną. Określenie „nieusprawiedliwione niepoddanie się badaniom” oznacza, że osoba, której to dotyczy, bez uzasadnionej przyczyny, mając świadomość ciężącego na niej obowiązku i nie podlegając żadnym znaczącym ograniczeniom – czyli ze swojej winy –

54 Wyrok WSA w Warszawie z dnia 3 czerwca 2015 r., II SA/Wa 1603/14, LEX nr 1768421.

obowiązku tego nie wykonała. Wpisanie przez lekarza w zaświadczeniu o chorobie skarżącego wskazania „chory może chodzić” nie zawsze oznacza, że w okresie nim objętym chory mógł poddać się badaniom, na które został skierowany. Należy zauważyć, że może zaistnieć sytuacja, że funkcjonariusz pomimo braku przeciwwskazań do chodzenia nie będzie mógł się stawić do wojskowej komisji lekarskiej. Taka sytuacja będzie miała miejsce w przypadku posiadania zwolnienia lekarskiego wystawionego przez lekarza psychiatrę, zalecenie bowiem nie wyklucza istnienia, usprawiedliwionych stanem zdrowia psychicznego, przeszkód w poddaniu się przez skarżącego tym badaniom. Nieusprawiedliwione niepoddanie się badaniom oznacza, że osoba, której to dotyczy, bez uzasadnionej przyczyn, mając świadomość ciężącego na niej obowiązku i nie podlegając żadnym znaczącym ograniczeniom – czyli ze swojej winy – obowiązku tego nie wykonała⁵⁵.

Nabycie obywatelstwa innego państwa (art. 19 ust. 2 pkt 9 ustawy)

Bogusław Banaszak zdefiniował obywatelstwo „jako stosunek przynależności jednostki do państwa, z którego to stosunku wynikają skutki prawne, określone w prawie wewnętrznym danego państwa, a także prawa i obowiązki wspólne wszystkim osobom mającym to obywatelstwo, chyba że pewnym ich grupom zapewniono specjalny status”⁵⁶. Z kolei Jacek Jagielski definiuje obywatelstwo jako „instytucję prawną, której istota polega na istnieniu względnie trwałego w czasie i przestrzeni węzła prawnego łączącego jednostkę z państwem i wyznaczającego jej przynależność do tego państwa, który stwarza podstawę zaistnienia kompleksu wzajemnych praw i obowiązków jednostki i państwa”⁵⁷.

Definicja obywatelstwa pojawia się na szczeblu europejskim. Artykuł 2a Europejskiej Konwencji o Obywatelstwie definiuje „obywatelstwo” jako prawną więź pomiędzy osobą a państwem i nie wskazuje na pochodzenie etniczne tej osoby. Bardziej szczegółową definicję obywatelstwa zawiera rozporządzenie (We) Nr 862/2007 Parlamentu Europejskiego i Rady z 11 lipca 2007 roku

55 Wyrok NSA z dnia 14 listopada 2007 r., I OSK 78/07, LEX nr 432939.

56 B. Banaszak, *Porównawcze prawo konstytucyjne współczesnych państw demokratycznych*, Warszawa 2007, s. 181.

57 J. Jagielski, *Obywatelstwo polskie. Komentarz do ustawy*, Warszawa 2016, s. 18–19.

w sprawie statystyk Wspólnoty z zakresu migracji i ochrony międzynarodowej oraz uchylające rozporządzenie Rady (EWG) nr 311/76 w sprawie zestawienia statystyk dotyczących pracowników cudzoziemców⁵⁸. W myśl wspomnianego rozporządzenia „obywatelstwo” oznacza szczególną więź prawną pomiędzy osobą a jej państwem, nabytą poprzez urodzenie lub naturalizację, niezależnie od tego, czy odbywa się ona poprzez deklarację, wybór, małżeństwo lub w inny sposób zgodny z prawem krajowym (art. 2 ust. 1 lit. d).

Polskie prawo dopuszcza posiadanie wielokrotnego obywatelstwa. Zgodnie z art. 3 ustawy o obywatelstwie polskim⁵⁹ obywatel polski posiadający równocześnie obywatelstwo innego państwa ma wobec Rzeczypospolitej Polskiej takie same prawa i obowiązki jak osoba posiadająca wyłącznie obywatelstwo polskie. Ponadto obywatel polski nie może wobec władz Rzeczypospolitej Polskiej powoływać się ze skutkiem prawnym na posiadane równocześnie obywatelstwo innego państwa i na wynikające z niego prawa i obowiązki.

Z ustawy wprost wynika skutek prawny w postaci braku możliwości pełnienia takiej służby przez multiobywatela. Tego typu przepisy stanowią jednocześnie *lex specialis* wobec ogólnej zasady z art. 3 ust. 1 ustawy o obywatelstwie polskim. Należy jednak podkreślić, że są to przypadki wyjątkowe, szczególnie uzasadnione ważnym interesem państwa. Znacznie częściej spotykany jest sam wymóg posiadania obywatelstwa polskiego niezależnie od obywatelstwa innego państwa, co ciekawe nawet w przypadku służby wojskowej żołnierza zawodowego⁶⁰.

Zakończenie

W przeciwieństwie do przesłanek obligatoryjnych, wystąpienie przesłanek fakultatywnych powoduje jedynie możliwość zwolnienia funkcjonariusza ze

58 Rozporządzenie (We) nr 862/2007 Parlamentu Europejskiego i Rady z dnia 11 lipca 2007 r. w sprawie statystyk Wspólnoty z zakresu migracji i ochrony międzynarodowej oraz uchylające rozporządzenie Rady (EWG) nr 311/76 w sprawie zestawienia statystyk dotyczących pracowników cudzoziemców, Dz. Urz. UE 2007, L 199/23.

59 Ustawa z dnia 2 kwietnia 2009 r. o obywatelstwie polskim, t.j., Dz.U. 2023, poz. 1989.

60 Ł. Kierznowski, *Wielokrotne obywatelstwo i pozycja multiobywatela w prawie polskim*, [w:] *Umieędzynarodowienie krajowego obrotu prawnego*, t. 1, red. M. Perkowski, W. Zoń, Białystok 2016, s. 147.

służby. Oznacza to, że zwolnienie ze służby jest pozostawione ocenie organu. Walorem ochronnym fakultatywnego zwolnienia ze służby jest to, że podlega ono uznaniu administracyjnemu. Wynika z niego, że organ decyduje o zwolnieniu ze służby, decyzja powinna być jednak odpowiednio uzasadniona. Organ powinien wszechstronnie rozważyć zarówno dobro służby, jak i słuszny interes funkcjonariusza. Stosunkowo długa lista możliwości fakultatywnego zwolnienia funkcjonariusza Służby Kontrwywiadu Wojskowego lub Służby Wywiadu Wojskowego ze służby uzasadnia szczególną rolę tych służb w kształtowaniu bezpieczeństwa wewnętrznego i zewnętrznego państwa.

Bibliografia

- Banaszak B., *Porównawcze prawo konstytucyjne współczesnych państw demokratycznych*, Warszawa 2007.
- Domżałski M., *Przyczyny obligatoryjnego rozwiązania stosunku służbowego w wybranych służbach mundurowych*, „Prawo i Polityka” 2023, t. 11.
- Gardocki L., *Prawo karne*, Warszawa 1999.
- Jagielski J., *Obywatelstwo polskie. Komentarz do ustawy*, Warszawa 2016.
- Jaworski B., *System opiniowania funkcjonariuszy służb mundurowych*, „Acta Universitatis Lodzianensis” 2019, t. 87.
- Kierznowski Ł., *Wielokrotne obywatelstwo i pozycja multiobywatela w prawie polskim*, [w:] *Umiędzynarodowienie krajowego obrotu prawnego*, t. 1, red. M. Perkowski, W. Zoń, Białystok 2016.
- Mazurczak-Jasińska E., *Ustanie stosunku służbowego*, [w:] *System prawa administracyjnego. Stosunek służbowy*, t. 11, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2011.
- Opaliński B., *Postępowanie dyscyplinarne funkcjonariuszy służb mundurowych w orzecznictwie Trybunału Konstytucyjnego. Zagadnienia wybrane*, [w:] *Funkcjonowanie służb mundurowych i żołnierzy zawodowych w polskim systemie prawnym. Zagadnienia wybrane*, red. Opaliński B., Szustakiewicz P., Warszawa 2015.
- Pocztowski A., *Zarządzanie zasobami ludzkimi. Strategie, procesy, metody*, Warszawa 2008.
- Ścibiorek Z., *Personel w organizacjach zhierarchizowanych*, Szczytno 2012.
- Zubik M., *Ustrojowe założenia niepołączalności mandatu parlamentarnego*, „Przegląd Sejmowy” 2008, nr 4.

Optional Exemption from Service of Officers of the Military Counterintelligence Service and the Military Intelligence Service

Abstract

The legislator established the Military Counterintelligence Service as a special service responsible for matters of protection against internal threats to the state's defence, security, and combat capability of the Armed Forces of the Republic of Poland and other organisational units subordinate to or supervised by the Minister of National Defence. The Military Intelligence Service, in turn, was established as a special service responsible for matters of protection against external threats to the state's defence, security and combat capability of the Armed Forces of the Republic of Poland and other organizational units subordinate to or supervised by the Minister of National Defence. Due to the fact that the tasks of both of these services are of great importance for the country's defence, the status of officers of these services is also important, and in particular the stability of the service.

Keywords

uniformed services, dismissal, service relationship

Dariusz Andrzej Magierek

Wydział Humanistyczny

Politechniki Koszalińskiej

ORCID: 0000-0002-7835-3282

e-mail: dariusz.magierek@tu.koszalin.pl

Ciągłość działania w przedsiębiorstwie z punktu widzenia bezpieczeństwa

Streszczenie

Ze względu na szybko zmieniające się otoczenie przedsiębiorstwa przykładają coraz większą uwagę do zarządzania ciągłością działania. Wiele mówi się o zagrożeniu współczesnego świata, jakim jest uzależnienie od technologii, które powoduje, że ciągłość działania staje się podstawowym czynnikiem sukcesu wielu organizacji. Świadome przedsiębiorstwa zabezpieczają się na różne sposoby, żeby nie stracić zaufania klientów, nie stracić przychodów, a także zapobiec utracie ewentualnych korzyści.

Autor podjął problematykę właściwego działania przedsiębiorstwa z punktu widzenia jego bezpieczeństwa. W związku z tym ważne jest zarządzanie ciągłością jego działania, co przekłada się bezpośrednio na bezpieczeństwo przedsiębiorstwa.

Słowa kluczowe

przedsiębiorstwo, bezpieczeństwo, zarządzanie

Wstęp

Ze względu na zapewnienie przedsiębiorstwu bezpieczeństwa jest tworzona analiza ryzyka, również operacyjnego, a na jej podstawie opracowuje się procedury i plany awaryjne, które mają uchronić przedsiębiorstwo na wypadek incydentów, kryzysów czy katastrof. Czy w tych planach jest miejsce dla marketingu? Głównym celem badawczym niniejszego artykułu jest zbadanie czy ciągłość działania organizacji wpływa na bezpieczeństwo przedsiębiorstwa? W związku z powyższym

zostaną przedstawione pojęcia „bezpieczeństwo przedsiębiorstwa” i „ciągłość działania”, a także jak zarządza się nią w organizacji oraz jakich narzędzi można do tego użyć. Ponadto zostanie omówiona istota analizy ryzyka w przedsiębiorstwie, procedury oraz plany awaryjne tworzone w celu zapewnienia ciągłości działania w przedsiębiorstwie, a także standardy, które muszą spełniać plany ciągłości działania, oraz korzyści z przygotowania i odpowiedniego zabezpieczenia się w celu utrzymania ciągłości działania w zmieniającym się środowisku.

Pojęcie bezpieczeństwa przedsiębiorstwa

Współcześnie biznes jest coraz bardziej wymagający, a warunki do jego prowadzenia coraz bardziej zmienne. Zaczynając od małych przedsiębiorstw, a kończąc na dużych korporacjach, bez względu na branżę czy klienta, coraz większe wyzwania stoją przed firmami i ich prowadzącymi. Ostatnie lata pokazują jak bardzo elastyczne powinno być przedsiębiorstwo, żeby dostosować się do zmiennego środowiska i warunków.

Organizacje określają swoje misje i cele strategiczne w każdym z obszarów działalności¹. Na drodze do osiągnięcia celu istnieje ryzyko napotkania pewnych barier mających wszelakie podłoże. Mogą to być bariery zarówno ekonomiczne, jak i komunikacyjne czy informacyjne².

Poziom osiągnięcia tych celów jest uzależniony od odpowiedniego planu i zabezpieczenia się przed ryzykiem, które organizacja może napotkać. Skuteczność tego planu jest zdeterminowana odpowiednim podejściem i jego dobrym przygotowaniem, a także zachowaniem odpowiednich procedur bezpieczeństwa³.

Współcześnie obserwuję się, że bardzo wzrosła świadomość ryzyka, możliwości jego pojawienia się i zakłócenia poprawnego funkcjonowania firmy⁴. Organizacje zabezpieczają się na wiele sposobów, żeby utrzymać ciągłość działania przedsiębiorstwa, utrzymać jego zasoby i procesy na wypadek pojawienia się zewnętrznych bądź wewnętrznych zakłóceń.

1 H Bieniok i in., *Metody sprawnego zarządzania*, Warszawa 2004 s. 50.

2 *Marketing przedsiębiorstw przemysłowych*, red. W. Mantura, Poznań 2000, s. 12.

3 P. Zaskórski, *Informacyjno-biznesowa ciągłość działania firmy*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki” 2011, nr 5, s. 218.

4 J. Zawila-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*, Kraków–Warszawa 2013, s. 14.

Ostatnie dziesięciolecie cechuje rosnąca zmienność i złożoność warunków działania podmiotów gospodarczych, co powoduje, że nieustannie poszukuje się sposobów minimalizacji ryzyka towarzyszącego podejmowanym decyzjom, zwłaszcza strategicznym. Dlatego tak ważne jest, żeby wszelkie procesy w przedsiębiorstwie były poprawnie zabezpieczone i w kryzysowym dla firmy momencie pomogły jej przetrwać bez zakłóceń, a co za tym idzie, pomogły jej utrzymać ciągłość biznesową. Bezpieczeństwo w przedsiębiorstwie jest ściśle powiązane z ryzykiem i ciągłością działania. W organizacji biznesowej możemy wyróżnić następujące rodzaje bezpieczeństwa:

- środowiskowe,
- procesowe,
- pracy,
- osobowe,
- informacji,
- informatyczne,
- fizyczne,
- techniczne⁵.

Ponadto ze względu na aspekty związane z bezpieczeństwem wyróżniamy:

- zarządzanie w kryzysie,
- ochronę wartości materialnych i niematerialnych,
- ciągłość działania,
- ryzyko zawodowe⁶.

Zabezpieczenie wyżej wymienionych obszarów pozwala zapewnić funkcjonowanie przedsiębiorstwa. Szczególną ochroną można objąć całą organizację bądź poszczególną jednostkę (np. jeden z działów). Bezpieczeństwo jest ważne także w kontekście współpracy z jednostkami zewnętrznymi takimi jak firmy outsourcingowe. Tutaj firma również powinna mieć obraną strategię na wypadek wystąpienia zakłóceń lub zagrożeń, które mogą wpłynąć na kontynuację biznesu. W kontekście zarządzania ryzykiem termin „bezpieczeństwo” to określony stan rzeczywistości społecznej oraz podmiotowej. Jest także dobrem społecznym w aspekcie wartości humanistycznych, praw człowieka czy potrzeb ludzkich⁷.

5 *Ryzyko operacyjne w naukach o zarządzaniu*, red. nauk. I. Staniec, J. Zawila-Niedźwiecki, Warszawa 2015, s. 119.

6 Ph. Kotler, G. Armstrong, J. Saunders, V. Wong, *Marketing. Podręcznik europejski*, Warszawa 2002, s. 45.

7 E. Michalski, *Marketing*, Warszawa 2004, s. 187–189.

Zgodnie z klasycznymi badaniami Maslowa poczucie bezpieczeństwa jest drugą z podstawowych potrzeb człowieka. Samo zapewnienie przedsiębiorstwu bezpieczeństwa jest także działaniem prewencyjnym, ponieważ polega na rozwiązaniach, których głównym celem jest zapobieganie pojawieniu się sytuacji krytycznej poprzez dostrzeżenie czynników zagrożenia, a także wczesne monitorowanie charakterystycznych symptomów wskazujących na możliwość pojawienia się zagrożenia dla działalności. Jeżeli te kroki zawiodą i dojdzie do zakłóceń działalności organizacji, to wtedy przychodzi pora na zaplanowaną i zorganizowaną aktywność naprawczą, której zadaniem jest zapewnić akceptowalną zdolność do utrzymywania ciągłości działania⁸.

Istotnym zagadnieniem jest także kwestia zapewnienia bezpieczeństwa zasobów organizacji. Jeżeli tych zasobów brak bądź można zaobserwować ich niedostatek, to tworzy również zagrożenie. Zachowanie zasobów organizacji na odpowiednim poziomie to przejaw zapewnienia efektywnego bezpieczeństwa⁹, które jest kojarzone z rodzajem zasobu, co znajduje swoje odzwierciedlenie w organizacji i możemy podzielić je na dwie kategorie, tj. ochronę fizyczną, techniczną i bezpieczeństwo osobowe, a także bezpieczeństwo informacji i systemów informatycznych oraz zapewnienie ciągłości działania.

Zamiast sformułowania „zarządzanie ryzykiem operacyjnym” możemy też spotkać określenie „zarządzanie zapewnianiem bezpieczeństwa operacyjnego”, w pełnym ujęciu jako zintegrowane zarządzanie zapewnianiem bezpieczeństwa” (TSM – total security management)¹⁰.

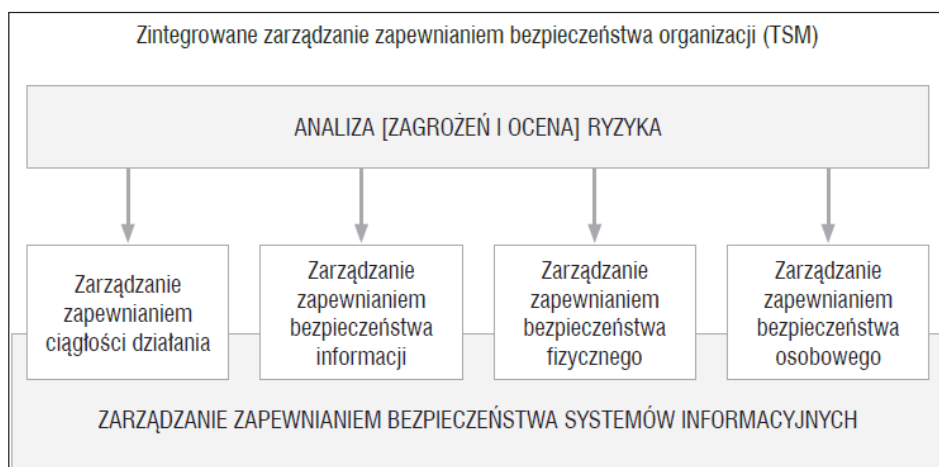
Każdy z obszarów TSM ma swoje zasady, dobre praktyki i odpowiednie metody mające na celu zapewnienie bezpieczeństwa organizacji (schemat 1). Wyróżnienie kwestii bezpieczeństwa systemów informacyjnych zostało pokazane po to, żeby podkreślić obecność informacji w zarządzaniu oraz informatyki w działalności organizacji. Pominięcie w TSM ryzyka związanego z niedoborem zasobów finansowych jest powiązane z zarządzaniem ryzykiem biznesowym i ryzykiem finansowym oraz z tym, że jest ono rozwiązywane w ramach zarządzania tymi rodzajami ryzyka¹¹.

8 Ibidem, s. 85.

9 Ibidem, s. 84.

10 J. Zawila-Niedźwiecki, op. cit., s. 84.

11 Ibidem



Źródło: M. Blim, M. Byczkowski, J. Zawila-Niedźwiecki, *Zintegrowane zarządzanie bezpieczeństwem organizacji*, [w:] *Systemy informatyczne. Bankowość i finanse*, red. F. Marecki, J.K. Grabara, J. Nowak, Warszawa 2005, s. 12.

Schemat 1. Konceptcja zintegrowanego zarządzania bezpieczeństwem

Zapewnianie bezpieczeństwa organizacji, zwłaszcza w ujęciu TSM, jest odnoszone do poszczególnych rodzajów zasobów¹². Jak już zostało wspomniane, wyróżniamy bezpieczeństwa: osobowe, fizyczne i techniczne, finansowe oraz informacji i informatyczne. Zapewnianie bezpieczeństwa fizycznego i technicznego wywodzi się z następujących podstawowych przesłanek:

- potrzeby precyzyjnego zakreszenia granic lokalizacji organizacji oraz stref wykonywania poszczególnych funkcji i usług na rzecz klientów, a także przez pracowników organizacji oraz na ich rzecz,
- potrzeby wyobrażenia sobie i zdefiniowania potencjalnych zagrożeń oraz możliwych scenariuszy ich realizowania się jako zakłóceń normalnej pracy organizacji,
- potrzeby zorganizowania procesów wykonywania funkcji organizacji, zapewniania ochrony fizycznej oraz dobierania i stosowania rozwiązań ochronnych, w tym także technicznych¹³.

Z kolei zapewnianie bezpieczeństwa osobowego wynika z następujących głównych przesłanek:

¹² M. Blim, M. Byczkowski, J. Zawila-Niedźwiecki, op. cit., s. 12.

¹³ *Ryzyko operacyjne w naukach...*, s. 22.

- potrzeby doboru i zatrudniania pracowników odznaczających się wysokim poziomem morale i odpowiedzialności (tzw. reguła prawości),
- wymogu adekwatności umiejętności zawodowych pracowników do wykonywanych zadań oraz potencjalnej zdolności do adaptowania się do zmieniających się wymagań, co może być pochodną rozwoju organizacyjnego i biznesowego podmiotu lub konkurencyjnego rozwoju rynku (tzw. reguła fachowości),
- potrzeby doboru pracowników oraz organizacji pracy, które z dwu stron współprzyczyniają się do stworzenia atmosfery i warunków do identyfikacji powodzenia zawodowego¹⁴.

Jeżeli chodzi o bezpieczeństwo informacji, to wywodzi się z następujących podstawowych przesłanek:

- zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. reguła poufności),
- zapewnienia zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania (tzw. reguła integralności),
- zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. reguła dostępności)¹⁵.

Określa się trzy poziomy merytorycznego zarządzania bezpieczeństwem informacji:

- polityka bezpieczeństwa informacji – określenie wymagań bezpieczeństwa na poziomie całej organizacji i w odniesieniu do wszystkich grup informacji oraz wszystkich systemów i rozwiązań służących przetwarzaniu tych informacji (w tym przechowywaniu i transportowaniu),
- grupa informacji – uszczegółowienie wymagań bezpieczeństwa dla grup informacji, wyodrębnianych przede wszystkim jako autonomiczna klasa informacji służących określonym zagadnieniom, przetwarzanych w określonym pionie funkcjonalnym (np. informacje finansowe, informacje kadrowe, informacje o klientach itd.), ale także niekiedy objętych odrębnymi przepisami prawa ogólnego, np. informacje niejawne, informacje o danych osobowych,
- system przetwarzania – spełnienie wymagań bezpieczeństwa przez systemy także tradycyjne, ale przeważnie informatyczne, które przetwarzają określone grupy informacji na rzecz pewnej kategorii użytkowników¹⁶.

14 Ibidem.

15 K. Lidermann, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017, s. 12.

16 M. Rydel, *Komunikacja jako element marketingu*, [w:] *Komunikacja marketingowa*, red. idem, Gdańsk 2001, s. 21.

Jeżeli mowa o bezpieczeństwie informacji, to warto wspomnieć o zaproponowanym przez Stowarzyszenie Audytorów Informatycznych (Information Security Audit and Control Association – ISACA¹⁷) modelu, który pokazuje poziomy dojrzałości zarządzania bezpieczeństwem informacji (schemat 2). Zarządzanie zapewnianiem bezpieczeństwa przedsiębiorstwa jest prowadzone w zależności od obszaru, którego dotyczy¹⁸.

Stopień 0 Brak świadomości	<ul style="list-style-type: none"> – brak zdefiniowania wymagań bezpieczeństwa – bezpieczeństwo traktowane jako problem poszczególnych użytkowników
Stopień I Początkowy	<ul style="list-style-type: none"> – świadomość potrzeby – kierownictwo uważa to za problem służb IT (typu: prawa dostępu, ochrona antywirusowa)
Stopień II Intuicyjny	<ul style="list-style-type: none"> – próby tworzenia zabezpieczeń – brak jednolitego podejścia – efekty zależne od zaangażowania osób zainteresowanych
Stopień III Zdefiniowany	<ul style="list-style-type: none"> – zdefiniowane zasady (w tym polityka bezpieczeństwa) w całej organizacji – procedury bezpieczeństwa są utrzymywane i komunikowane – brak kontroli stosowania
Stopień IV Zarządzany	<ul style="list-style-type: none"> – jednolite podejście dla wszystkich komórek i wszystkich rozwiązań – obowiązuje perspektywa biznesu – funkcjonuje mechanizm kontroli stosowania
Stopień V Optymalizowany	<ul style="list-style-type: none"> – świadome zarządzanie ryzykiem – zgodność strategii bezpieczeństwa ze strategią biznesową – zapewnianie bezpieczeństwa jako proces (wiedza, doskonalenie)

Źródło: M. Forystek, *Audyty informacyjne*, Zgierz 2005, s. 23.

Schemat 2. Poziomy dojrzałości zarządzania bezpieczeństwem informacji

17 Zob. <https://engage.isaca.org/warsawchapter/home> [dostęp: 3.02.2025].

18 J. Zawila-Niedźwiecki, op. cit., s. 92.

W zależności od stopnia dojrzałości organizacji zmienia się podejście do bezpieczeństwa, a także sposób zarządzania ryzykiem. Odpowiada za nie każda jednostka w firmie, ponieważ każda z nich może stworzyć potencjalne zagrożenie. Dlatego tak ważna jest ochrona danych w różnych działach zarówno IT, jak i zasobów ludzkich, który dysponuje informacjami o pracownikach czy działu obsługi klienta mającego dane klientów. Wszystkie te obszary w firmie powinny być zabezpieczone¹⁹. Ważna jest również świadomość użytkowników, którzy je przetwarzają.

Zarządzenie ciągłości działania jako podstawowe narzędzie w procesie zapewnienia bezpieczeństwa przedsiębiorstwa

Negatywne zjawiska, kryzysy czy nieprzewidziane zdarzenia wpływają na ludzkie postawy²⁰. Pod koniec XX wieku powstała dyscyplina zwana „zarządzanie ryzykiem”. Jednocześnie menadżerowie zaczęli zastanawiać się jak utrzymywać ciągłość działania przedsiębiorstwa, którym zarządzają? Chyba zarządzają²¹. Współcześnie coraz bardziej rozwija się pojęcie kontroli jakości w firmie, co ma bardzo istotny wpływ na ciągłość działania zarówno dużych spółek, jak i małych podmiotów gospodarczych²².

Ciągłość działania oznacza zdolność funkcjonowania w sytuacji wystąpienia np.: klęsk żywiołowych, nieszczęśliwych wypadków, aktów sabotażu, ataków terrorystycznych lub poważnych awarii najważniejszych maszyn i urządzeń produkcyjnych²³. Trzeba podkreślić, że problematyka zapewniania ciągłości jest dość trudna do wyodrębnienia z elementów, które składają się na zarządzanie ryzykiem oraz zapewnianie bezpieczeństwa w firmie²⁴. Wzorcem w systematycznym podejściu do zapewniania ciągłości działania jest koncepcja Business Continuity Management (BCM), którą Business Continuity Institute²⁵ zdefiniował jako holistyczny proces zarządzania, który ma na

19 A. Sznajder, *Marketing. Encyklopedia biznesu*, t. 1, Warszawa 1995, s. 475.

20 T.T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania*, Warszawa 2009, s. 146.

21 Ibidem, s. 23.

22 Ibidem, s. 43.

23 Ibidem, s. 44.

24 J. Zawila-Niedźwiecki, op. cit., s. 140.

25 Zob. www.thebci.org [dostęp: 15.02.2025].

celu określenie potencjalnego wpływu zakłóceń na organizację i stworzenie warunków budowania odporności na nie oraz zdolności skutecznej reakcji w zakresie ochrony kluczowych interesów właścicieli, reputacji i marki organizacji, a także wartości osiągniętych w jej dotychczasowej działalności²⁶.

Do powyższej definicji odwołują się również normy ISO 22301, BS 25777 i BS 25999, które rekomendują spiralny cykl procesu zarządzania zapewnianiem ciągłości działania (schemat 3). W tym miejscu warto wspomnieć również o holistycznym procesie zapewniania ciągłości działania zaproponowanym również przez Business Continuity Institute (schemat 4), która identyfikuje potencjalne zagrożenia organizacji wraz ze skutkami, tych zagrożeń dla biznesu. Żeby dobrze zrozumieć cały ten proces, należy zacząć od cyklu życia zarządzania ciągłością działania, która przedstawia się następująco:

- 1) zrozumienie organizacji,
- 2) określenie strategii,
- 3) opracowanie i wdrożenie reakcji,
- 4) ćwiczenia, utrzymanie i przegląd²⁷.

Wszystkie te zadania, wykonywane w odpowiedniej kolejności, pomagają w zarządzaniu przedsiębiorstwem w razie wystąpienia sytuacji mogących zakłócić ciągłość funkcjonowania firmy²⁸.

Żeby zachować ciągłość funkcjonowanie przedsiębiorstwa, należy je na taką okoliczność przygotować. Zgodnie z przeprowadzonymi badaniami przez Janusza Zawilą-Niedźwieckiego, autora książki o zarządzaniu ryzykiem operacyjnym, możemy wyróżnić pięć podstawowych czynności składających się na plan przygotowań przedsiębiorstwa na wypadek wystąpienia sytuacji kryzysowej²⁹:

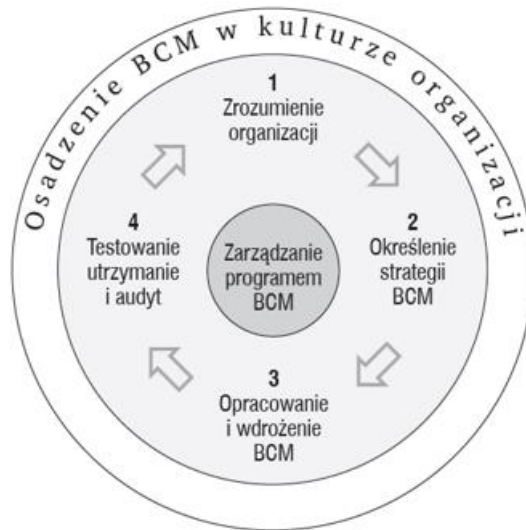
- 1) ustalenie, co jest krytyczne dla organizacji, jakie zasoby i procesy mogłyby zostać zagrożone i w jakiej sytuacji,
- 2) określenie, w jaki sposób organizacja będzie osiągać cel, jak spełni biznesowe wymagania związane z zapewnieniem ciągłości, w jakiej kolejności oraz w jaki sposób,

26 P. Waniowski, D. Sobotkiewicz, M. Daszkiewicz, *Marketing – teoria i przykłady*, Warszawa, 2010, s. 34.

27 BS 25999-2: Business Continuity Management – Specification, London 2007, s. 3.

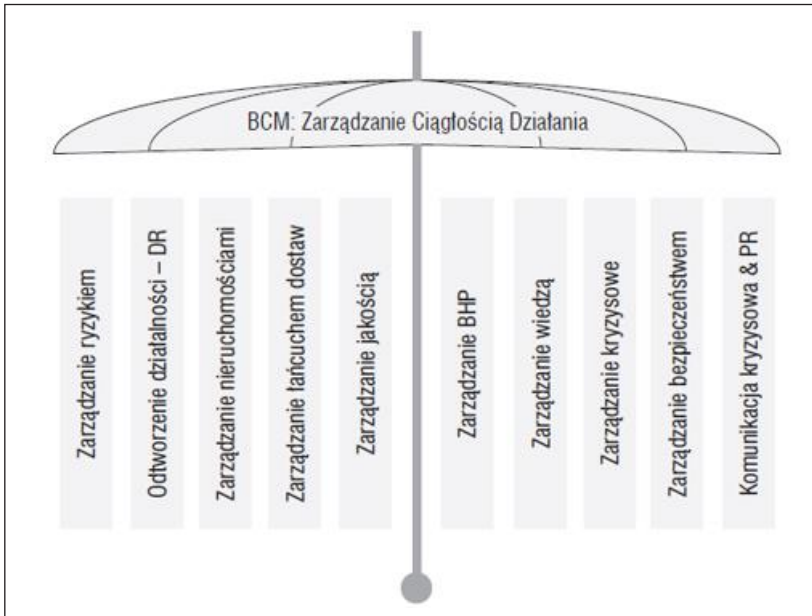
28 P. Waniowski, D. Sobotkiewicz, M. Daszkiewicz, op. cit., s. 35.

29 J.L. Lambin, *Strategiczne zarządzanie marketingowe*, Warszawa 2001, s. 21–22.



Źródło: Norma BS 25999: Business Continuity Management – Specification, London 2007.

Schemat 3. Modelowy cykl zarządzania zapewnianiem ciągłości działania (BCM)



Źródło: Business Continuity Institute, <https://www.thebci.org> [dostęp: 15.02.2025].

Schemat 4. Holistyczny proces zarządzania zapewnianiem ciągłości działania

3) stworzenie rozwiązań, które zapewnią ciągłość i będą ściśle powiązane z charakterem organizacji,

4) implementacja tych rozwiązań, przeprowadzenie testów zazwyczaj w warunkach symulowanych, co pomaga przyszykować się do sprostania zagrożeniu w sytuacji rzeczywistej,

5) założenie, że problematyka dotyczy wszystkich pracowników, dlatego każdy z nich powinien znać rozwiązania odnośnie do jego obszaru i stanowiska. Powinien również aktywnie uczestniczyć w ich opracowaniu³⁰.

Zakłócenia są obiektem działań określanymi jako powszechnie rozumiana polityka zapewniania ciągłości działania. Wobec tego można stwierdzić, że postępowanie, które służy zapewnianiu ciągłości działania, jest podobne do postępowania mającego na celu zabezpieczenie przed zagrożeniami. Różni je jedynie czas i charakter oddziaływania na zagrożenia. Obydwa uzupełniają się tak, żeby zapewnić przedsiębiorstwu oczekiwaną odporność na czynniki zewnętrzne, które mogą zakłócić codzienną działalność³¹.

Podstawowe obszary zapewniania ciągłości działania to:

- mechanizm reagowania organizacji na zakłócenia,
- proces rozwijania ww. mechanizmu zdolności reagowania na zakłócenia,
- proces zarządzania bieżącą zdolnością zapewniania ciągłości działania

oraz jej stałym doskonaleniem.

Z kolei na reagowanie na zakłócenia składają się:

- struktura organizacyjna odpowiednia do zadania zapewniania ciągłości, uzupełniająca ogólną strukturę organizacyjną,
- formalne uregulowania określające relacje w strukturze organizacyjnej związane z zadaniem zapewniania ciągłości,
- utrwalona praktyka postępowania w sytuacjach, gdy wymagana jest reakcja na zaistniałe zakłócenie³².

Należy zaznaczyć, że reagowanie na zakłócenia, jako zapewnianie ciągłości działania, trzeba rozumieć nie tylko jako bezpośrednie postępowanie wobec występujących zakłóceń, lecz także jako aktywność o charakterze prewencyjnym, związaną z analizą ryzyka, zagrożeń i podatności oraz z poszukiwaniem

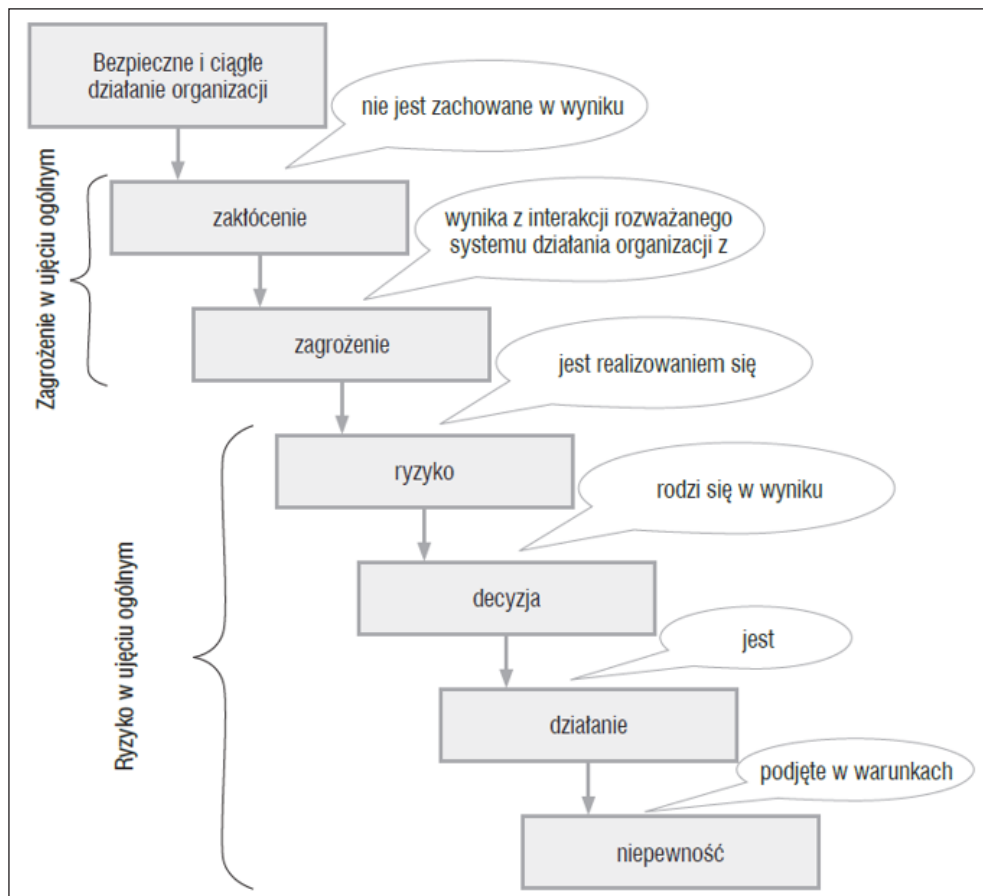
³⁰ J. Zawila-Niedźwiecki, op. cit., s. 166.

³¹ Ibidem, s. 92.

³² J.L. Lambin, op. cit., s. 32.

metod i rozwiązań zapobiegania powstaniu zakłóceń. W tym znaczeniu starania o ciągłość działania i bezpieczeństwo się splatają³³.

Z punktu widzenia ciągłości działania rozwiązania bezpieczeństwa zapewniają prewencję wobec zagrożeń, natomiast z punktu widzenia bezpieczeństwa rozwiązania ciągłości działania stanowią dodatkowe zabezpieczenie wówczas, gdy zawiodą nominalne rozwiązania bezpieczeństwa³⁴ (schemat 5).



Źródło: J. Zawila-Niedźwiecki, op. cit., s. 121.

Schemat 5. Mechanizm logiczny naruszenia poprawnego działania organizacji

33 Ibidem, s. 97.

34 J. Zawila-Niedźwiecki, op. cit., s. 96–97.

W związku z tym, jeżeli mowa o ciągłości działania, to mamy na myśli stan odporności organizacji na zakłócenie, jeżeli mowa o zapewnieniu ciągłości działania, to chodzi o ciąg planowanych działań, które zmierzają do usuwania zakłóceń, a gdy mowa o zarządzaniu zapewnianiem ciągłości działania, wówczas jest to proces polegający na określaniu zadań, przygotowaniu planu i monitorowaniu rozwiązań mających na celu zapewnienie ciągłości.

Kiedy mowa o ciągłości działania jako narzędziu biorącym udział w zabezpieczeniu przedsiębiorstwa, nie można pominąć również kwestii ryzyka. W zależności od przedziału czasowego możemy wyróżnić różne dyscypliny zajmujące się naturą ryzyka, bezpieczeństwem i ciągłością działania.

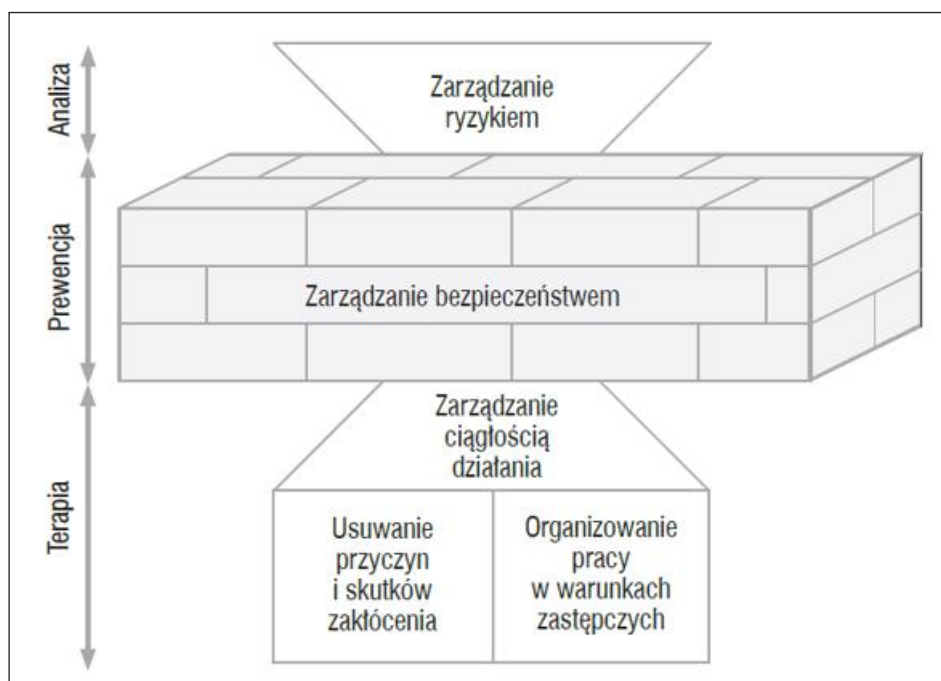
Kiedy mówimy o czasie odległym, wtedy będzie to kwestia z dziedziny ekonomii, ponieważ mamy na myśli odległe skutki i przyczyny (wzrost i rozwój). Gdy przyjmiemy perspektywę bliską czasowo, wówczas jest to kwestia z zakresu nauk o zarządzaniu, ponieważ ryzyko operacyjne jest traktowane jako ryzyko niewystarczającej skuteczności działania z punktu widzenia celu bieżącego tego działania. Tym samym w tym ujęciu ryzyko polega na możliwości niespełnienia wymogów czy oczekiwań³⁵.

Konsekwencją tego jest zabezpieczenie się i przygotowanie odpowiednich rozwiązań, dlatego pojawia się synergiczny związek ciągłości działań i bezpieczeństwa. Wszelkie działania na rzecz bezpieczeństwa mają charakter prewencyjny. Kiedy ochrona okazuje się nieskuteczna, wtedy rozwiązania ciągłości działania będą reakcją naprawczą (schemat 6)³⁶.

Triada: ryzyko – bezpieczeństwo – ciągłość oznacza zatem panowanie nad ryzykiem polegające na racjonalnym rozłożeniu akcentów między prewencję wobec zagrożeń dla działania organizacji a zaprojektowane reagowanie na występowanie zakłóceń.

³⁵ J. Zawila-Niedźwiecki, op. cit., s. 55.

³⁶ Ibidem, s. 56.



Źródło: J. Zawila-Niedźwiecki, op. cit., s. 121.

Schemat 6. Relacje zadań zapewnienia bezpieczeństwa i ciągłości działania

Analiza ryzyka w przedsiębiorstwie

Analiza ryzyka ma na celu rozpoznać procesy i działy w firmie, które są najbardziej narażone na nieprzewidziane negatywne sytuacje. Pokazuje stopień odporności przedsiębiorstwa na sytuacje trudne do przewidzenia i groźne dla firmy³⁷. Istnieje wiele rodzajów analiz, które mogą pomóc osobom zarządzającym w firmie dobrze przygotować odpowiednie procesy i zapobiec przerwaniu funkcjonowania firmy³⁸.

Jedną z najbardziej popularnych analiz jest Business Impact Analysis (BIA), która pozwala zdefiniować oraz sklasyfikować wszystkie nieprawidłowości. Dzięki tej analizie można określić działania o charakterze operacyjnym i strategicznym. Ważnym atutem BIA jest możliwość określenia czasu

37 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 58.

38 S. Zapłata, M. Kaźmierczak, *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Warszawa 2011, s. 153.

wystąpienia zagrożenia, a także zakresu jego oddziaływania na poszczególne podsystemy w firmie³⁹. Dzięki niej można pozyskać informacje dotyczące procesów, zasobów i ludzi⁴⁰.

Pierwszym krokiem BIA jest poznanie rzeczywistej sytuacji firmy, gdy analiza dostarczy już wystarczającą ilość szczegółowych danych. Na ich podstawie zostaje wdrożona odpowiednia strategia i zostają podjęte odpowiednie działania. Dzięki tej analizie możemy także oszacować czas występowania sytuacji niepożądanego i zakres jej oddziaływania na poszczególne działy organizacji⁴¹. Celem ostatecznym BIA jest wskazanie krytycznych z punktu widzenia prowadzonego biznesu i niekrytycznych zdarzeń i sytuacji, z którymi spotyka się firma⁴². W zdarzeniach zaliczanych jako krytyczne możemy wyróżnić dwie zmienne:

- RPO (Recovery Point Objective) – określa minimalną ilość zasobów, które przedsiębiorstwo musi odzyskać w danym przedziale czasowym,
- RTO (Recovery Time Objective) – określa maksymalny czas przeznaczony na odbudowę najważniejszych procesów czy też na odzyskanie zasobów w firmie.

Taką analizę należy przeprowadzić nie tylko w przypadku zdarzeń nieprzewidzianych, np. klęska żywiołowa, ale warto ją wdrożyć również przed podjęciem codziennych działań biznesowych takich, jak np.:

- wprowadzanie nowego produktu,
- zmiana strategii bądź struktury organizacyjnej,
- zmiana głównego dostawcy lub firm podwykonawczych,
- wdrożenie nowej technologii.

Wyniki z analizy BIA pomagają ocenić ewentualne straty finansowe spowodowane kryzysowym zdarzeniem i odnaleźć słabe elementy w organizacji (Single Point of Failure – SPOF).

Analiza istniejącej sytuacji (analiza luki – Gap Analysis) pomaga organizacjom określić jak najlepiej osiągać swoje cele biznesowe. W tej analizie należy zacząć od stanu faktycznego, zazwyczaj sytuacji wyjściowej znacznie

39 https://www-arch.polsl.pl/wydzialy/ROZ/ZN/Documents/z97/38_po_rec_056_Sta-rosta.pdf [dostęp: 9.06.2024].

40 J.L. Lambin, op. cit., s. 45.

41 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 57.

42 Ibidem, s. 56.

odbiegającej od docelowej⁴³. Kolejnym etapem będzie szukanie obszarów niespełniających wymagań, w których zauważymy luki. Następnie, po zaangażowaniu jak największej liczby osób, wspólnie jest opracowywany plan, który trzeba wdrożyć, żeby zapełnić dotychczasowe luki.

Uzyskane informacje będą bardzo potrzebne do kolejnej analizy, tj. analizy SWOT⁴⁴. To analiza popularna i często używana w organizacjach. Polega ona na określeniu mocnych i słabych stron oraz możliwości i zagrożeń. Podczas opracowywania strategii należy również uwzględnić czynniki zewnętrzne. Po przepracowaniu analizy możemy znaleźć w wynikach słabe punkty i zagrożenia, które mogą mieć wpływ na ciągłość zarządzania. Analizę warto przeprowadzać zawsze po pojawieniu się zmian w firmie⁴⁵.

Do kompletu analiz, które mają za zadanie wspierać organizację i zapobiec ewentualnemu przerwaniu funkcjonowania organizacji, zaliczymy również analizę oceny ryzyka. Można wykonać ją w pięciu następujących krokach:

- zebranie potrzebnych informacji,
- identyfikacja zagrożeń,
- oszacowanie ryzyka,
- określenie działań eliminujących lub ograniczających ryzyko,
- dokumentowanie wyników⁴⁶.

Wynikiem tej analizy jest macierz, która w stopniach pokazuje poziom ryzyka.

Analiza systemowa, która jest oficjalnym, a także jawnym badaniem mającym wspomóc działanie osób odpowiedzialnych za decyzje w danej sytuacji, charakteryzuje się niepewnością. Polega na określeniu pożądanego działania poprzez rozważenie wielu wariantów oraz porównanie ich scenariuszy w celu przewidzenia skutków⁴⁷.

Aby utrzymać prawidłowo funkcjonujące procesy, musimy znać powiązania i zależności między nimi; tutaj przyda się analiza powiązań i zależności.

43 Ibidem, s. 125.

44 SWOT – akronimem od angielskich wyrazów określających cztery elementy analizy: S – Strengths (mocne strony), W – Weaknesses (słabe strony), O – Opportunities (możliwości), T – Threats (zagrożenia).

45 T.T. Kaczmarek, G. Ćwiek, op. cit., s. 126.

46 *Ocena ryzyka zawodowego*, <https://www.pip.gov.pl/dla-pracodawcow/niezbednik-pracodawcy/ocena-ryzyka-zawodowego> [dostęp: 20.05.2025].

47 W. Findeisen, *Analiza systemowa. Podstawy i metodologia*, Warszawa 1985, s. 13.

W sytuacjach kryzysowych, gdy ciągłość może zostać zachwiana, należy dążyć do przywrócenia łańcucha procesów, które funkcjonowały w przedsiębiorstwie przed wystąpieniem kryzysu.

Wszystkie wymienione analizy mają za zadanie przygotować organizację na ewentualne sytuacje kryzysowe, które mogą pojawić się na ich biznesowej drodze. Żeby odpowiednio to zrozumieć, warto przyjrzeć się procesowi zarządzania ryzykiem⁴⁸.

Przed wszystkim organizacja musi zidentyfikować, przeanalizować i ocenić kategorie ryzyka, na które może być narażone. Kolejnym krokiem jest wypracowanie odpowiednich działań, a także metod, które pozwolą zminimalizować ryzyko i jednocześnie maksymalizować zyski. Zaproponowane rozwiązania muszą zgadzać się ze specyfiką firmy⁴⁹.

Celem analizy ryzyka jest zmniejszenie potencjalnego zagrożenia i jego konsekwencji na funkcjonowanie przedsiębiorstwa. Poprawnie przeprowadzona analiza ryzyka bazuje na najlepszych dostępnych źródłach informacji takich, jak: doświadczenia, dane z poprzednich lat, prognozy i opinie ekspertów, informacje zwrotne od wszystkich interesariuszy czy obserwacje⁵⁰.

Analiza ryzyka obejmuje m.in. czynniki ludzkie i kulturowe⁵¹. W założeniu powinna być:

- przejrzysta i kompleksowa,
- dynamiczna i powtarzalna,
- elastyczna, łatwo dostosowująca się do zmian oraz dopasowana do wewnętrznych i zewnętrznych uwarunkowań organizacji,
- bazująca na najlepszych z dostępnych źródeł informacji⁵².

48 J.L. Lambin, op. cit., s. 46.

49 <https://uhy-pl.com/blog-posts/4-metody-na-zidentyfikowanie-ryzyka-w-przedsiębiorstwie/> [dostęp: 10.06.2021].

50 B. Szlachcic, *Analiza ryzyka w zarządzaniu kryzysowym*, [w:] *Analiza informacji w zarządzaniu bezpieczeństwem*, red. nauk. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2013, s. 92–114.

51 B. Szlachcic, *Analiza ryzyka i zarządzania ryzykiem jako element systemu zarządzania kryzysowego w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie” 2014, nr 103, s. 233.

52 J.L. Lambin, op. cit., s. 51.

Zarówno analiza ryzyka, jak i wszystkie wspomniane jej cechy prowadzone w sposób systematyczny mogą przyczynić się do poprawy efektywności, a także uzyskania jednolitych i wiarygodnych rezultatów⁵³.

Analiza ryzyka pomaga przygotować się do kryzysu, w którym jeżeli nadejdzie, to będzie można szybko uruchomić procedury naprawcze i wdrożyć plany kryzysowe, a następnie plany naprawcze⁵⁴.

Procedury i plany awaryjne w procesie zarządzania bezpieczeństwem przedsiębiorstwa

Jeżeli dojdzie do sytuacji kryzysowej bądź przed taką sytuacją w celach prewencyjnych, to należy mieć przygotowany udokumentowany plan naprawczy, który jest w stanie złagodzić lub naprawić skutki powstałego zdarzenia. Każda firma dostosowuje plany i procedury na podstawie dogłębnych analiz w zależności od swoich potrzeb oraz rodzaju przewidywanego zagrożenia. W celu efektywnego zarządzania ciągłością działania konieczne jest stworzenie takich planów⁵⁵.

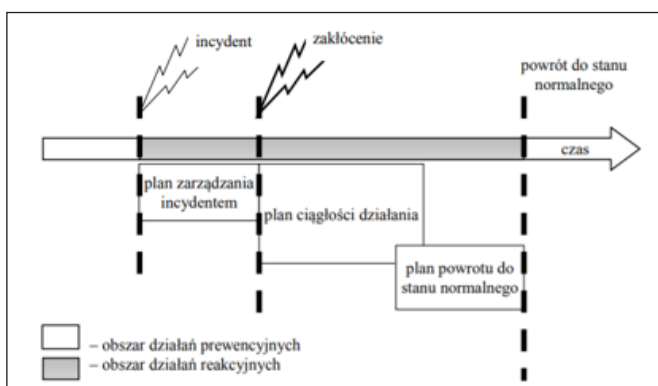
Zgodnie z wymaganiami ISO 22301 jednym z niezbędnych dokumentów jest posiadanie planu ciągłości biznesowej zawierającego procedury i informacji, które zostaną wykorzystane w razie wystąpienia zagrożenia. Drugim jest plan zarządzania zdarzeniem/incydem, czyli udokumentowany plan działania obejmujący personel i zasoby organizacji, stosowany w przypadku wystąpienia incydem. Plan zarządzania incydem jest uruchamiany każdorazowo po jego wystąpieniu. Pomiędzy obydwojema planami występują zależności (schemat 7). Jeżeli incydem przeradza się w kryzys, to podejmuje się działania określone w planie ciągłości działania⁵⁶. Nowy standard do tej normy zwany ISO 22301 kładzie również nacisk na elementy dotyczące komunikacji oraz zwiększenie odpowiedzialności. Dodatkowo stawia na bardziej aktywne przywództwo kierowników wyższego szczebla.

53 Ibidem, s. 233.

54 Ibidem, s. 238.

55 K. Białycki, *Instrumenty marketingu*, Bydgoszcz–Warszawa 2006, s. 18.

56 S. Zapłata, *Systemowe zarządzanie ciągłością działania BS 25999 w działalności usługowej*, Poznań 2012, s. 250.



Źródło: S. Zapłata, M. Kaźmierczak, *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Warszawa 2011, s. 152.

Schemat 7. Plany w systemie zarządzania ciągłością działania

Ponieważ plany awaryjne służą możliwości odtworzenia działalności organizacji na nowo, dlatego tak ważne jest określenie rodzajów incydentów, które mogą tę ciągłość zakłócić. Oprócz procedur mających minimalizować straty plany te obejmują dokładne instrukcje jak odtworzyć dany proces⁵⁷.

Podczas tworzeniu procedur w planach dotyczących ciągłości działania musimy pamiętać, że w sytuacji kryzysowej nie wszystkie zasoby mogą być dostępne. Warto również zwrócić uwagę na dwa zagadnienia, tj. zarządzanie organizacją w sytuacji kryzysowej wymagające szybkich działań, stąd pojawia się konieczność uproszczenia schematu decyzyjnego, oraz komunikację w sytuacji kryzysowej obejmująca wymianę z klientami zewnętrznymi dostawcami, administracją czy mediami, a także komunikację wewnętrzną w firmie⁵⁸.

Zgodnie z *good practice guide*⁵⁹ wszystkie plany i koncepcje utrzymania ciągłości działania powinny opierać się na krytycznej ocenie głównych obszarów aktywności przedsiębiorstwa (Mission Critical Activities – MCA), a także na ocenie skutków zaistniałych i możliwych strat (Business Impact Analysis – BIA). Ponieważ środowisko i rynek się zmieniają, zatem odpowiednie części planu powinny być na bieżąco aktualizowane. Wszystkie te czynności tworzą

⁵⁷ T.T. Kaczmarek, G. Ćwiek, op. cit., s. 21.

⁵⁸ Ibidem, s. 21.

⁵⁹ Kodeks dobrych praktyk tu odnosi się do konkretnych opracowań dotyczących zarządzania ciągłością działania.

jeden proces, o którym mowa również w normie ISO 22301. Obejmuje on następujące fazy:

- zrozumienie założeń prowadzonego biznesu,
- zdefiniowanie strategii utrzymania ciągłości działania,
- przygotowanie planu oraz jego wdrożenie,
- stworzenie kultury utrzymania ciągłości działania,
- wprowadzenie planu w życie, dodatkowo testy i audyty⁶⁰.

Ważną kwestią w wymienionych fazach jest istota testów i audytów. Wszystkie przygotowane plany powinny być dobrze znane, a ludzie pracujący w organizacji powinni być z nich przeszkoleni. Praktyka będzie tutaj najlepszym nauczycielem. W wielu firmach organizuje się szkolenia na ten temat. Podstawowym celem testów i ćwiczeń jest stwierdzenie, czy sprawne są programy UCD, plany kontynuacji, zarządzania ryzykiem i zarządzania kryzysowego czy w dostatecznym stopniu jest zabezpieczone całe przedsiębiorstwo przed negatywnymi skutkami nieprzewidzianych zdarzeń losowych⁶¹.

Wszystkie te fazy są modyfikowane zgodnie z potrzebami do czasu aż cała organizacja osiągnie akceptowalny poziom utrzymania ciągłości działania. Przyczynami zmian są różne zdarzenia i okoliczności zarówno te pozytywne, jak i negatywne⁶². Jeżeli plan skutecznie nie zadziała, to firmie grożą poważne konsekwencje, a nawet zakończenie działalności, dlatego omawiane fazy powinny być tak sformułowane, żeby wyraźnie wynikała z nich ochrona głównego interesu przedsiębiorstwa⁶³. Ważne jest utworzenie zespołu, który będzie koordynował i opracowywał szczegółowe procedury w sytuacjach awaryjnych⁶⁴. Według koncepcji BCP (Business Continuity Planning) przedsiębiorstwo ma możliwość rozstrzygnięcia wielu pytań odnoszących się do przyszłości w oparciu o poniższe pojęcia:

- Business Continuity Planning (BCP) – planowanie kontynuacji działania (pol. UCD),
- Disaster Recovery Planning (DRP) – planowanie odzyskania podstawowych zasobów po incydencie,

60 T.T. Kaczmarek, G. Ćwiek, op. cit. s. 46.

61 Ibidem, s. 45.

62 Ibidem, s. 48.

63 Ibidem, s. 55.

64 J. Zawila-Niedźwiecki, op. cit., s. 156.

– Contingency Planning (CP) – planowanie działań na wypadek nieprzewidzianych zdarzeń⁶⁵.

Opracowanie planu UCD jest procesem wieloaspektowym, który obejmuje następujące najważniejsze fazy:

- założenia do przyszłych analiz (Business Impact Analysis – BIA),
- plan odtworzenia zniszczonego majątku (Disaster Recovery Plan – DRP),
- zespół ds. Disaster Recovery – testowanie sytuacji awaryjnych;
- utrzymanie planu UCD w stałej gotowości do stosowania⁶⁶.

Posiadanie planów UCD adekwatnych do wielkości firmy i skali ma większe znaczenie w mniejszych firmach niż w przypadku korporacji, dlatego że są one bardziej narażone i zazwyczaj w mniejszym stopniu przygotowane na kryzysy, które mogą je spotkać. Ponadto jest istotna kwestia możliwości finansowania, czyli pobierania funduszy w celu dokonania przedsięwzięć w przedsiębiorstwie⁶⁷. Dla kadry zarządzającej jest ważne jak w razie kryzysu bądź zagrożenia firma zostanie odebrana przez środowisko, jak sobie poradzi i jakie opinie negatywne może spowodować wydarzenie? W tym punkcie warto przywrzeć się marketingowi jako procesowi ważnemu w naprawie skutków kryzysu. Dział ten często bywa angażowany w plany naprawcze, ponieważ każda negatywna sytuacja może wpłynąć na markę, a zadaniem marketingu jest budować dobry wizerunek.

Zakończenie

Każde przedsiębiorstwo posiada założone cele, mimo to jednym z głównych jest osiągnięcie konkretnego zysku finansowego. Żeby organizacja mogła działać i osiągać zysk, jest konieczne prowadzenie właściwie zaplanowanych działań marketingowych.

Równie ważne jest to, żeby organizacja mogła działać w sposób bezpieczny i przewidywalny, zwłaszcza wtedy, kiedy bierze się pod uwagę to, że funkcjonując w turbulentnym otoczeniu, jest narażona na występowanie licznych sytuacji kryzysowych.

⁶⁵ Ibidem, s. 66.

⁶⁶ Ibidem, s. 72–74.

⁶⁷ Ibidem, s. 71.

Dzięki zastosowaniu odpowiednich narzędzi marketingowych przedsiębiorstwo może uzyskać stałą przewagę konkurencyjną. Tworzenie pozycji konkurencyjnej i działanie w niestabilnym otoczeniu powoduje, że każde przedsiębiorstwo musi dbać o sprawy związane z zarządzaniem ciągłością działania. Jednakże, chcąc sprostać konkurencji, a tym samym dbać o bezpieczeństwo, należy przedsiębiorstwo zabezpieczać wieloaspektowo. Z jednej strony jego działania muszą się koncentrować na pogłębianiu zaufania klientów, żeby nie stracić przychodów, z drugiej, zapobiegać ewentualnym przyszłym sytuacjom kryzysowym.

Żeby zapobiec niekorzystnym sytuacjom, firmy tworzą analizy ryzyka, w których określają ewentualne problemy lub zagrożenia w bieżącej działalności firmy. Identyfikacja ryzyk pozwala na opracowanie procedur i planów zarządzania ciągłością działania, co ma uchronić przedsiębiorstwo na wypadek incydentów i sytuacji kryzysowych mogących wystąpić w funkcjonowaniu organizacji.

Wobec tego można się zastanowić, czy w planach zarządzania ciągłością działania jest miejsce na marketing? Wydaje się, że na tak postawione pytanie należy odpowiedzieć pozytywnie, dzięki bowiem działaniom marketingowym można stosować plan naprawczy, który pomoże organizacji przetrwać i budować nową pozycję na rynku. Każda organizacja musi być zabezpieczona na różne okoliczności, w tym jak skutecznie sobie radzić z sytuacjami kryzysowymi, w jaki sposób kształtować komunikację kryzysową, w którym kierunku prowadzić działania rozwojowe.

Celem niniejszego artykułu było pokazanie roli marketingu w procesie zarządzania ciągłością działania. Autor przeanalizował dziesięć spółek kapitałowych pod kątem sposobu podchodzenia do tego zagadnienia ze szczególnym uwzględnieniem roli i znaczenia działań marketingowych. Żeby realizować proces zarządzania ciągłością działań, należy stale doskonalić przedsiębiorstwo. Pomaga w tym skuteczny i efektywny marketing, który może być wdrażany w organizacji na różne sposoby. Ta doskonałość co prawda pozostaje w strefie niedoścignionego ideału, ale dążą do niego firmy, które samodzielnie decydują o sposobie doskonalenia swojej działalności.

Ważne jest pozyskanie w miarę pełnej wiedzy o wszystkich zjawiskach. Oczywiście, pełne przewidywanie takich zjawisk jest niemożliwe, dlatego że ich różnorodność zagraża osiągnięciu zamierzonych celów przez przedsiębiorstwo.

Niebezpieczeństwa te rodzą się w różnych uwarunkowaniach organizacyjno-prawnych, ekonomiczno-finansowych, techniczno-technologicznych i innych. Oznacza to powstawanie nowych rodzajów ryzyka i przeobrażenie już istniejących. W tym kontekście przedsiębiorstwa podejmują określone wzorce, z których najbardziej powszechna jest metoda BCM, dzięki której można wprowadzić model oceny dojrzałości zarządzania ryzykiem. We wdrażaniu tych narzędzi może pomóc skuteczny i nowoczesny marketing. Oczywiście, nie istnieje złota metoda na implementację takiego samego rozwiązania w każdej firmie, mimo to efektywnie prowadzony marketing ma wpływ na sprawność realizacji procesu ciągłości działania.

Bibliografia

- Białecki K., *Instrumenty marketingu*, Bydgoszcz–Warszawa 2006.
- Bieniok H. i in., *Metody sprawnego zarządzania*, Warszawa 2004.
- Blim M., Byczkowski M., Zawila-Niedźwiecki J., *Zintegrowane zarządzanie bezpieczeństwem organizacji*, [w:] *Systemy informatyczne. Bankowość i finanse*, red. F. Marecki, J.K. Grabara, J. Nowak, Warszawa 2005.
- Findeisen W., *Analiza systemowa. Podstawy i metodologia*, Warszawa 1985.
- <https://uhy-pl.com/blog-posts/4-metody-na-zidentyfikowanie-ryzyka-w-przedsiębiorstwie/> [dostęp: 10.06.2021].
- Kaczmarek T., Ćwiek G., *Ryzyko kryzysu a ciągłość działania*, Warszawa 2015.
- Kotler Ph., Armstrong G., Saunders J., Wong V., *Marketing. Podręcznik europejski*, Warszawa 2002.
- Lambin J.L., *Strategiczne zarządzanie marketingowe*, Warszawa 2001.
- Lidermann K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017.
- Marketing przedsiębiorstw przemysłowych*, red. W. Mantura, Poznań 2000.
- Michalski E., *Marketing*, Warszawa 2004.
- Ocena ryzyka zawodowego*, <https://www.pip.gov.pl/dla-pracodawcow/niezbednik-pracodawcy/ocena-ryzyka-zawodowego> [dostęp: 20.05.2025].
- Rydel M., *Komunikacja jako element marketingu*, [w:] *Komunikacja marketingowa*, red. M. Rydel, Gdańsk 2001.
- Ryzyko operacyjne w naukach o zarządzaniu*, red. nauk. I. Staniec, J. Zawila-Niedźwiecki, Warszawa 2015.
- Szlachcic B., *Analiza ryzyka i zarządzania ryzykiem jako element systemu zarządzania kryzysowego w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie” 2014, nr 103.
- Sznajder A., *Marketing. Encyklopedia biznesu*, t. 1, Warszawa 1995.
- Waniowski P., Sobotkiewicz D., Daszkiewicz M., *Marketing – teoria i przykłady*, Wydawnictwo Placet, Warszawa 2010.

- Zapłata S., *Systemowe zarządzanie ciągłością działania BS 25999 w działalności usługowej*, Poznań 2012.
- Zapłata S., Kaźmierczak M., *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Warszawa 2011.
- Zaskórski P. *Informacyjno-biznesowa ciągłość działania firmy*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki” 2011, nr 5.
- Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania*, Kraków 2013.

Business Continuity in the Enterprise from a Security Perspective

Abstract

Due to the rapidly changing environment, enterprises are paying more and more attention to the issue of business continuity management. Much is said about the threat of the modern world, which is the dependence on technology, which causes business continuity to become a fundamental factor of success for many organisations. Conscious enterprises protect themselves in many layers so as not to lose trust among customers, not to lose revenue, and also to prevent the loss of potential benefits.

The article addresses the issue of proper operation of the enterprise from a security perspective. Therefore, managing your business continuity becomes important, which directly translates into the security of the enterprise.

Keywords:

enterprise, security, management

Kazimierz J. Pawelec

Instytut Nauk o Bezpieczeństwie

Uniwersytet w Siedlcach

ORCID: 0000-0001-8669-0249

pawelec.kancelaria@op.pl

Wyjaśnienia oskarżonych i podejrzanych a ich wpływ na bezpieczeństwo prawne

Streszczenie

Publikacja dotyczy prawa do kłamstwa sprawcy przestępstwa, późniejszego podejrzanego, podejrzanego, oskarżonego i wreszcie skazanego niewątpliwie należy do kontrowersyjnych, gdyż traktuje prawo do kłamstwa wymienionych osób wyłącznie jako środek obrony, a więc niewyczerpujący znamion zarówno przestępstwa popełnienia, jak i innych przestępstw służących uniknięciu odpowiedzialności karnej, utrudnieniu prowadzonego postępowania, symulowaniu choroby czy wykorzystywaniu dokumentów zawierających nieprawdziwe treści. Rozważa, czy w wyjaśnieniach czy to fałszywym samooskarżeniu lub też kłamliwym obciążaniu niewinnych osób stanowi nadużycie prawa do obrony i jest podstawą do ścigania karnego, w tym także przestępstw z oskarżenia prywatnego, np. zniesławienia. Oparta została na obserwacji praktyki, w tym wykorzystywaniu przez nią pozyskanych nielegalnie treści zawartych w dokumentach, nośnikach, komputerach czy z cyberprzestrzeni. Zwraca uwagę, że decydujący o odpowiedzialności karnej jest zamiar sprawcy przestępstwa zmierzający do uniknięcia odpowiedzialności i poniesienia kary, który niejako ma swój początek w chwili jego popełnienia, a kończy się z datą odbycia kary.

Słowa kluczowe

sprawca, podejrzan, oskarżony, skazany, wyjaśnienia

Wstęp

Nie może budzić sporów twierdzenie, że odpowiedzialność karna musi opierać się na zasadzie indywidualizacji oraz winy (art. 1 § 1 i 3 k.k.). Skazanie oskarżonego nie może zatem pomijać jego winy, którą należy udowodnić konkretnymi dowodami uzyskanymi zgodnie z zasadami, a także szczegółowymi przepisami procedury karnej. Nie można opierać się na domniemaniach czy prawdopodobieństwie, nawet choćby było ono bardzo duże. Dlatego do rekonstrukcji strony podmiotowej czynu, czyli zamiaru bądź zachowania należytę staranności, konieczna jest kompleksowa analiza materiału dowodowego, tj. okoliczności podmiotowych i przedmiotowych. W katalogu dowodów należy wobec tego wskazać również wyjaśnienia oskarżonego (podejrzanego), które w procesie karnym odgrywają klasycznie podwójną rolę, stanowią jednocześnie środek obrony i dowód, chociaż bardzo specyficzny z uwagi na pozycję oraz uprawnienia oskarżonego. Oskarżony może skorzystać z tzw. prawa do milczenia, odmowy udzielenia odpowiedzi na poszczególne pytania, wiele czynności dowodowych z jego udziałem wymaga uzyskania jego zgody, a wyjaśnienia wcale nie muszą być prawdziwe.

Wyjaśnienia oskarżonego (podejrzanego) są to jego ustne, dobrowolne wypowiedzi, które zostały zaprotokołowane, dotyczące przedmiotu dowodzenia. Oskarżony wypowiada się w nich zarówno co do kwestii faktycznych, jak i prawnych¹.

Niewątpliwie istotne znaczenie mają te wyjaśnienia, w których oskarżony potwierdza okoliczności dla siebie niekorzystne, zwłaszcza wówczas, gdy przyznaje się do winy. Wartość tego rodzaju wyjaśnień uzyskanych z zachowaniem wszystkich gwarancji procesowych nabiera szczególnego znaczenia. Wyjaśnienia tego rodzaju mogą jednak skutkować określonymi w kodeksie karnym preferencjami, w tym nadzwyczajnym złagodzeniem kary, a nawet odstąpieniem od jej wymierzenia czy wreszcie, po spełnieniu warunków proceduralnych, skorzystania ze statusu świadka koronnego, czyli w konsekwencji uniknięcia odpowiedzialności karnej. Mimo tego rodzaju, przykładowo, wymienionych preferencji przyznanie się do winy jest tylko jednym z dowodów podlegających ocenie organu procesowego.

1 Por. S. Kalinowski, *Polski proces karny*, Warszawa 1971, s. 311.

W niniejszej publikacji będą nas interesowały zarówno fałszywe samooskarżenia, wyjaśnienia obciążające nazywane również pomówieniami, jak i inne zachowania podejrzewanych, podejrzanych, oskarżonych oraz skazanych zmierzających do uniknięcia odpowiedzialności karnej, jej zmniejszenia czy uniknięcia odbycia kary. Niewątpliwie są to kwestie trudne i kontrowersyjne, a praktyka dostarcza przykładów spraw traktujących poczynania wymienionych jako inne przestępstwa, chociaż ich zamiarem oraz świadomością było objęcie przestępstwo poplecznictwa, którego oskarżony czy skazany nie może popełnić.

Fałszywe samooskarżenie

Od przyznania się do niepopelnionego przestępstwa trzeba odróżnić fałszywe samooskarżenie². Należy zwrócić uwagę, że przyznanie się do przestępstwa niepopelnionego nie pociąga za sobą konsekwencji prawnych w przeciwieństwie do fałszywego samooskarżenia. O fałszywym samooskarżeniu można mówić w dwojakim znaczeniu, tj. *sensu stricto*, czyli w sytuacji złożenia oświadczenia o popełnieniu przez siebie przestępstwa lub wykroczenia, o którym organy ścigania nie wiedziały bądź miały o nim informacje, lecz nie kojarzyły z określoną osobą albo nie miały dostatecznych podstaw, żeby podjąć przeciwko niej postępowanie. Z kolei *sensu largo* oznacza każde dostarczenie przeciwko sobie dowodów, które wprost lub pośrednio mogły wskazywać na popełnienie przestępstwa³.

Fałszywe samooskarżenie ma miejsce również wówczas, gdy ktoś inny swoimi wyjaśnieniami spowodował wszczęcie postępowania karnego przeciwko innej osobie, a ta ostatnia temu nie zaprzeczyła, wręcz przeciwnie, przyjęła na siebie winę przez przyznanie się do jego popełnienia. Prawo karne, podobnie jak proces karny, nie nakładają na nikogo obowiązku ujawnienia

- 2 Por. K. Otłowski, *Podejrzany w postępowaniu karnym. Studium kryminalistyczne*, Warszawa 1979, s. 180–184; H. Rajzman, *Glosa do uchwały całej Izby Sądu Najwyższego z 18.02.1961 r.*, VI KO 29/59, OSPiKA 1961, nr 78, s. 464.
- 3 Por. K.J. Pawelec, *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych*, Warszawa 2021, s. 291 oraz podana literatura.

własnego przestępstwa, co jest konsekwencją obowiązywania zasady domniemania niewinności⁴.

Wyjątek stanowi art. 178 § 1 k.k. czy też art. 178b k.k., np. w razie ucieczki sprawcy wypadku z miejsca jego zaistnienia w celu uniknięcia odpowiedzialności, zatajenia stanu trzeźwości, bycia pod wpływem środków odurzających czy ucieczki przed policyjnym pościgiem, np. w celu uniknięcia odpowiedzialności z art. 178a § 1 k.k. Brak obowiązku ujawnienia własnego przestępstwa oraz przyznania się do winy nie oznacza, że jedno i drugie jest obojętne z punktu widzenia prawa karnego materialnego. Przede wszystkim należy wziąć je pod uwagę jako okoliczność charakteryzującą zachowanie sprawcy popełnionego przestępstwa (art. 53 § 1–3 k.k., art. 60 § 1–2 k.k.). Ujawnienie przestępstwa przez samego sprawcę ma szczególne znaczenie, gdy ustawa wiąże z tym faktem uchylenie karalności bądź zapewnienie sprawcy, który ujawnił swoje przestępstwo, łagodniejszą karę. We wszystkich tych sytuacjach zawiadomienie o przestępstwie lub osobiste zgłoszenie się do organu ścigania, jak wymaga tego np. ustawa o amnestii, nie jest traktowane jako obowiązek. Ustawodawca daje sprawcy szansę zależną od jego woli, ale powodującą uwolnienie od odpowiedzialności karnej. Jednakże nie oznacza to automatycznego uchylenia karalności wynikającego z innych przepisów pozostających w zbiegu⁵.

Praktyka zna przypadki, że wyjaśnienia oskarżonego (podejrzanego) zawierają całkowite lub częściowe przyznanie się do winy. Tego rodzaju przyznanie może mieć miejsce zarówno w przypadku rzeczywistego popełnienia przez daną osobę przestępstwa, jak i wtedy, kiedy osoba przyznająca się do popełnienia czynu zabronionego nie popełniła go, a nawet, gdy przestępstwo nie zostało popełnione⁶.

Samo przyznanie się do winy, niepotwierdzone innymi dowodami bezpośrednimi lub choćby pośrednimi, nie powinno być podstawą do dokonania ustaleń faktycznych. Nie można przecież wykluczyć, na co wskazuje praktyka,

4 Por. S. Glaser, A. Mogilnicki, *Kodeks karny. Komentarz*, Kraków 1934, s. 476; K. Sychta, [w:] *Kodeks postępowania karnego. Komentarz*, red. J. Zagrodnik, Lex/el 2023.

5 Por. Uchwała SN z 15.10.1970 r., VI KZP 15/70, „Nowe Prawo” 1971, nr 1, poz. 139; K.J. Pawelec, *Zarys...*, s. 292 oraz podana literatura i orzecznictwo.

6 Więcej zob. Z. Czeczot, *Falszywe samooskarżenie*, „Problemy Kryminalistyki” 1964, nr 49, s. 319 i n.

że oskarżony (podejrzany) mógł mieć interes w obciążaniu siebie wbrew prawdzie⁷.

Tego rodzaju wyjaśnienia, nazywane autopopiecznictwem (samopopiecznictwo) nie jest jednak przestępstwem z art. 239 § 1 k.k. nie tylko wówczas, gdy działania zmierzające do uniknięcia odpowiedzialności karnej podejmuje sam sprawca (współsprawca) przestępstwa, działając wyłącznie we własnym interesie procesowym, lecz także wtedy, kiedy oprócz interesu sprawcy także inne osoby miałyby lub mogłyby odnieść z tego korzyść procesową, zauważył Sąd Najwyższy w wyroku z 5 sierpnia 2009 roku (II KK 136/09, Lex nr 519594). Taki oskarżony może podejmować różne działania zmierzające do uniknięcia odpowiedzialności karnej. Samopopiecznictwo jest bezkarne, a dotyczy również udzielenia pomocy współsprawcy⁸.

Pomówienia (wyjaśnienia obciążające)

Szczególnym rodzajem wyjaśnień oskarżonego, także podejrzanego, są takie, w których zaprzecza on swojemu sprawstwu, jednocześnie twierdzi, że przestępstwo popełniła inna osoba bądź przyznając się do winy, stwierdza, że czynu zabronionego dopuścił się we współdziałaniu z kimś innym, i wskazuje jednocześnie jego personalia. Kodeks postępowania karnego nie odnosi się do tego rodzaju wyjaśnień nazywanych potocznie pomówieniami, a także wyjaśnieniami obciążającymi⁹.

Powyższą kwestię pozostawia praktyce oraz teorii procesu karnego. Jednakże praktyka pokazuje, że wielu sprawcom przestępstw udowodniono winę dzięki pomówieniom współoskarżonych, co miało miejsce zwłaszcza w odniesieniu do grup przestępczych.

7 Por.: Wyrok Sądu Najwyższego z 4.05.1955 r., III K 1501/54, OSN 1955/IV, poz. 50; Wyrok Sądu Najwyższego I K 340/57, [w:] K.J. Pawelec, *Zarys...*, s. 293; Wyrok Sądu Najwyższego z 22.03.1960 r., IV K 708/59, OSNPG 1960, nr 6, poz. 108; Z. Czeczot, op. cit., s. 311.

8 Por. Wyrok Sądu Administracyjnego w Lublinie z 30.12.2009 r., II AKa 197/09, Lex nr 658421; Postanowienie Sądu Najwyższego z 17.11.2020 r., IV KK 83/20, Lex nr 3080550.

9 Por. K. Otłowski, op. cit., s. 198.

O pomówieniu możemy mówić w znaczeniu *sensu stricto* i *sensu largo*. Pierwsze są to twierdzenia oskarżonego, że zarzuconego mu czynu dopuścił się we współdziałaniu z jeszcze inną osobą bądź osobami, *sensu largo* – to depozycje oskarżonego jakiegokolwiek innego przestępstwa dokonanego przez kogoś innego¹⁰.

Podczas oceny pomówienia niezbędne jest rozważenie, czy istnieją dowody bezpośrednie lub pośrednie potwierdzające wyjaśnienia tego rodzaju, a nadto logiczne, niewykazujące chwiejności czy wręcz nieprawdopodobieństwa. Ten rodzaj wyjaśnień wymaga wnikliwej i ostrożnej oceny, unikania wszelkiego rodzaju automatyzmu. Należy podejmować próby ustalenia powodów ich złożenia, a mogą być one bardzo różne – związane z chęcią zrzucenia z siebie winy, rozłożenia odpowiedzialności, zemstą, poprawieniem swojej sytuacji procesowej, pozorowaniem skruchy, a nawet uleganiem wpływom, naciskom, obietnicom oraz naciskom organów policyjnych¹¹.

Można, i chyba należy, bronić poglądu, że pomówienie jest wyłącznie linią obrony, podobnie jak wyjaśnienia nieprawdziwe, ale nieobciążające nikogo. W ten sposób oskarżony realizuje swoje procesowe uprawnienia. Jednakże tego rodzaju wyjaśnienia mają również walor dowodu podlegającego ocenie, chociaż bardzo ostrożnej, z zachowaniem szczególnego krytycyzmu, zwłaszcza wówczas, gdy cechuje je zmienność, a oskarżony tę zmienność uzasadnia.

Orzecznictwo Sądu Najwyższego, już od lat, konsekwentnie stoi na stanowisku, że same wyjaśnienia mające charakter pomówienia mogą być uznane za wystarczający dowód winy i zasadniczo nie wymaga ich wzmocnienia innymi dowodami. Jednakże przestrzega, że jest to dowód szczególnego rodzaju, wymagający szczególnej ostrożności podczas dokonywania jego oceny, a to z uwagi na specyficzną sytuację procesową oskarżonego (podejrzanego). Wszak nie ma on obowiązku mówienia prawdy. Może mieć przecież interes prawny w obciążaniu innej osoby. Należy przy tym zaznaczyć, że wyjaśnienia

10 Por.: Wyrok Sądu Najwyższego z 6.02.1970 r., IV KR 249/69, OSNKW 1970, nr 4–5, poz. 46; Wyrok Sądu Najwyższego z 10.06.1972 r., II KR 25/72, „Biuletyn Sądu Najwyższego” 1973, nr 1, s. 11.

11 Więcej zob. K.J. Pawelec, *Zarys...*, s. 335–349 oraz podana literatura i orzecznictwo; R. Koper, *Swoboda wypowiedzi osoby przesłuchiwanej w procesie karnym*, Warszawa 2022 oraz podana literatura.

współoskarżonego nie są poszlakami, lecz dowodami bezpośrednimi i na taki ich charakter nie ma wpływu ocena ich wiarygodności¹².

Praktyka dostarcza aż nadto przykładów potwierdzających, że oskarżeni (podejrzani) pomawiają inne osoby o popełnienie przestępstw, których one się nie dopuściły. Tym samym jest zasadne pytanie, jak daleko sięga prawo do obrony oskarżonego, który broniąc siebie, oskarża inną osobę? Odpowiedź jest prosta wtedy, kiedy pomówienie okazuje się prawdziwe. Jeżeli jednak, a to w praktyce nie są odosobnione przypadki, sprawca pomawia inną osobę niezgodnie z prawdą, to czy wówczas nie nadużywa swojego prawa do obrony, jeżeli zaś działa w złej wierze, to też istnieją podstawy do pociągnięcia takiej osoby do odpowiedzialności karnej? Sąd Najwyższy w postanowieniu z 11 października 1952 roku (KO 117/52) stwierdził, że świadome fałszywe oskarżenie w toku postępowania karnego przez oskarżonego (podejrzanego) innej osoby o popełnienie przestępstwa stanowi przekroczenie prawa do obrony i jest występkiem¹³.

W obowiązującym stanie prawnym kwestia ta została potraktowana jako niejednoznaczna. Nie jest bowiem w dyrektywie art. 74 § 1 k.p.k. uznane, że fałszywe oskarżenie zawarte w takich wyjaśnieniach, które dało początek postępowaniu karnemu lub mogło je zainicjować, może stanowić przestępstwo fałszywego oskarżenia¹⁴.

Podsumowując omawianą kwestię, można stwierdzić, że prawo oskarżonego (podejrzanego) do obrony nie powinno iść tak daleko, żeby mógł on w toku składania we własnej sprawie wyjaśnień „kłamliwie” oskarżać inne osoby. Tego rodzaju nadużycie, niewątpliwie, powinno być uzależnione od złej woli oskarżonego, który ma zamiar i świadomość bezpodstawnego oskarżenia innej osoby. W tego rodzaju sytuacji, niewątpliwie, nie ma przeszkód do pociągnięcia do odpowiedzialności, np. z art. 212 k.k., czyli przestępstwa z oskarżenia prywatnego, chyba że fałszywie pomówił taką osobę o udział

12 Por. J. Kasiński, [w:] *Kodeks postępowania karnego. Orzecznictwo*, red. D. Świecki, Warszawa 2022; K. Boratyńska, [w:] *System prawa karnego procesowego*, t. 6, red. P. Hofmański, C. Kulesza, Warszawa 2016; K.J. Pawelec, *Zarys...*, s. 294.

13 Ibidem, s. 294. Por. Uchwała SN z 18.02.1961 r., VI KO 29/59, OSN 1961, nr 11, poz. 20.

14 Por. K. Siwek, *Odpowiedzialność za fałszywe wyjaśnienia*, „Przegląd Sądowy” 2017, nr 7–8, s. 124–135 oraz podana literatura i orzecznictwo; M. Gabriel-Węglowski, *Odpowiedzialność karna sprawcy przestępstwa za fałszywe pomówienie innej osoby o udział w tym przestępstwie*, Lex/el 2021 oraz podane orzecznictwo.

w danym przestępstwie, ale w celu ukrycia tożsamości rzeczywistych współuczestników, a nie w celu własnej obrony. W tego rodzaju przypadku wykracza poza granice przysługującego mu prawa do obrony i może ponieść odpowiedzialność z art. 234 k.k.¹⁵.

Inne czynności zmierzające do uniknięcia odpowiedzialności lub kary

W wyroku z 31 maja 2017 roku Sąd Apelacyjny we Wrocławiu (II AKa 111/17, Lex nr 2329079) sformułowano trafną tezę: „Skoro ustawodawca w art. 239 § 1 k.k. za poplecznictwo wprowadza odrębną określoną sankcję i odnosi to do osoby, która sprawcy pomaga, utrudniając lub udaremniając prowadzenie postępowania, jasnym się staje, że nie może dotyczyć to oskarżonego także poprzez zaostrenie kary za zachowania, które utrudniają lub udaremniają postępowanie karne. Korzystający ze swych ustawowo przyznanych uprawnień sprawca nie może ponosić konsekwencji, podejmowania dozwolonych prawem zachowań, poprzez ich wpływ – w sposób zaostrażający wymiar kary”.

Wobec tego przytoczona teza eliminuje wszelkie działania sprawcy przestępstwa, poczynając od zachowań zmierzających przez niego do zachowania *in cognito* bądź uniknięcia surowego potraktowania. Tego rodzaju zachowania, np.: zacieranie śladów przestępstwa, usuwanie dowodów rzeczowych, tworzenie fałszywego alibi, ukrywanie się, posługiwanie się fałszywymi dokumentami czy też symulowanie choroby psychicznej oraz innej uniemożliwiającej udział w procesie albo odbywania kary pozbawienia wolności, *de facto* mają swój początek niejako od daty popełnienia przestępstwa (chyba że przygotowanie traktowane jest jako czyn karalny), poprzez wszystkie stadia postępowania karnego, aż do końca orzeczonej kary, a nawet wcześniej, której zamierza uniknąć. Udowodnienie tych wszystkich poczynań spoczywa na organach ścigania, choć nie stoi na przeszkodzie uznania ich jako obawy mactwa stanowiącej szczegółową przesłankę do zastosowania np. tymczasowego aresztowania, oczywiście jeżeli istnieje przesłanka ogólna, czyli „dużego

15 Por. Uchwała Sądu Najwyższego z 11.01.2006 r., I KZP 2006r/I KZP 49/05, OSNKW 2006, nr 2, poz. 12. Więcej zob. K. Liżyńska, *Kwalifikowana postać przestępstwa pomówienia a ochrona wolności słowa*, „Państwo i Prawo” 2012, nr 9, s. 98–107, literatura i orzecnictwem.

prawdopodobieństwa sprawstwa”. Jednakże praktyka dostarcza przykładów spraw, w których oskarżeni (podejrzani) podejmowali próby uniknięcia odpowiedzialności lub skorzystania z nadzwyczajnego złagodzenia kary przez symulowanie choroby psychicznej, podżegania do uzyskania nieprawdziwej dokumentacji medycznej czy też innej zawierającej takie informacje. Analitycząc tego rodzaju sprawy, należy przede wszystkim zwrócić uwagę na określenie zamiaru sprawcy, a także świadomości podejmowanych przez niego działań, co, oczywiście, jest zadaniem w sam raz dla oskarżyciela, ale bez tolerowania prób obchodzenia tego, co chce sprawca osiągnąć, co ściśle łączy się z określeniem jego winy, czyli możliwością pociągnięcia do odpowiedzialności. Jeżeli zostanie ustalone, że sprawca zmierzał do uniknięcia odpowiedzialności karnej, niezależnie od rodzaju składanych wyjaśnień, to też swoim zachowaniem wyczerpuje znamiona przestępstwa poplecznictwa, którego jednak nie może być podmiotem. Sąd Najwyższy w wyroku z 12 marca 2020 roku (III KK 66/19, Lex nr 3180104) zasadnie stwierdził: „Za przestępstwo poplecznictwa odpowiada osoba udzielająca pomocy sprawcy przestępstwa, a nie sprawcy czynu zabronionego. Powyższe oznacza, że znamion tego występku nie realizuje ten kto udziela pomocy osobie, której z jakichkolwiek względów (np. z uwagi na zaistnienie okoliczności wyłączających bezprawność lub winę) nie można przypisać odpowiedzialności karnej za dokonanie popełnionego przez nią czynu”.

Realizacja znamion występku z art. 239 § 1 k.k. charakteryzuje się stworzeniem przeszkód w wykryciu sprawcy przestępstwa, udowodnienia mu winy, przedłużenia postępowania, uniknięcia kary czy stworzenia okoliczności uzasadniających możliwość jej nadzwyczajnego złagodzenia, a nawet odstąpienia od jej wymierzenia¹⁶.

Przestępstwo poplecznictwa, choć nie dotyczy sprawcy, może być popełnione jeszcze przed wszczęciem postępowania karnego w każdej jego fazie aż do czasu zakończenia kary. Podmiotem tego przestępstwa może być każdy

16 Por.: Wyrok Sądu Administracyjnego we Wrocławiu z 9.10.2019 r., II AKa 273/19, Lex nr 2749801; Wyrok Sądu Administracyjnego w Białymstoku z 12.09.2019 r., II AKa 97/19, Lex nr 3028932; Wyrok Sądu Administracyjnego we Wrocławiu z 7.11.2016 r., II AKa 14/16, Lex nr 2174870.

człowiek, gdyż należy do powszechnych. Jednakże nie może być nim sam sprawca, a także nie obejmuje samopolecznictwa oraz współsprawstwa¹⁷.

Aktualnie przed warszawskimi sądami toczą się postępowania karne przeciwko oskarżonym o podżeganie lekarzy lub biegłych w zamian za udzielenie korzyści majątkowych do sporządzenia fałszywych opinii, dokumentacji medycznej, a następnie posługiwanie się nimi, co miało stanowić podstawy uniknięcia odpowiedzialności karnej, odbycia reszty kary pozbawienia wolności czy też skorzystania z możliwości nadzwyczajnego złagodzenia kary. W uzasadnieniach aktów oskarżenia wprost stwierdzono, że sprawcy wymienionych przestępstw symulowali choroby psychiczne lub neurologiczne, czyli mieli zamiary utrudniania postępowań karnych. Nie sposób zatem nie zapytać, czy można było postawić im tego rodzaju zarzuty w sytuacji, gdy ich zamiarem było popełnienie popelecznictwa, za co nie mogli ponieść odpowiedzialności, realizacją zaś tego zamiaru było skorumpowanie określonych osób bądź symulowanie schorzeń? Czy prokuratura z premedytacją pomijała rzeczywiste zamiary sprawców, co miało podstawowe znaczenie dla przypisania im winy oraz prawidłowego zakwalifikowania czynów? Na tak postawione pytania sądy nie udzieliły jeszcze odpowiedzi, gdyż zawisłe przed nimi sprawy trwają, ponadto do tej pory oskarżyciele nie przedstawili dowodów, że oskarżeni działali przebiegle i wprowadzili w błąd wystawców opinii oraz dokumentów albo w innym celu niż uniknięcie zarówno odpowiedzialności, jak i kary¹⁸.

Zwraca na siebie uwagę również praktyka substytuowania wyjaśnień lub zeznań notatkami bądź zapiskami, a także przesłuchania jako świadków funkcjonariuszy policji lub innych osób na okoliczności przeprowadzanych nieformalnych rozmów bądź wykorzystywanie nielegalnie urządzeń technicznych lub informatycznych, a także pozyskiwanie dokumentów, nośników oraz informacji z cyberprzestrzeni zawierających tajemnice zawodowe, przedsiębiorstw albo naruszających sfery prywatności¹⁹.

17 Por. Wyrok Sądu Administracyjnego we Wrocławiu z 21.04.2016 r., II AKa 87/16, Lex nr 2052594.

18 Por. Wyrok Sądu Administracyjnego we Wrocławiu z 29.09.2022 r., II AKa 85/22, Lex nr 3455543; J. Piórkowska-Flieger, Glosa do wyroku SN z 26.11.2014 r., II KK 138/14, częściowo krytyczna, OSP 2015, nr 9, poz. 81.

19 Więcej zob.: K.J. Pawelec, *Znaczenie dowodowe czynności operacyjno-rozpoznawczych w cyberprzestrzeni. Granice zastosowania i konieczne ograniczenia*, [w:] *Bezpieczeństwo informacyjne. Wieloaspektowość poznania*, red. H. Wyrębek, Siedlece 2024 oraz

Zakończenie

Kodeks postępowania karnego w kwestii roli oskarżonego zajmuje tylko pozornie jasne stanowisko, stanowi bowiem, że jest stroną postępowania. Jednakże w rzeczywistości tak nie jest, gdyż jego wyjaśnienia to nie tylko środek obrony, ale należy również zaliczyć je do środków dowodowych, na których podstawie można ustalić stan faktyczny sprawy. Ustawodawca w tej materii nie jest jednoznaczny. Wychodzi zapewne z założenia, że oskarżony sam najczęściej jest „świadkiem” zarzuconego mu czynu, i to niekiedy nawet jedynym, dlatego jego wyjaśnienia mogą mieć dla wykrycia prawdy obiektywnej ważne znaczenie. Mogą mieć istotny walor dowodowy oraz wpływ na efekt postępowania. Dlatego, uwzględniając poczynione wcześniej zastrzeżenia dotyczące wiarygodności wyjaśnień oskarżonego, jego zainteresowanie wynikiem postępowania, należy stwierdzić, że nie sposób zrezygnować z tego środka dowodowego. Jednakże nie można zapominać, że oskarżony jest przede wszystkim stroną postępowania. Jeżeli decyduje się na składanie wyjaśnień, to przedstawia przebieg wydarzeń związanych z zarzuconym mu czynem, ale też wykorzystuje przysługujące mu uprawnienia strony. Nie ma obowiązku dostarczania dowodów przeciwko sobie ani dowodzić swojej niewinności. Stąd przyjęta teza o jego podwójnej roli znajduje swoje uzasadnienie. Ta dwiema rolami jest odgrywana na każdym etapie postępowania karnego – od jego wszczęcia, w fazie *ad rem*, *ad personam*, do prawomocnego rozstrzygnięcia oraz końca orzeczonej kary. Nie można zapominać, że wyjaśnienia oskarżonego zalicza się do materiału dowodowego, choćby nawet nie zostały uznane za wiarygodne²⁰.

podana literatura i orzecznictwo; K.J. Pawelec, *Informacje zawarte w systemach wspomagających kierującego i pojazdach autonomicznych oraz możliwości ich procesowego wykorzystania w systemie cyberbezpieczeństwa*, [w:] *Wielowymiarowość cyberbezpieczeństwa*, red. J. Żylińska, K. Huczek, K. Borkowski, Warszawa 2024, s. 157–177 wraz z literaturą i orzecznictwem; K.J. Pawelec, *Ujawnianie przestępczości narkotykowej w cyberprzestrzeni i jej dowodowe znaczenie w polskim procesie karnym*, [w:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, red. M. Karpiuk, Warszawa 2024, s. 176–189 i podana literatura oraz orzecznictwo; K.J. Pawelec, *Zarys...*, s. 335–353 z orzecznictwem i literaturą.

- 20 Por. L. Hochberg, *Wyjaśnienia oskarżonego w procesie karnym i ich wartość dowodowa*, Warszawa 1961, s. 9; S. Śliwiński, *Polski proces karny przed sądem powszechnym*.

Orzecznictwo Sądu Najwyższego od lat konsekwentnie prezentuje zapatrywanie dotyczące zrównania wartości dowodowej wyjaśnień złożonych w toku postępowania przygotowawczego i rozprawy sądowej²¹.

Wynika z niego, że w razie istnienia sprzeczności w wyjaśnieniach ich wartość dowodowa była taka sama, niezależnie od tego, czy zostały one złożone w postępowaniu przygotowawczym czy na rozprawie sądowej. Na sąd został nałożony obowiązek ustosunkowania się do takich wyjaśnień i dokonania wyboru, którą ze sprzecznych wersji uznaje za wiarygodną, oczywiście, po skonfrontowaniu z pozostałym materiałem dowodowym, czego dokonuje sąd.

W doktrynie były wyszczególniane różnego rodzaju wyjaśnienia, do których była zaliczana również odmowa wyjaśnień. Wyróżnia przyznanie się oskarżonego do winy, fałszywe samooskarżenie, wyjaśnienia obciążające, nieprzyznanie się do winy, zmienność wyjaśnień oraz tzw. ostatnie słowo²².

Bibliografia

- Boratyńska K., [w:] *System prawa karnego procesowego*, t. 6, red. P. Hofmański, C. Kulesza, Warszawa 2016.
- Czczot Z., *Fałszywe samooskarżenie*, „Problemy Kryminalistyki” 1964, nr 49.
- Gabriel-Węglowski M., *Odpowiedzialność karna sprawcy przestępstwa za fałszywe pomówienie innej osoby o udział w tym przestępstwie*, Lex/el 2021.
- Glaser S., Mogilnicki A., *Kodeks karny. Komentarz*, Kraków 1934.
- Gruszewska D., [w:] *Proces karny*, red. J. Skorupka, Warszawa 2017.
- Hochberg L., *Wyjaśnienia oskarżonego w procesie karnym i ich wartość dowodowa*, Warszawa 1961.
- Kalinowski S., *Polski proces karny*, Warszawa 1971.
- Kasiński J., [w:] *Kodeks postępowania karnego. Orzecznictwo*, red. D. Świecki, Warszawa 2022.
- Koper R., *Swoboda wypowiedzi osoby przesłuchiwanej w procesie karnym*, Warszawa 2022.
- Liżyńska K., *Kwalifikowana postać przestępstwa pomówienia a ochrona wolności słowa*, „Państwo i Prawo” 2012, nr 9.

Zasady ogólne, Warszawa 1961, s. 324; D. Gruszewska, [w:] *Proces karny*, red. J. Skorupka, Warszawa 2017, s. 426–430 oraz podana literatura i orzecznictwo.

21 Por. Wyrok Sądu Najwyższego z 14.02.1980 r., I KR 10/80, OSPiKA 1981, nr 1, poz. 10.

22 Więcej zob. K.J. Pawelec, *Zarys...*, s. 287–300 oraz podana literatura i orzecznictwo.

- Otłowski K., *Podejrzany w postępowaniu karnym. Studium kryminalistyczne*, Warszawa 1979.
- Pawelec K.J., *Informacje zawarte w systemach wspomagających kierującego i pojazdach autonomicznych oraz możliwości ich procesowego wykorzystania w systemie cyberbezpieczeństwa*, [w:] *Wielowymiarowość cyberbezpieczeństwa*, red. J. Żylińska, K. Huczek, K. Borkowski, Warszawa 2024.
- Pawelec K.J., *Ujawnianie przestępczości narkotykowej w cyberprzestrzeni i jej dowodowe znaczenie w polskim procesie karnym*, [w:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, red. M. Karpiuk, Warszawa 2024.
- Pawelec K.J., *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych*, Warszawa 2021.
- Pawelec K.J., *Znaczenie dowodowe czynności operacyjno-rozpoznawczych w cyberprzestrzeni. Granice zastosowania i konieczne ograniczenia*, [w:] *Bezpieczeństwo informacyjne. Wieloaspektowość poznania*, red. H. Wyrębek, Siedlce 2024.
- Siwek K., *Odpowiedzialność za fałszywe wyjaśnienia*, „Przegląd Sądowy” 2017, nr 7–8.
- Sychta K., [w:] *Kodeks postępowania karnego. Komentarz*, red. J. Zagrodnik, Lex/el 2023.
- Śliwiński S., *Polski proces karny przed sądem powszechnym. Zasady ogólne*, Warszawa 1961.

Explanations of Accused and Suspects and Their Impact on Legal Security

Abstract

The publication, which deals with the right to lie of the perpetrator of a crime, the later suspect, suspect, accused and finally convicted, is undoubtedly controversial because it treats the right to lie of the above-mentioned persons solely as a means of defence, and therefore does not exhaust the features of both the crime of aiding and abetting, as well as other crimes aimed at avoiding criminal liability, hindering the conducted proceedings, simulating illness, or using documents containing false content. It considers whether in explanations, either false self-incrimination or lying incrimination of innocent people constitutes an abuse of the right to defense and is the basis for criminal prosecution, including crimes at private indictment, e.g. defamation. It is based on observation of practice, including the use of illegally obtained content contained in documents, media, computers, or from cyberspace. It points out that the decisive factor for criminal liability is the intention of the perpetrator of the crime to avoid responsibility and suffer punishment, which in a way begins at the moment of its commission and ends on the date of serving the sentence.

Keywords

perpetrator, suspect, accused, convicted, explanation