Akademia Bialska im. Jana Pawła II

Wielowymiarowość środowiska bezpieczeństwa

Redakcja naukowa
Dariusz Brążkiewicz
Marta Chodyka
Tomasz Grudniewski
Sławomir Żurawski

Część druga

Wielowymiarowość środowiska bezpieczeństwa

Część druga

Redakcja naukowa

Dariusz Brążkiewicz
Marta Chodyka
Tomasz Grudniewski
Sławomir Żurawski

Biała Podlaska 2025

Wydawca
Akademia Bialska im. Jana Pawła II

Recenzenci
prof. dr hab. inż. Marian Kopczewski, Akademia Wojsk Lądowych
dr hab. inż. Henryk Wyrębek, prof. uczelni, Uniwersytet w Siedlcach

Korekta językowa
mgr Marzanna Brążkiewicz

ISBN 978-83-68103-20-5
https://doi.org/10.29316/9788368103205

Nakład: 80 egzemplarzy

Wydawnictwo AB JPII
ul. Sidorska 95/97
21-500 Biała Podlaska
wydawnictwo.akademiabialska.pl

Projekt okładki, skład i druk

druk-24h.com.pl
DRUKARNIA CYFROWA
Hurtowa 21, 15-399 Białystok
tel. 535 500 898
e-mail: studio@druk-24h.com.pl

Spis treści

WSTĘP

Epoka cyfryzacji XXI wieku zdecydowanie wpływa na wymiar bezpieczeństwa państwa, całego społeczeństwa lub wybranych grup etniczno-narodowościowych. Zjawisko to przyspiesza również proces globalizacji. Dostęp do Internetu przeważającej części światowej populacji zwiększa zakres oddziaływania zarówno pozytywnego, jak i negatywnego. Na to oddziaływanie znaczną presję wywierają procesy rozwoju sztucznej inteligencji oraz ich konsekwencje dla bezpieczeństwa systemów informatycznych Są to procesy o różnym nasileniu, ale stanowią, zwłaszcza te negatywne, zagrożenie dla bezpieczeństwa różnego szczebla: państwowego czy społecznego. Wiele informacji publikowanych jest z zamiarem wywierania wpływu na odpowiednio dobrane grupy odbiorców tychże wiadomości. Tym samym, takie operacje albo wykorzystują realne wydarzenia, albo są spreparowane i obejmują działania informacyjne realizowane dla kierunkowania rozumowania wybranych grup społecznych w danym regionie lub instytucji czy rządów wybranych państw.

Rozwijająca się cyberprzestępczość, stanowiąca tak szerokie zagrożenie, musi być w sposób systemowy wykrywana, izolowana i unieszkodliwiana. Do walki z tym niebezpieczeństwem należy wypracowywać skuteczne narzędzia oraz rozwijać zdolności do monitorowania poziomu zagrożeń oraz utrzymania kontroli nad skalą cyberzagrożeń, aby uniknąć nieprzewidywalnych konsekwencji. Działania te wynikają z faktu wykorzystywania Internetu w wielu dziedzinach życia, takich jak np.: korespondencja, zakupy, płatności co powoduje, że z wielką trudnością przychodzi nam wyobrażenie sobie braku możliwości korzystania z nich. Na przykładzie Polski można stwierdzić, że cyberprzestępczość w naszym kraju charakteryzuje się głównie tym, iż czyny przestępcze popełniane są w większości z wykorzystaniem Internetu. Tym samym, głównym zadaniem państwa jest posiadanie instytucji i narzędzi prawnych w celu prawidłowego i pozytywnego realizowania całego procesu wykrywczego, a w konsekwencji ukarania sprawców takich działań.

Współcześnie, jednym z elementów kształtującym środowisko bezpieczeństwa, jest trwająca wojna rosyjsko-ukraińska. Wbrew pozorom, zasięg oddziaływania tej wojny nie obejmuje tylko obszaru Europy

Środkowo-Wschodniej, ale państwa Europy, czy kraje zaangażowane po którejś ze stron konfliktu lub państwa zależne od dostaw np. ukraińskiego zboża. Jednym z elementów oddziaływania na agresora – Federację Rosyjską, są m.in. sankcje nakładane przez poszczególne państwa lub w ramach Unii Europejskiej. W przypadku tych ostatnich sankcji, są to pakiety sankcyjne, których głównym założeniem jest wywarcie presji politycznej i gospodarczej na Federację Rosyjską, aby zmniejszyć jej zdolność do prowadzenia wojny oraz skłonić ją do zakończenia agresji. Tym samym Unia Europejska posiada możliwości prawne oddziaływania w ten sposób. Są to m. in. ograniczenia w handlu towarami o znaczeniu strategicznym (technologie wysokiego ryzyka, surowce energetyczne), zakazy finansowych inwestycji w rosyjskie przedsiębiorstwa państwowe, ograniczenia usług doradczych, prawnych, audytorskich oraz zakaz współpracy w sektorze naftowym i gazowym. Bardzo ważna, a jednocześnie restrykcyjna jest polityka zamrażania aktywów rosyjskich. Działania te pokazują wyraźnie, że Unia Europejska ma możliwość mocnego oddziaływania polityczno-gospodarczego na Federację Rosyjską. Drugim aspektem wojny rosyjsko-ukraińskiej jest migracja obywateli Ukrainy na zachód, której szczyt osiągnięto w bardzo szybkim tempie w pierwszych miesiącach po wybuchu otwartej wojny rosyjsko-ukraińskiej w 2022 r. Jednym z krajów o największej intensywności przyjmowania migrantów z Ukrainy była Polska. To na naszym kraju spoczął cały logistyczny oraz prawny ciąg obowiązków wynikających z przekraczania granic strefy Schengen. W związku z napływem uchodźców wojennych z Ukrainy, Polska wdrożyła szereg rozwiązań legislacyjnych i administracyjnych, mających na celu zapewnienie efektywnej ochrony i integracji osób objętych ustawą o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa. Analizując wojskowe aspekty tej wojny należy zwrócić uwagę na zaangażowanie Federacji Rosyjskiej w rozwój poszczególnych rodzajów sił zbrojnych, szczególnie wojsk specjalnych, zaangażowanych na najważniejszych odcinkach frontu i do agresywnych działań, skutkujących zdobywaniem kolejnych wyodrębnionych obszarów Ukrainy. Ten militarystyczny element rosyjskich działań pokazuje, jak duże środki finansowe i ludzkie poświęcane są w celu prowadzenia tej wojny.

Trwająca wojna za naszą wschodnią granicą przynosi działania ochronne, takie jak odbudowa lub budowa elementów bezpieczeństwa wewnętrznego obywateli, na wypadek podobnych działań na terenie Polski. Podjęte działania,

oprócz budowy elementu militarnego, mają również przynieść rozwiązania bezpieczeństwa ludności cywilnej, a co za tym stoi – reaktywowania Obrony Cywilnej. Spośród wielu zadań tej formacji jednym z ważniejszych jest informowanie, ostrzeganie i wspieranie ludności cywilnej, z ewakuacją włącznie. Przyjęty pod koniec 2024 r. akt prawny normuje sytuację, gdy w wypadku stanu wojennego i w czasie wojny, ochrona ludności staje się obroną cywilną. Jest to jeden z fundamentów płynnego przejścia ze stanu działań kryzysowych okresu pokoju, do działań w czasie wojny. Kolejnym elementem przygotowań obrony cywilnej powinna być możliwość przypisania organizacjom pozarządowym zadań na czas wojny. Tym samym system obrony cywilnej powinien być nadal doskonalony w zakresie funkcjonowania zarówno własnych organów, jak i podmiotów, w tym przygotowania przeszkolonego personelu i zasobów do zagrożeń oraz działań gwarantujących przetrwanie ludności.

Prezentowana monografia jest przeglądem wiedzy autorów dotyczącym szeroko rozumianego bezpieczeństwa wewnętrznego, jak międzynarodowego, wynikającego ze współczesnych zagrożeń istniejącego i tworzącego się środowiska bezpieczeństwa, w obszarze globalnym, jak i regionalnym. Przedstawiane przez autorów rozdziałów reprezentujących różne ośrodki akademickie wnioski, przybliżają rezultaty tych badań. W monografii użyto wielu metod, technik i narzędzi badawczych, a uzyskane odpowiedzi wynikają z pytań badawczych, które przedstawiono w treści poszczególnych rozdziałów. Tym samym, przedstawione wnioski należy traktować jako wprowadzenie do otwartej dyskusji na temat globalnych i regionalnych zagrożeń dla bezpieczeństwa, w obszarze międzynarodowym i krajowym. Konsekwencją przedstawianych zagrożeń jest budowa odporności w wielu dziedzinach bezpieczeństwa. Poprawa tego bezpieczeństwa powinna wynikać z synergii tych działań w najbliższej przyszłości, co powinno wpłynąć na zagrożone bezpieczeństwo. Wiele tych aspektów omawia niniejsza monografia.

mgr inż. Marcin Nowak
ORCID: 0000-0002-1115-5679

https://doi.org/10.29316/9788368103205_1

CYBERPRZESTĘPCZOŚĆ JAKO WYZWANIE SYSTEMOWE

CYBERCRIME AS A SYSTEMIC CHALLENGE

Streszczenie

W rozdziale, za cel przyjęto kompleksową analizę zjawiska cyberprzestępczości w kontekście jego technologicznych uwarunkowań, różnorodnych form oraz działań podejmowanych przez państwa i organizacje międzynarodowe w celu przeciwdziałania tym zagrożeniom. Rozdział składa się z trzech zasadniczych części. W pierwszej przedstawiono ewolucję Internetu i rozwój technologii informacyjnych jako podstawę rozwoju środowiska sprzyjającego cyberprzestępczości. Druga część poświęcona została definicjom, klasyfikacjom oraz formom przestępstw popełnianych w cyberprzestrzeni, uwzględniając metody działania sprawców oraz dane statystyczne. Trzecia część omawia aktualne regulacje prawne oraz działania instytucjonalne podejmowane w Polsce i Unii Europejskiej w zakresie przeciwdziałania cyberzagrożeniom. Autor stawia pytanie badawcze: w jaki sposób rozwój Internetu oraz niedoskonałości systemów prawnych i organizacyjnych wpływają na skalę i skuteczność zwalczania

Summary

The aim of this chapter is to provide a comprehensive analysis of the phenomenon of cybercrime in the context of its technological determinants, various forms and actions taken by states and international organizations to counteract these threats. The chapter consists of three main parts. The first part presents the evolution of the Internet and the development of information technologies as the basis for the development of an environment conducive to cybercrime. The second part is devoted to definitions, classifications and forms of crimes committed in cyberspace, including the methods of action of perpetrators and statistical data. The third part discusses the current legal regulations and institutional activities undertaken in Poland and the European Union in the field of counteracting cyber threats. The author poses a research question: how do the development of the Internet and the imperfections of legal and organizational systems affect the scale and effectiveness of combating cybercrime? The hypothesis assumes that the

cyberprzestępczości? Postawiona hipoteza zakłada, że efektywność przeciwdziałania cyberprzestępczości zależy od poziomu integracji legislacyjnej, sprawności instytucji odpowiedzialnych za bezpieczeństwo cyfrowe oraz zdolności adaptacyjnych systemów ochrony wobec dynamicznie zmieniających się zagrożeń w cyberprzestrzeni. Zastosowane metody badawcze obejmują analizę literatury przedmiotu, przegląd źródeł prawa krajowego i międzynarodowego.

Słowa kluczowe: cyberprzestępczość, bezpieczeństwo cyfrowe, prawo karne, Internetu, instytucje państwowe

effectiveness of counteracting cybercrime depends on the level of legislative integration, the efficiency of institutions responsible for digital security and the ability of adaptive protection systems to dynamically changing threats in cyberspace. The research methods used include an analysis of the literature on the subject, a review of sources of national and international law.

Keywords: cybercrime, digital security, criminal law, Internet, state institutions

Wstęp

Współczesny świat, zdominowany przez technologię cyfrową i nieustanny rozwój Internetu, otwiera przed ludzkością niespotykane wcześniej możliwości komunikacji, pracy, handlu czy rozrywki. Jednocześnie jednak niesie ze sobą nowe, poważne zagrożenia. Cyberprzestępczość jako zjawisko stosunkowo nowe, lecz niezwykle dynamiczne, stała się istotnym wyzwaniem dla użytkowników indywidualnych, instytucji oraz państw.

Celem niniejszego rozdziału jest wszechstronna analiza zjawiska cyberprzestępczości: od historycznych i technologicznych uwarunkowań, przez definicyjne i klasyfikacyjne podejścia do czynów karalnych w przestrzeni cyfrowej, aż po odpowiedzi legislacyjne i instytucjonalne na poziomie krajowym i unijnym. W pierwszej części ukazano genezę i rozwój Internet jako fundament środowiska cyberprzestępczego. Druga część zawiera przegląd definicji, rodzajów cyberprzestępstw oraz metod działania sprawców, oparty o ujęcia przyjmowane przez organizacje międzynarodowe i prawo krajowe. Trzecia część koncentruje się na analizie systemu przeciwdziałania cyberprzestępczości – w tym barier prawnych, rozwiązań organizacyjnych i kierunków polityki bezpieczeństwa.

Podejście przyjęte w rozdziale ma charakter interdyscyplinarny: łączy perspektywę technologii informatycznych, prawa karnego, nauk o bezpieczeństwie i polityki publicznej. Autor opiera analizę na źródłach normatywnych, literaturze specjalistycznej oraz danych statystycznych. Całość prowadzi do wniosku, że

efektywne przeciwdziałanie cyberprzestępczości wymaga systemowej koordynacji działań międzyinstytucjonalnych, ciągłego doskonalenia przepisów prawa oraz międzynarodowej współpracy opartej na jednolitych standardach.

Geneza i rozwój Internetu jako podstawa zjawiska cyberprzestępczości

Analizując zjawisko i temat cyberprzestępczości oraz poprawne zdefiniowanie tego zjawiska, należy sięgnąć do korzeni, czyli początków powstania Internetu w Polsce i na świecie. Narodziny internatu to czas, który znacząco różni się od czasów dzisiejszych czyli współczesnego pojęcia i funkcjonowania Internetu. W tamtych czasach nie było „tradycyjnych" wyszukiwarek czy też przeglądarek internetowych, które obecnie służą nam jako niezbędne narzędzia do pozyskiwania danych czy najaktualniejszych informacji.

Ponieważ kolejne lata były ściśle powiązane z systematyczną zmianą projektową oraz nowymi koncepcjami zdalnej wymiany informacji, to z retrospektywnego punktu widzenia genezy Internetu, dość trudno i jednoznacznie wskazać jedynego twórcę tego „sieciowego wynalazku".

Początków Internetu możemy upatrywać w koncepcji połączenia ze sobą zdalnie komputerów opisanej przez Josepha Licklidera, a także w dwunastotomowej pracy napisanej przez Paula Barana dla Sił Zbrojnych Stanów Zjednoczonych w 1962 r., która zakładała stworzenie transmisji danych pomiędzy komputerami na znaczną odległość. Jednakże za faktyczny początek Internetu uznać należy powstanie pierwszych węzłów sieci nazywanych ARPANET. Ich początek datuje się na 29 października 1969 r., i rozpoczęcie eksperymentu na Uniwersytecie Kalifornijskim celem, którego było zbudowanie sieci komputerowej niemającej lokalizacji centralnej, która byłaby w stanie kierować pozostałymi podpiętymi komputerami[1]. Chodziło o taką sieć, która byłaby w stanie zachować swoje funkcjonowanie nawet w przypadku awarii lub odłączenia konkretnych elementów. Eksperyment był o tyle ważny, iż dotychczasowe sieci były sterowane za pomocą jednego komputera, co wiązało się z ryzykiem, że w przypadku jego awarii cała sieć była narażona na wyłączenie[2].

[1] J. C. R. Licklider, Man-Computer Symbiosis, https://worrydream.com/refs/Licklider_1960_-_Man-Computer_Symbiosis.pdf, [dostęp: 15.05.2025].

[2] K. Ashton, *That 'Internet of Things' Thing. In the real world, things matter more than ideas*, RFID Journal, http://www.rfid journal.com/articles/pdf?4986, [dostęp: 15.05.2025].

Pierwszym krajem, który wykorzystał koncepcję sieci rozproszonej Paula Barana, były Stany Zjednoczone. Wykorzystanie tej koncepcji było podyktowane świadomością państwa iż w przypadku ataku jako pierwszy będzie zniszczony komputer centralny. Skuteczność tej metody, okazała się na tyle progresywnym działaniem w rozwoju sieci, że stopniowo zatrudniano coraz to większą grupę naukowców do jej usprawniania.

Do końca lat 60. ubiegłego wieku funkcjonowanie sieci ARPANET było ściśle powiązane tylko z zamkniętą strukturą komputerów rządowych. Drzemiące zatem możliwości i potencjał w rozproszonej sieci dawały możliwość „wyjścia" poza potrzeby wojskowe i rządowe. Niestety pomimo wspomnianych możliwości sieci odczuwalne braki były po stronie rozbudowanych algorytmów tj. identyfikacja poszczególnych komputerów w obszarze konkretnej sieci. Było to niewątpliwym utrudnieniem w rozwoju Internetu w aspekcie globalnym[3].

Z początkiem lat 70. XX wieku, na przytoczone powyżej problemy w rozwoju sieci internetowej, przyszedł protokół TCP/IP. Był to krok milowy w rozwoju informatyzacji i sieci globalnej ogółem. TCP skupiał się na kontrolowaniu transferu danych przesyłanych za pomocą Internetu tj.: bezpośrednio z punktu A do punktu B, natomiast IP odpowiedzialne było za metodę adresowania, czyli nadanie każdemu komputerowi osobistego adresu, dzięki któremu powstała możliwość prawidłowego przesyłania danych do konkretnego komputera. Dodatkowo należy zaznaczyć, iż protokół TCP/IP, w przypadku błędu lub usterki w obszarze połączonych ze sobą komputerów w sieć, podczas przesyłania informacji taką usterkę ma możliwość ominąć i trafić do odbiorcy inną drogą. Takie zdarzenie to niezależność TCP od konkretnego ID, co tym samym zwiększa przepływ informacji oraz eliminuje opóźnienia spowodowane ewentualną awarią komputera głównego[4].

Początek lat 80. to unifikacja i stworzenie wykorzystywanego po dziś dzień systemu DNS tzn. numery IP są ściśle związane z nazwami domen internetowych.

Tuż po instytucjach wojskowych i rządowych zapotrzebowanie i „dobrodziejstwo" na ten typ i formę rozwoju technologicznego dostrzegły wyższe

[3] *Historia powstania Internetu - czyli jak narodziła się sieć?*, https://poradnikprzedsiebiorcy.pl/-historia-powstania-internetu, [dostęp: 15.05.2025].

[4] M. Mikołajewski, *Historia Internetu w pigułce Historia sieci, czyli od ARPANET-u do Internetu*, https://pclab.pl/art33917-2.html, [dostęp: 15.05.2025].

uczelnie oraz większość organizacji naukowych. Od 1989 r. Internet stał się nieodłącznym narzędziem do prac naukowych i badawczych. Siła Internetu, była na tyle mocno rozwojową stroną technologiczną, iż nie brakowało chętnych wśród społeczeństwa z segmentu prywatnego do jego wykorzystywania. Używanie Internetu do celów komercyjnych przez osoby prywatne jest możliwe po zniesieniu zakazu przez NSF (National Science Foundation) w 1991 r.

Koniec lat 90. ubiegłego wieku to powstanie pierwszej sieci dokumentów hipertekstowych o nazwie Word Wide Web, gdzie autorami był duet Tim Berners-Lee oraz Robert Cailliau, jak również stworzenie wyciąć osobiście przez Tima Bernersa-Lee pierwszego HTML-u, czyli pierwszej strony internetowej. Oczywiście strona ta nie działała tak jak obecne strony internetowe z którymi mamy do czynienia współcześnie. Ponieważ brakowało przeglądarek internetowych niektóre funkcje były bardzo mocno ograniczone.

Mosaic – to pierwsza internetowa przeglądarka, którą w 1994 r. stworzył – założyciel firmy Netscape – Marc Andressen. Firma Marca Anderessena poszła o krok dalej i stworzyła bardziej zaawansowaną przeglądarkę o nazwie Netscape Commerce S, która stała się wzorem do naśladowania dla nowych produktów internetowych. Graczami o stanowisko lidera w tym zakresie były dwie firmy, wspomniana Netscape i Microsoft. Zwycięzcą okazał się Bill Gates.Tak jak pierwsze przeglądarki, tak również pierwsze wyszukiwarki internetowe odbiegały nieco swoją konstrukcją od dzisiejszych. Pierwszą na świecie wyszukiwarkę stworzyli Alan Emtag i Peter J. Deutscha pod nazwą Archie (1990 r.). Celem Archie było bardzo szybkie wyszukiwanie plików zamieszczonych na serwerach FTP. 1993 r. to czas, kiedy pierwszy raz pojawiła się wyszukiwarka Wandex – narzędzie współpracujące bezpośrednio z odnośnikami hipertekstowymi, w następstwie czego dochodziło do odwiedzania stron internetowych za ich pośrednictwem. Twórcą tego produktu był Matthew Gray. To wydarzenie dało zielone światło do rozwoju robotów indeksujących o nazwie WWW Wanderer i rozwinięcie tej idei w przyszłości przez Google oraz Yahoo[5].

Kolejne lata to już błyskawiczny progres rozwoju sieci Internetowej. Coraz to bardziej zaawansowane narzędzia technologiczne, dawały możliwość precyzyjnego i skutecznego wyszukiwania konkretnych informacji

[5] *Historia powstania Internetu - czyli jak narodziła się sieć?*, https://poradnikprzedsiebiorcy.pl/-historia-powstania-internetu, [dostęp: 15.05.2025].

w sieci. Rozwój sieci przyniósł ze sobą większe znaczenie komunikacji a co za tym idzie różnego rodzaju komunikatorów typu: grupy dyskusyjne, blogi, fora, chaty czy serwisy społecznościowe, powodując postęp technologiczny w branży nośników informacji. Zapomniane już dzisiaj dyskietki, następnie płyty CD, DVD, Blue Ray, pendraive'y to tylko niektóre nośniki z którymi mieliśmy lub mamy do czynienia. Pokoleniu urodzonemu w latach 90. i później może się wydawać, że Internet towarzyszył ludziom od zawsze – zwłaszcza w Polsce – tymczasem to wciąż stosunkowo nowe osiągnięcie technologiczne[6].

Za pierwsze połączenie internetowe w naszym kraju, uznaje się sierpień 1991 r., kiedy to pracownik Wydziału Fizyki Uniwersytetu Warszawskiego wysłał e-mail z budynku przy ulicy Hożej. Na tamten czas należy uznać to za niezłe osiągnięcie, ponieważ dostępna prędkość Internetu niestety wynosiła tylko 9600 bit/s. Była to bardzo prosta komunikacja, nieskomplikowana, ale też pasująca do ówczesnych komputerów. Należy też wspomnieć, że Internet był narzędziem używanym tylko w niektórych miejscach np.: urzędach, firmach czy wybranych instytucjach. Zwykli obywatele nie mieli możliwości korzystania tych dobrodziejstw techniki.

Rok 1996 przyniósł ogromną rewolucję dla polskiego Internetu. W tamtym czasie Telekomunikacja Polska, największy wówczas operator telefoniczny w kraju, udostępniła numer 0-20 21 22, dzięki któremu była możliwość łączenia się z siecią przy pomocy modemu telefonicznego. Z pewnością rodzaj tego łączenia większość Polaków pamięta do dziś, gdyż przy łączeniu się z siecią towarzyszył charakterystyczny dźwięk. Największy renesans tej usługi przypada na lata 1998-2001. Mimo tego, iż szybkość połączenia wynosiła do 56 kb/s, większości użytkownikom w Polsce takie parametry nie przeszkadzały. Cieszył wówczas fakt, że sieć internetowa w ogóle działała[7].

Definicje, formy i klasyfikacje cyberprzestępczości

Od początku swojego istnienia, postępująca cyfryzacja, niemal we wszystkich dziedzinach naszego życia, przyniosła za sobą nie tylko korzyści dla codziennego egzystowania, ale również zagrożenia, wzmacniane przy tym

[6] Ł. Sarowski, *Od Internetu WEB 1.0 do Internetu WEB 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci*, Rozprawy Społeczne, 11(1), 2017, s. 34.

[7] *Historia Internetu w Polsce – Poradnik Orange*, https://www.orange.pl/poradnik/twoj-internet/historia-internetu-w-polsce/, [dostęp: 15.05.2025].

przez niezwykłą wręcz dynamikę i nieprzewidywalność rozwoju technologicznego ostatnich lat[8]. Ewolucja ta spowodowała iż przestały istnieć podziały w oparciu o bariery językowe czy granice państw, ponieważ dla każdego użytkownika Internetu światowa przestrzeń jest na wyciągnięcie ręki. Internet stał się oknem na świat, w którym każdy miał jednakowe prawa i każdy mógł się stać zarówno odbiorcą informacji, jak i ich twórcą dla innych użytkowników.

Przełom XX i XXI wieku to czas, nie tylko na świecie, ale także w Polsce, gigantycznego rozwoju zarówno komputerów, jak i sieci internetowej wraz z dostępem i użyciem technologii mobilnych.

W dzisiejszym świecie, Internet stał się nieodłącznym elementem naszego codziennego życia. Ponieważ wykorzystywany jest w wielu dziedzinach takich jak np.: banki, e-urzędy, e-zakupy czy poczta elektroniczna, z wielką trudnością przychodzi nam wyobrażenie sobie dnia bez korzystania z Internetu.

W okresie, kiedy Internet był dostępny tylko dla wąskiej grupy osób, kwestię bezpieczeństwa traktowano w sposób wybiórczy, bardziej jako problem marginalny. Dziś z uwagi na niespotykane dotychczas nasycenie wszystkich dziedzin życia nowoczesnymi technologiami, przestępczość komputerowa stanowi poważniejszy problem, a z każdym rokiem liczba przestępstw odnotowywana w policyjnych statystykach się zwiększa.[9]

W związku z coraz większym zaangażowaniem środków finansowych poprzez instytucje bankowe, a co za tym idzie wzrost kwot przelewanych elektronicznie, czy też zwiększający się obrót sklepów internetowych, portali ogłoszeniowych i aukcyjnych, tematyka zagrożeń w cyberprzestrzeni przestała być domeną wąskiej grupy specjalistów, stając się niebudzącym wątpliwości istotnym problemem współczesnego świata.[10]

Stanisław Lem, w książce pt.: „Bomba megabitowa" stwierdził, że „Zjawisko Internetu przypomina poniekąd znany nam potop, czyli nadmiar wód, w którym można ze wszystkim utonąć, jeżeli nie zdołamy dla ratunku, jak Noe, zbudować sobie Arki. Ale jakby miała wyglądać Arka Noego dla Internetu…?"[11].

---

[8] C. Banasiński (red.), *Cyberbezpieczeństwo – Zarys Wykładu*, Wolters Kluwer, Warszawa 2023, s. 15.

[9] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik Policyjny, Nr 4/2017, s. 20.

[10] C. Banasiński (red.), *Cyberbezpieczeństwo…*, op. cit., s. 15.

[11] G. Szpor, A. Gryszczyńska, *Internet – Strategie bezpieczeństwa*, Wydawnictwo C.H Beck, Warszawa 2017, s. 31.

Wyjaśnijmy zatem jaka jest definicja cyberprzestępczości. Co ona oznacza i jak ją mamy rozumieć w dzisiejszym świecie.

W latach 60. XX w., wraz z rozwojem nowych technologii i ich wykorzystywaniem w celach przestępczych pojawiła się potrzeba określenia grupy czynów polegających na posługiwaniu się komputerem do naruszania dóbr prawnych tradycyjnie chronione przez prawo karne. W literaturze przedmiotu opisując to zjawisko, zaczęto posługiwać się takimi pojęciami jak „przestępczość komputerowa" lub „przestępstwa związane z wykorzystaniem komputera". Od początku pojawienia się tych terminów wskazywano na liczne wątpliwości, co do ich zakresu znaczeniowego[12].

Z punktu widzenia cybernetyki oraz teorii informacji[13] termin ten definiowany jest jako „zbiór faktów", zdarzeń, cech itp., określonych obiektów (rzeczy, procesów systemów) zawartych w wiadomościach (komunikacie), tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne"[14]. W ujęciu tym informacja jest pojęciem ściśle związanym z człowiekiem i zdolnością jego celowego działania[15].

W myśl definicji opracowanej i zamieszczonej w „Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" przyjętej w dniu 25 czerwca 2013 r. w drodze uchwały przez Radę Ministrów, cyberprzestępstwo stanowi czyn zabroniony popełniony w obszarze cyberprzestrzeni, czyli przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[16] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[17].

---

[12] M. Siwicki, *Monografie Prawnicze – Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 10.

[13] T. Szewc, *Publicznoprawna ochrona informacji*, Wydawnictwo C. H. Beck, Warszawa 2007, s. 4.

[14] J. Petzel, *Informatyka prawnicza, Zagadnienia Teorii i praktyki*, Wydawnictwo Liber, Warszawa 1999, s. 35

[15] C. Banasiński (red.), *Cyberbezpieczeństwo…*, op. cit., s. 22.

[16] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 11 października 2024 r. w sprawie ogłoszenia jednolitego tekstu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557).

[17] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Komitet Stały Rady Ministrów, 25 czerwca 2013 r.

Interpol definiuje i określa cyberprzestępczość w dwóch ujęciach. Pierwsze z nich to wertykalnym a drugie horyzontalne. Ujęciem wertykalnym można nazwać przestępstwa specyficzne dla cyberprzestrzeni, czyli takie, które tylko tam mogą być dokonane, np. hacking czy sabotaż komputerowy. Z kolei w ujęciu horyzontalnym zakłada się popełnianie przestępstw za pomocą technik komputerowych (np. oszustwa komputerowe, fałszowanie pieniędzy, pranie brudnych pieniędzy itp.)[18].

Z przyjętej konwencji Rady Europy dotyczącej przedmiotu cyberprzestępczości[19] zjawisko to można określić jako, umyślny i bezprawny dostęp do całości lub części systemu informatycznego, umyślne i bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne, umyślne i bezprawne niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych, poważne zakłócenia funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych, produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw lub hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw[20].

Przyjęta konwencja wyróżnia rodzaje przestępstw m.in.: przeciwko poufności, integralności oraz dostępności danych informatycznych. Do przestępstw komputerowych zalicza się fałszerstwo i oszustwo komputerowe jak również mamy do czynienia z przestępstwami ze względu na charakter zawartych informacji i naruszeniem praw autorskich.

---

[18] *Przestępstwa komputerowe – Prawo karne - kodeks karny, oskarżony przed sądem, świadek, ofiara przestępstwa*, http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe, [dostęp: 15.05.2025].

[19] Dz. U. z 2015 r. poz. 728.

[20] M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik Policyjny, Nr 4/2017, s. 20.

Wg Unii Europejskiej definicję cyberprzestępczości – Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. „W kierunku ogólnej strategii zwalczania cyberprzestępczości" – należy interpretować jako odniesienie do trzech rodzajów przestępstw. Pierwsze odniesienie ukierunkowane jest na tradycyjne formy przestępstw np.: oszustwo czy fałszerstwo, jednak w aspekcie cyberprzestępczości dotyczą one konkretnych przestępstw popełnionych przy użyciu elektronicznych sieci informatycznych oraz systemów informatycznych. Drugi rodzaj przestępstw dotyczy nielegalnych publikacji treści w mediach elektronicznych. Za przykład możemy tu podać materiały związane z pornografią dziecięcą czy też nawoływaniem do ksenofobi. Trzeci rodzaj przestępstw można uznać za przestępstwa natury technicznej, ponieważ dotyczą typowo sieci łączności elektronicznej. To tej grupy przestępstw można zaliczyć ataki przeciwko systemom informatycznym, hakerstwo lub ataki typu DOS. Tego typu ataki są bardzo dobrze zorganizowane, a ich celem jest wymuszenie[21].

Definicję cyberprzestępczości w ujęciu wąskim i szerokim przyjął X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców. Zgodnie z przyjętymi zapisami wg ONZ, pojęcie cyberprzestępstwa w wąskim ujęciu to wszelkie nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzonych przeciw bezpieczeństwu systemów komputerowych lub też procesowanych przez te systemy danych.

Cyberprzestępstwo w szerokim sensie, czyli przestępstwo dotyczące komputerów, to takie, które dotyczy wszelkich nielegalnych działań popełnionych za pomocą lub dotyczących systemów lub sieci komputerowych, włączając w to między innymi bezprawne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[22].

Istotny jest jednak nie tyle spór definicyjny o istotę pojęcia cyberprzestępstwa, ile fakt, że rozwój technologii informacyjnych i komunikacyjnych oraz ich współczesna powszechność spowodował wyjątkową łatwość i swobodę dystrybucji, dostępu i wymiany informacji[23].

---

[21] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów „W kierunku ogólnej strategii zwalczania cyberprzestępczości" 22 maja 2007 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267, [dostęp: 15.05.2025].

[22] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010, s. 55.

[23] C. Banasiński (red.), *Cyberbezpieczeństwo…,* op. cit., s. 22.

Cyberprzestępczość przybrała wiele form i rodzajów działania. Pierwsza kategoria to przestępstwa typowe dla cyberprzestępczości, czyli takie, których celem jest bezpośredni atak na komputer lub też globalne przetwarzanie danych w systemach informatycznych. Do tej grupy można zaliczyć: fałszywe profile, hakowanie (hacking), czyli bezprawne uzyskanie informacji, podawanie się za inną osobę, sniffing, czyli podsłuch komputerowy, udaremnienie uzyskania informacji, sabotaż komputerowy, rozpowszechnianie złośliwych programów, oszustwa komputerowe czy też stosowanie narzędzi hackerskich[24].

Do drugiej kategorii cyberprzestępstw należy zaliczyć przestępstwa dotyczące wykorzystania typowo sieci internetowej a komputer jest jedynie środkiem do jego popełnienia. Typowe działania tej grupy cyberprzestępstw to m.in.: obraza uczuć religijnych, publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim, faszystowskim lub innym totalitarnym ustroju danego państwa oraz nawoływanie do nienawiści, na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość, czyli szeroko rozumiana mowa nienawiści. Handel fikcyjnymi kosztami, zbywanie własnego lub cudzego dokumentu stwierdzającego tożsamość tzw.: przestępstwa przeciwko wiarygodności dokumentów, oszustwa popełniane za pośrednictwem portali aukcyjnych[25].

Jak podaje w Monogramie Prawniczym Maciej Siwicki, cyberprzestępczość można podzielić na trzy generacje. Pierwsza z nich obejmowała głównie naruszenia integralności systemów komputerowych i modyfikację znajdujących się tam danych na skutek wprowadzenia programów określanych jako „wirus" lub „robak". Druga generacja cyberprzestępstwa była ściśle związana z rozwojem sieci teleinformatycznych i atakami przez hakerów na bezpieczeństwo elektroniczne przetwarzanych tam informacji. Trzecia generacja cyberprzestępczości jest związana z zauważalnym procesem „automatyzacji" cyberprzestępczości, będącej m.in. efektem wykorzystania złośliwego oprogramowania i bitnetów. Generację tą charakteryzuje niskie prawdopodobieństwo wykrycia sprawcy oraz zorganizowane struktury przestępcze, skupione wokół tzw.: „podziemia komputerowego"[26].

Nowa generacja cyberprzestępstw to zautomatyzowane, rozproszone ataki przeprowadzone z wykorzystaniem napisanego w tym celu

[24] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 21.

[25] Ibidem.

[26] M. Siwicki, *Monografie Prawnicze – Cyberprzestępczość…*, op. cit., s. 1.

oprogramowania, które mają również charakter transgraniczny, co jest szczególnym utrudnieniem w ściganiu sprawców i zabezpieczaniu dowodów, jak również wymusza międzynarodową współpracę i koordynację podejmowanych działań[27].

Rosnący zakres działań cyberprzestępców to nie tylko ataki na globalne spółki, systemy bankowe, włamania do instytucji finansowych i podmiotów publicznych na całym świecie – w tym również w Polsce, ale ataki te mogą być również ukierunkowane na pozyskanie informacji, wpływanie na decyzje o charakterze strategicznym lub nastroje społeczne oraz powodowanie destabilizacji zarówno politycznej, jak i gospodarczej. Przykładem takiego ataku może być - ostatnio bardzo popularne narzędzie polityczne: fake news. Kampanie dezinformacyjne oraz ataki na infrastrukturę informacyjną są bardzo ważnym elementem wojny hybrydowej. Okazuje się zatem, że polityka w dzisiejszych czasach do „dziedzina, w której Internet może się przyczynić do zła o wiele szybciej, łatwiej, pewniej, aniżeli do dobra"[28].

Wg aktualnych szacunków, ogólna wartość globalnych strat poniesionych na skutek występowania cyberprzestępstw obecnie, porównywalna jest do wartości całego rynku narkotykowego, plasując się na poziomie około 388 miliardów dolarów rocznie[29].

Z danych policyjnych wynika, że rocznie ilość osób, które padły ofiarą różnej formy cyberprzestępstwa jest niemal pół miliarda ludzi na świecie, co za tym idzie średnio prawie 14 ofiar bezprawnej aktywności na sekundę. Polska niestety nie jest wyjątkiem. Według danych Policji, w Polsce w 2010 r. zgłoszono prawie 8 tys. cyberprzestępstw, z czego ponad 6 tys. przypadków to oszustwa[30]. Na rok 2012 przypada 19 tys. zgłoszonych przestępstw komputerowych w Polsce, z czego blisko 75% to przypadki oszustw. W 2015 r. liczba odnotowanych w naszym kraju cyberprzestępstw przekroczyła gigantyczny poziom, bo aż dwadzieścia tysięcy. Należy tu zaznaczyć, iż ogromna

[27] G. Szpor, A. Gryszczyńska, *Internet – Strategie bezpieczeństwa*, Wydawnictwo C.H Beck, Warszawa 2017, s. 31-32.

[28] S. Lem, *Bomba megabitowa*, Kraków 1999, s. 13-14.

[29] *Norton Cybercrime Report 2011*, http://pl.norton.com/cybercrimereport, [dostęp: 15.05.2025].

[30] Statystyka Policyjna, http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html, [dostęp: 15.05.2025].

liczba cyberprzestępstw pozostaje zamaskowana w szarej strefie, wymykając się obliczeniom statystycznym[31].

Polska cyberprzestępczość charakteryzuje się głównie tym, iż czyny przestępcze popełniane są w większości z wykorzystaniem Internetu. Wynika to z faktu, iż w dużej mierze ma na to wpływ duży progres postępu technologicznego, coraz łatwiejszy i obciążony niskimi kosztami dostęp do Internetu, uruchamianie coraz większej ilości hot spotów z anonimowym i darmowym dostępem do sieci czy też zwiększająca się z roku na rok liczba komputerów i urządzeń mobilnych. Inny czynnik, który ma na ten proceder wpływ to „komfort przestępcy". Przestępca nie musi angażować całej armii ludzi i sił, jak również środków finansowych, tak jak to się odbywa w rzeczywistości. Będąc aktywnym użytkownikiem komputera w domu, za pomocą kilku kliknięć jest w stanie dokonać oszustwa, wymienić się materiałami o naturze pedofilskiej lub też dokonać wpisu typu fake news szkalującego i obrażającego inną osobę[32].

Intensywna działalność cyberprzestępców – szczególnie w XXI w., to dla władz wielu państw bardzo poważny problem. Od dawna kraje te poszukują konkretnych rozwiązań – prawnych i technologicznych – które w sposób skuteczny pomogłyby w walce z przestępczością komputerową. Nasz kraj nie jest wyjątkiem. Efektywne ściganie przestępców komputerowych napotyka na co dzień wiele trudności. Pokonanie tych trudności jest konieczne do prawidłowego i pozytywnego zakończenia całego procesu wykrywczego, a co za tym idzie, ostatecznie ukarania sprawcy[33]. Jedną z przyczyn, która ma bezpośredni wpływ na utrudnienie, czasami wręcz uniemożliwiające skuteczne ściganie cyberprzestępstw jest fakt, że obowiązujące prawo w dużej mierze nie nadąża za bardzo szybkimi zmianami. Błyskawiczny progres zmian następuje zarówno w codziennej egzystencji, jak również w sieci Internetowej. Kolejną przyczyną, o której informują służby prawne i policyjne kraju, to – można powiedzieć- „konflikt" między wprowadzanymi zmianami w obowiązujących przepisach prawnych, które z założenia chronią wolność obywatelską, ale

[31] M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, Czasopismo Prawa Karnego i Nauk Penalnych, z. 1, 2000.

[32] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 23.

[33] *Prezydent RP: Cyfrowe zagrożenia na liście kluczowych problemów*, https://www.bbn.gov.pl/pl/wydarzenia/8326,Prezydent-RP-Cyfrowe-zagrozenia-na-liscie-kluczowych-problemow.html?search=51534879342831, [dostęp: 15.05.2025].

niestety mają znaczący wpływ na „zakłócenia" w podjęciu niezbędnych czynności przez organy ścigania[34].

Jako przykład wspomnianego „konfliktu" może być podana ustawa z dnia 16 lipca 2004 r.: Prawo telekomunikacyjne[35], w której wprowadzona nowelizacja w styczniu 2013 roku skróciła okres przechowywania istotnych dla organów ścigania danych tzw.: retencyjnych z 24 miesięcy do 12. Dodatkowo, skutkiem wprowadzonych zmian w tej ustawie, wszystkie bazy z danymi starsze niż 12 miesięcy, zaczynając liczenie od daty wejścia w życie nowych zapisów, zostały usunięte przez operatorów, a dostęp do nich stał się zupełnie niemożliwy.

Pozytywną i jak na razie jedyną zmianą w przedmiotowej ustawie, która ułatwia ściganie cyberprzestępców, jest wprowadzony w połowie 2016 r., nawiązujący do ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[36], obowiązek rejestracji u polskich operatorów wszystkich kart SIM, które działają w systemie prepaid.

Niestety dla osób zajmujących się „fachową" cyberprzestępczością, to tylko niewielka przeszkoda techniczno-prawna. Bez większego wysiłku, cyberprzestępcy mogą pozyskać przez sieć – najczęściej z portali aukcyjnych lub też sklepów internetowych – kartę SIM od zagranicznych operatorów, na których nie spoczywa obowiązek takiej rejestracji, lub też mają możliwość kupienia karty SIM z tzw.: „drugiego obiegu", którą rejestrują na tzw.: „słupa".

Kolejną nieprecyzyjną pozycją prawną jest ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[37], w której brakuje doprecyzowania zapisów dotyczących okresu retencji danych. Dane, które usługodawca jest zobligowany do gromadzenia, zbierania i przechowywania uzależnione jest od potencjału finansowego firmy i „dobrych chęci" przez dowolny okres – może to być rok, pół lub miesiąc czy tylko tydzień.

Efektem takich nieprecyzyjnych zapisów prawnych są bezpowrotnie utracone dane, które w całym procesie wykrywania cyberprzestępczości mają

[34] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 23.

[35] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800).

[36] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2016 r. poz. 904).

[37] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204).

olbrzymie znaczenie dla prowadzonych postępowań i niejednokrotnie stanowią jedyną podstawę i kierunek prowadzenia dalszych czynności operacyjnych[38].

Regulacje prawne i instytucjonalna odpowiedź na cyberzagrożenia

Kolejnym „zielonym światłem" dla cyberprzestępców jest możliwość korzystania z anonimowego dostępu do Internetu, który realizowany jest poprzez wykorzystanie punktów darmowego dostępu do Internetu tzw.: hotspot.

Znaczącą trudnością w zwalczaniu cyberprzestępczości są również różnice legislacyjne pomiędzy krajami. Wydłuża to lub uniemożliwia błyskawiczne ustalenie sprawcy. Dzieje się tak dlatego, iż składane wnioski o ściganie przestępców, które trafiły do tamtejszych sądów, rozpatrywane są według litery prawa, obowiązującej w danym kraju. W sytuacji, gdy w danym państwie czyn nie stanowi przestępstwa, zamknięta jest droga prawna do wydania takich danych. Najczęściej wnioski te są rozpatrzone negatywnie. Zjawisko takie ma destrukcyjny wpływ na szybkie wykrycie sprawcy, gdyż jak wiadomo w tego typu procederze czas jest kluczem do sukcesu. Transgraniczność sieci internetowej, to kolejne istotne utrudnienie dla organów ścigania[39]. Polega to na bardzo łatwym dostępie do usług świadczonych przez firmy zarejestrowane poza granicami kraju. Taka sytuacja wymusza prowadzenie innych- dodatkowych czynności operacyjnych, angażując przy tym organy ścigania innych państw[40].

Pierwszym krajem na świecie, który wprowadził do swojego systemu prawnego karalność przestępczości komputerowej były Stany Zjednoczone. Pierwszymi przepisami stanowymi w USA, których celem było przeciwdziałanie przestępczości komputerowej były przepisy karne stanu Floryda, które datuje się na 1 sierpnia 1978 r. Na wzór Florydy podobne rozwiązanie przepisów prawnych zostało wprowadzone w stanie Arkansas, West Virginia i rok 1989 oraz Maine i rok 1990 to stany, które jako ostanie przyjęły podobne rozwiązania prawne. Zderzając ze sobą przepisy stanowych kodeksów karnych,

[38] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s. 23.

[39] *Raport Cyberbezpieczeństwo A.D. 2018*, NASK – Państwowy Instytut Badawczy, Warszawa 2019, https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpieczeństwo-A.D.-2018.pdf, [dostęp: 15.05.2025].

[40] M. Stefanowicz, *Cyberprzestępczość…,* op. cit., s.24.

których przedmiotem jest przestępczość komputerowa, można łatwo stwierdzić, że różnią się one nie tylko ilością zamieszczonych artykułów, i ich treścią, lecz również zakresem dyspozycji i sankcji, które są przewidziane za ten sam czyn przestępny. Przykładem tego rozwiązania są przepisy Texas Penal Code – teksańskiego kodeksu karnego. O rodzaju przestępstwa drugiego czy trzeciego stopnia albo czy czyn taki jest występkiem, decyduje wartość powstałej szkody[41].

Przenosząc temat na obszar europejski, nie bez znaczenia – iż pomimo pozytywnej działalności przez pierwszy rok Europejskiego Centrum ds. Walki z Cyberprzestępczością, którego głównym zadaniem jest wspieranie, a w przypadku potrzeby również koordynowanie operacji dochodzeniowych prowadzonych przez państwa członkowskie[42], jest raport przygotowany przez Business Software Alliance (BSA) pt.: „European CyberSecurity Dashboard", opublikowany w marcu 2015 r.[43], w którym zwrócono szczególną uwagę na braki w cyberbezpieczeństwie UE. Braki te wynikały głównie z różnic politycznych, zapisów prawnych, jak również potencjału państw członkowskich.

Choć początki aktywności Unii Europejskiej w obszarze cyberbezpieczeństwa przypadają na rok 1997, „kiedy to Parlament wraz z Radą UE wydały dyrektywę w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym"[44], możliwości UE w obszarze prawa karnego były bardzo mocno ograniczone, natomiast wydawane dyrektywy bardzo rzadko nawiązywały do prawnokarnych środków ochrony. Wraz z wejściem w życie Traktatu z Lizbony[45], sytuacja ulegała zmianie. Przepisy prawa karnego stały się osobnym zakresem współpracy międzynarodowej. Artykuły od 82 do 86 Traktatu o Funkcjonowaniu Unii Europejskiej upoważniają Unię do ujednolicenia przepisów prawa karnego. Na szczególną uwagę zasługuje

[41] C. Banasiński (red.), *Cyberbezpieczeństwo…,* op. cit., s. 45.

[42] Komisja Europejska - Komunikat Prasowy: Europejskie Centrum ds. Walki z Cyberprzestępczością - pierwszy rok działalności.

[43] European CyberSecurity Dashboard and 28 Country Reports Launched - 3 March 2015.

[44] Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (97/66/WE).

[45] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r. (Dz. U. z 2009 r. Nr 203, poz. 1569).

potrzeba przeciwdziałania przestępczości ukierunkowanej na transgraniczność jak również współpraca w zakresie ich zwalczania[46].

Obecnie podstawy prawne cyberbezpieczeństwa w Unii Europejskiej są silnie zintegrowane z dokumentami programowymi, które stanowią „przedwiośnie" określonych regulacji prawnych na poziomie europejskim, albo też stanowią ich uzupełnienie o działania je wspomagające. Wyrazem tego podejścia jest Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa UE,[47] zastępująca Europejską Strategię Bezpieczeństwa z 2003 r. Strategia ta o tyle jest istotna, że określa priorytety działań zewnętrznych UE, którymi są: bezpieczeństwo, odporność państwa i społeczeństwa, zintegrowane podejście do konfliktów i kryzysów, wspieranie współpracy regionalnej oraz zarządzanie globalne w XXI wieku.[48] W przedmiotowej strategii wskazano konieczność wzmocnienia cyberbezpieczeństwa w drodze zwiększenia odporności infrastruktury krytycznej i sieci przesyłowych, walki z cyberprzestępczością, a przede wszystkim poprzez włączenie kwestii związanych z tym obszarem w inne polityki unijne oraz zacieśnienie współpracy między państwami członkowskimi, a także USA i NATO[49].

Punktem zwrotnym na rzecz zintegrowanego podejścia do problematyki cyberbezpieczeństwa była Europejska agenda cyfrowa, która była elementem przyjętej przez Komisję Strategii „Europa 2020" i zakłada, że technologie informacyjno-komunikacyjne powinny pełnić podstawową funkcję rozwojową – jeśli Europa za cel obrała realizację swoich ambitnych założeń do 2020 r. W strategii „Europa 2020" wyraźnie zwrócono bowiem uwagę na znaczenie upowszechnienia szeroko pasmowego Internetu, co ma sprzyjać włączeniu społecznemu i konkurencyjności gospodarki UE[50].

W Polsce, pierwsze próby dostosowania obowiązujących norm prawnych do zwalczania cyberprzestępczości, zostały podjęte w połowie lat 90

---

[46] Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE z 2012 r. C 326/47).

[47] *List Prezydenta na IV Europejskie Forum Cyberbezpieczeństwa* Cybersec, https://www.prezydent.pl/aktualnosci/wypowiedzi-prezydenta-rp/inne/art,826,list-prezydenta-na-iv-europejskie-forum-cyberbezpieczenstwa-cybersec-.html, [dostęp: 15.05.2025].

[48] *Notatka BBN nt. Europejskiej Agendy Bezpieczeństwa na lata 2015-2020***,** https://www.bbn.gov.pl/pl/wydarzenia/6721, NOTATKA-BBN-Europejska-Agenda-Bezpieczenstwa-na-lata-2015-2020.html?search=43892397, [dostęp: 15.05.2025].

[49] M. Wróblewska-Łysik, *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Bezpieczeństwo Narodowe, 1-4, 2016, s. 67.

[50] C. Banasiński (red.), *Cyberbezpieczeństwo…*, op. cit., s. 45-46.

XX wieku. Do chwili obecnej zapisy prawa karnego wciąż poddawane są nowelizacjom[51].

Zgodnie z obowiązującym stanem prawnym, w Polsce to Minister Cyfryzacji odpowiada za zapewnienie minimalnych wymagań w zakresie bezpieczeństwa teleinformatycznego w administracji publicznej. Wynika to wprost z ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne*[52] oraz mówi o tym rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[53].

2015 r. to zatwierdzenie przez Ministra Cyfryzacji *Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych.* Celem zatwierdzonego dokumentu jest gwarancja wsparcia przeprowadzenia kontroli działania systemów teleinformatycznych, które używane są do realizacji zadań publicznych – w tym również wymagań w obszarze bezpieczeństwa informacji.

Podjęcie prac kompleksowego uregulowania krajowego systemu cyberbezpieczeństwa w Polsce,[54] wynikało z potrzeby zapewnienia podejścia systemowego do krajowego systemu cyberbezpieczeństwa, jak również potrzeby systematycznego wdrażania do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady 2016/1148/UE[55].

Analizując temat cyberprzestępczości, należy tu zaakcentować fakt powstania w Polsce pewnego rodzaju instytucji z wyznaczonymi konkretnymi zadaniami, jakim jest Biuro do Walki z Cyberprzestępczością. Powstało ono 1 grudnia 2016 r. Głównymi zadaniami nowo powstałej jednostki są

---

[51] M. Siwicki, *Cyberprzestępczość*, wyd. C.H. Beck, Warszawa 2013, s. 25.

[52] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565).

[53] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526).

[54] Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL 2017, https://www.bbn.gov.pl/pl/wydarzenia/7865,Polskie-Forum-Cyberbezpieczenstwa-CYBERSEC-PL-2017.html?search=51534879342831, [15.05.2025].

[55] Uzasadnienie do Uchwały Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

„zadania związane z tworzeniem warunków do efektywnego wykrywania sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych”[56].

Do zadań Biura do Walki z Cyberprzestępczością należą w szczególności takie zadania jak: „… nadzorowanie, koordynowanie i wspieranie ukierunkowanych na zwalczanie cyberprzestępczości działań prowadzonych przez komendy wojewódzkie (Stołeczną) Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałanie z Centralnym Biurem Śledczym Policji w tym zakresie, prowadzenie czynności operacyjno-rozpoznawczych pozostających we właściwości biura, inicjowanie i prowadzenie współpracy z organami administracji rządowej, sądami, prokuraturami, instytucjami państwowymi, a także podmiotami prywatnymi w zakresie zadań pozostających we właściwości biura, prowadzenie współpracy międzynarodowej oraz współdziałanie z Biurem Międzynarodowej Współpracy Policji w zakresie zadań pozostających we właściwości biura, prowadzenie całodobowej służby mającej na celu koordynowanie działań Policji w zakresie zagrożeń przestępstwami w sieci Internet, ich zwalczania oraz współdziałania jednostek organizacyjnych Policji z krajowymi i zagranicznymi organami i podmiotami pozapolicyjnymi, prowadzenie konsultacji technicznych, inicjowanie i wspieranie badań oraz projektów, a także współpraca z podmiotami krajowymi i zagranicznymi zmierzająca do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z cyberprzestępczością…”[57].

W 2017 r. w kwietniu, uchwałą nr 52/2017 Rady Ministrów przyjęty został dokument strategiczny dotyczący bezpieczeństwa cyberprzestrzeni w postaci Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.[58] Dokument ten to efekt prac zespołu międzyresortowego pod kierunkiem Ministerstwa Cyfryzacji. Jednym z głównych zadań wskazanych w KRPC jest osiągnięcie jak najwyższego poziomu odporności krajowych systemów teleinformatycznych[59]. Dotyczy to świadczenia usług kluczowych, usług cyfrowych oraz usług administracji publicznej. Koncepcją jest

[56] http://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html

[57] http://policja.pl/pol/kgp/bwc/33358,Biuro-do-Walki-z-Cyberprzestepczoscia.html

[58] Notatka BBN nt. Europejskiej Agendy Bezpieczeństwa na lata 2015-2020.

[59] „*Pięć żywiołów. Wolność – informacja – bezpieczeństwo” – wystąpienie Szefa BBN*, https://www.bbn.gov.pl/pl/wydarzenia/5631,Piec-zywiolow-Wolnosc-informacja-bezpieczenstwo-wystapienie-Szefa-BBN.html?search=43892397, [dostęp: 15.05.2025].

rozbudowa krajowego systemu cyberbezpieczeństwa w takiej formie, aby mógł być on „ukierunkowany na zbudowanie zdolności w zakresie bieżącego monitorowania zagrożeń oraz zarządzania cyberbezpieczeństwem w skali kraju”[60].

Przedstawione działania, podjęte przez Ministerstwo Cyfryzacji we współpracy z innymi resortami podyktowane były zmianą ustawy o działach administracji rządowej w grudniu 2015 r.[61], jak również zaleceniami pokontrolnymi skierowanymi do byłego Ministerstwa Administracji i Cyfryzacji, w związku z przeprowadzoną kontrolą przez NIK w 2014 r., która dotyczyła instytucji publicznych odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.

Na obecną chwilę polski system prawny nie posiada przepisów, które regulują szczegółowo zagadnienia dotyczące cyberbezpieczeństwa w dziedzinach objętych zakresem dyrektywy PE i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE. Niektóre elementy o charakterze bezsankcyjnym, które wprost odnoszą się do regulacji wymagań bezpieczeństwa teleinformatycznego infrastruktury krytycznej, zostały zawarte w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK).

Wizja cyberbezpieczeństwa Polski, o której można przeczytać w załączniku do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. dot. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, „Polska będzie krajem bardziej odpornym na ataki i zagrożenia płynące z cyberprzestrzeni. Dzięki synergii działań wewnętrznych i międzynarodowych cyberprzestrzeń RP stanowić będzie bezpieczne środowisko umożliwiające realizowanie wszystkich funkcji państwa i pozwalać na pełne wykorzystywanie potencjału gospodarki cyfrowej, przy równoczesnym poszanowaniu praw i wolności obywateli”[62].

Z założeń przedmiotowej ustawy wynika, że Polska będzie krajem dążącym do kontynuacji dyskursu dotyczącego sprawnie funkcjonujących systemów międzynarodowych zarządzanych przez globalną sieć oraz zagadnień

[60] Uzasadnienie do Uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

[61] Ustawa z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. z 2015 r. poz. 2281).

[62] Załącznik do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. dot. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, s. 8, 25.

związanych z prawną oceną cyberataków. Dyskusja ta będzie miała na celu wypracowanie spójnych rozwiązań, które gwarantują pewność międzynarodowej wymiany informacji w Internecie. Ustawa zakłada iż Polska będzie angażować się we wzmacnianie środków budowy bezpieczeństwa i zaufania „w ramach istniejących forów międzynarodowych, w tym OBWE. Rząd będzie włączał się również w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym".

Podsumowanie

Cyberprzestępczość jest jednym z największych wyzwań współczesnego świata cyfrowego. Jej dynamiczny rozwój idzie w parze z postępem technologicznym, co sprawia, że coraz trudniej jest skutecznie się przed nią bronić. Jednocześnie jednak istnieją coraz bardziej zaawansowane metody przeciwdziałania zagrożeniom płynącym z sieci – od nowoczesnych systemów bezpieczeństwa, przez odpowiednie regulacje prawne, po rosnącą świadomość użytkowników. Skuteczna walka z cyberprzestępczością wymaga współpracy międzynarodowej, inwestycji w edukację oraz ciągłego dostosowywania środków ochronnych do zmieniających się realiów cyfrowych. Tylko w ten sposób możliwe będzie bezpieczne korzystanie z dobrodziejstw nowoczesnych technologii bez obaw o utratę danych, prywatności czy reputacji.

Z przeprowadzonych rozważań wynika, że kluczowym problemem w skutecznym przeciwdziałaniu cyberprzestępczości pozostaje niedostosowanie obowiązujących systemów prawnych do szybko ewoluujących form działalności przestępczej w sieci. Istotnym utrudnieniem jest także ograniczona skuteczność działań instytucji państwowych, wynikająca z braku jednoznacznych procedur, zbyt krótkiego okresu przechowywania danych oraz transgranicznego charakteru przestępstw, który wymaga ścisłej współpracy międzynarodowej.

Wnioskiem zasadniczym jest potrzeba przyjęcia podejścia systemowego, opartego na trzech filarach: harmonizacji prawa na poziomie krajowym i unijnym, wzmacnianiu kompetencji instytucji zajmujących się cyberbezpieczeństwem oraz ciągłej edukacji i uświadamianiu użytkowników sieci co do skali i form zagrożeń. Tylko przy zaangażowaniu wszystkich tych elementów możliwe jest ograniczenie skali cyberprzestępczości oraz zwiększenie

poziomu ochrony informacji, prywatności i interesów państwa w środowisku cyfrowym.

Literatura

1. Banasiński C. (red.), *Cyberbezpieczeństwo – Zarys Wykładu*, Wolters Kluwer, Warszawa 2023.
2. Dyrektywa Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym (97/66/WE).
3. European CyberSecurity Dashboard and 28 Country Reports Launched – 3 March 2015.
4. Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe*, Czasopismo Prawa Karnego i Nauk Penalnych, z. 1, 2000.
5. Komisja Europejska – Komunikat Prasowy: Europejskie Centrum ds. Walki z Cyberprzestępczością – pierwszy rok działalności.
6. Lem S., *Bomba megabitowa*, Kraków 1999.
7. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 24 lutego 2017 r. w sprawie ogłoszenia jednolitego tekstu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz. U. z 2017 r. poz. 570, z późn. zm.
8. Petzel J., *Informatyka prawnicza. Zagadnienia Teorii i praktyki*, Wyd. Liber, Warszawa 1999.
9. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Komitet Stały Rady Ministrów, 25 czerwca 2013 r.
10. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Dz.U. 2012 poz. 526.
11. Sarowski Ł., *Od internetu WEB 1.0 do internetu WEB 4.0 – ewolucja form przestrzeni komunikacyjnych w globalnej sieci*, Rozprawy Społeczne, 11(1), 2017.
12. Siwicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013.
13. Siwicki M., *Monografie Prawnicze – Cyberprzestępczość*, wyd. C.H. Beck, Warszawa 2013.
14. Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, Kwartalnik Policyjny Nr 4/2017.
15. Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010.
16. Szewc T., *Publicznoprawna ochrona informacji*, wyd. C. H. Beck, Warszawa 2007.
17. Szpor G., Gryszczyńska A., *Internet – Strategie bezpieczeństwa*, wyd. C.H Beck, Warszawa 2017.
18. Traktat o funkcjonowaniu Unii Europejskiej, Dz.Urz. UE 2012, C 326/47.

19. Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13 grudnia 2007 r., Dz.U. 2009 nr 203, poz. 1569.
20. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Dz.U. 2004 nr 171 poz. 1800.
21. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych. Dz.U. 2016 poz. 904.
22. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002 nr 144 poz. 1204.
23. Ustawa z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw. Dz.U. 2015 poz. 2281.
24. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005 nr 64 poz. 565.
25. Uzasadnienie do Uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.
26. Wróblewska-Łysik M., *Europejska Strategia Globalna a możliwości współpracy Unii Europejskiej z NATO po szczycie w Warszawie*, Bezpieczeństwo Narodowe, 1-4, 2016.
27. Załącznik do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. dot. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

Netografia

1. Ashton K., *That 'Internet of Things' Thing. In the real world, things matter more than ideas*, „RFID Journal", http://www.rfid journal.com/articles/pdf?4986.
2. *Historia powstania Internetu – czyli jak narodziła się sieć?*, https://poradnikprzedsiebiorcy.pl/-historia-powstania-internetu.
3. *Historia Internetu w Polsce – Poradnik Orange*, https://www.orange.pl/poradnik/twoj-internet/historia-internetu-w-polsce/.
4. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów „W kierunku ogólnej strategii zwalczania cyberprzestępczości" 22 maja 2007 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267.
5. Licklider J. C. R., *Man-Computer Symbiosis*, https://worrydream.com/refs/Licklider_1960_-_Man-Computer_Symbiosis.pdf.
6. List Prezydenta na IV Europejskie Forum Cyberbezpieczeństwa Cybersec, https://www.prezydent.pl/aktualnosci/wypowiedzi-prezydenta-rp/inne/art,826,list-prezydenta-na-iv-europejskie-forum-cyberbezpieczenstwa-cybersec-.html.
7. *Norton Cybercrime Report 2011*, http://pl.norton.com/cybercrimereport.
8. Notatka BBN nt. Europejskiej Agendy Bezpieczeństwa na lata 2015-2020, *Pięć żywiołów. Wolność – informacja – bezpieczeństwo* – wystąpienie Szefa BBN, https://www.bbn.gov.pl/pl/wydarzenia/5631,Piec-zywiolow-Wolnosc-informacja-bezpieczenstwo-wystapienie-Szefa-BBN.html?search=43892397.

9. Mikołajewski M., *Historia Internetu w pigułce Historia sieci, czyli od ARPA-NET-u do Internetu*, https://pclab.pl/art33917-2.html.
10. Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL 2017, https://www.bbn.gov.pl/pl/wydarzenia/7865,Polskie-Forum-Cyberbezpieczenstwa-CYBERSEC--PL-2017.html?search=51534879342831.
11. *Przestępstwa komputerowe – Prawo karne – kodeks karny, oskarżony przed sądem, świadek, ofiara przestępstwa*, http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe.
12. *Prezydent RP: Cyfrowe zagrożenia na liście kluczowych problemów*, https://www.bbn.gov.pl/pl/wydarzenia/8326,Prezydent-RP-Cyfrowe-zagrozenia-na-liscie--kluczowych-problemow.html?search=51534879342831 .
13. *Raport Cyberbezpieczeństwo A.D. 2018*, NASK – Państwowy Instytut Badawczy, Warszawa 2019, https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Raport-Cyberbezpiecze%C5%84stwo-A.D.-2018.pdf.
14. Statystyka Policyjna, http://www.statystyka.policja.pl/portal/st/840/71787/Przestepstwa_popelniane_w_sieci.html.

dr inż. Tomasz Grudniewski
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0003-3394-8992

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

dr Iwona Lasek-Surowiec
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0002-7231-7993

mgr Zuzanna Jordan
ORCID: 0009-0009-2636-8501

https://doi.org/10.29316/9788368103205_2

WPŁYW CYBERATAKÓW NA SEKTOR FINANSOWY

THE IMPACT OF CYBERATTACKS ON THE FINANCIAL SECTOR

Streszczenie

Celem rozdziału jest przedstawienie charakteru i skutków cyberataków wymierzonych w sektor finansowy. W pierwszej części zaprezentowano charakterystykę sektora finansowego jako obszaru szczególnie narażonego na cyberzagrożenia, z uwzględnieniem rodzaju ataków oraz ich wpływu na bezpieczeństwo danych i stabilność gospodarki. Druga część koncentruje się na analizie konkretnych przypadków cyberataków – głównie

Summary

The aim of the chapter is to present the nature and effects of cyberattacks aimed at the financial sector. The first part presents the characteristics of the financial sector as an area particularly vulnerable to cyber threats, taking into account the type of attacks and their impact on data security and economic stability. The second part focuses on the analysis of specific cases of cyberattacks – mainly in the context of actions against the Polish

w kontekście działań przeciwko KNF – oraz ich bezpośrednich i pośrednich konsekwencji. W części trzeciej opisano aktualne strategie reagowania, obowiązujące regulacje prawne oraz wyzwania i kierunki rozwoju systemu cyberbezpieczeństwa w instytucjach finansowych. Problem badawczy sformułowano: Jakie są główne zagrożenia cybernetyczne dla sektora finansowego w Polsce i w jaki sposób instytucje finansowe, w tym KNF, reagują na te zagrożenia? W rozdziale zastosowano analizę literatury przedmiotu, dokumentów, w szczególności raportu rocznego CSIRT KNF 2024 oraz rzetelnych źródeł internetowych. Rosnące zagrożenie cyberatakami wobec sektora finansowego wymaga systemowego podejścia, które łączy działania techniczne, prawne i edukacyjne, a także rozwój odporności instytucjonalnej opartej na współpracy i ciągłej adaptacji do zmieniających się realiów cyberprzestrzeni.

Słowa kluczowe: cyberbezpieczeństwo, sektor finansowy, KNF, cyberatak, fałszywe inwestycje

Financial Supervision Authority – and their direct and indirect consequences. The third part describes current response strategies, applicable legal regulations as well as challenges and directions of development of the cybersecurity system in financial institutions. The research problem was formulated: What are the main cyber threats to the financial sector in Poland and how do financial institutions, including the Polish Financial Supervision Authority, respond to these threats? The chapter uses an analysis of the literature on the subject, documents, in particular the annual report of the CSIRT KNF 2024 and reliable online sources. The growing threat of cyberattacks against the financial sector requires a systemic approach that combines technical, legal, and educational activities, as well as the development of institutional resilience based on cooperation and continuous adaptation to the changing realities of cyberspace.

Keywords: cybersecurity, financial sector, Polish Financial Supervision Authority, cyberattack, fake investments

Wstęp

W dobie postępującej cyfryzacji i rosnącej zależności od technologii informatycznych, sektor finansowy staje się jednym z głównych celów cyberprzestępców. Instytucje takie jak banki, domy maklerskie, giełdy, towarzystwa ubezpieczeniowe, a także organy nadzorcze – w tym Komisja Nadzoru Finansowego – przetwarzają i przechowują ogromne ilości danych wrażliwych oraz zarządzają infrastrukturą krytyczną dla funkcjonowania całej gospodarki. W konsekwencji każda luka w zabezpieczeniach może prowadzić do poważnych konsekwencji, zarówno dla pojedynczych podmiotów, jak i dla stabilności całego systemu finansowego.

Cyberataki na sektor finansowy przybierają coraz bardziej wyrafinowane formy. Złośliwe oprogramowanie, ataki typu phishing, ransomware, a także zaawansowane techniki inżynierii społecznej są wykorzystywane do uzyskania

dostępu do systemów informatycznych i danych klientów. Dodatkowo rośnie zagrożenie ze strony podmiotów państwowych i zorganizowanych grup cyberprzestępczych, które działają w sposób skoordynowany i często trudny do wykrycia. Z uwagi na skalę ryzyka, jak również potencjalne skutki społeczne i ekonomiczne, kwestia ochrony przed cyberatakami stała się jednym z priorytetów strategii bezpieczeństwa finansowego w Polsce i na świecie.

Przykłady incydentów z ostatnich lat, w tym cyberataków wymierzonych w Komisję Nadzoru Finansowego, pokazują, że nawet instytucje odpowiedzialne za nadzór i bezpieczeństwo nie są odporne na tego rodzaju zagrożenia. Naruszenia integralności danych, utrata dostępności do systemów czy upublicznienie poufnych informacji mogą prowadzić do spadku zaufania do całego rynku finansowego, a w skrajnych przypadkach – do destabilizacji jego funkcjonowania.

Celem niniejszego rozdziału jest analiza wpływu cyberataków na sektor finansowy w Polsce, ze szczególnym uwzględnieniem incydentów dotyczących Komisji Nadzoru Finansowego. W rozdziale omówione zostaną zarówno mechanizmy i techniki wykorzystywane przez cyberprzestępców, jak i działania podejmowane przez instytucje w odpowiedzi na rosnące zagrożenia. Podjęta zostanie również refleksja nad aktualnym stanem bezpieczeństwa cyfrowego w sektorze finansowym oraz nad potrzebą dalszego wzmacniania odporności instytucji na ataki w cyberprzestrzeni.

Sektor finansowy jako cel cyberataków

W ramach systemu finansowego funkcjonują różnorodne instytucje finansowe, które zajmują się szeroko pojętym zarządzaniem zasobami pieniężnymi państwa i obywateli[1], dlatego od lat znajduje się w centrum zainteresowania cyberprzestępców. Jest to obszar gospodarki o wyjątkowym znaczeniu systemowym, który nie tylko odpowiada za obrót kapitałem, ale także stanowi fundament zaufania społecznego i stabilności ekonomicznej. W związku z tym każdy incydent bezpieczeństwa w tym sektorze może mieć daleko idące konsekwencje – od strat finansowych po kryzysy zaufania i zaburzenia płynności rynkowej. RCB jako główne wskazało następujące segmenty systemu:

[1] R. Hennig, *Cyberterroryzm vs infrastruktura krytyczna. Cz. V. System finansowy*, Kwartalnik Bellona, Nr 2, Wydawnictwo MON, Warszawa 2017, s. 184.

- budżetowy, związany z funkcjonowaniem finansowych struktur państwowych;
- bankowy, odnoszący się do funkcjonowania banków i instytucji kredytowych;
- ubezpieczeniowy, związany z ubezpieczeniami społecznymi oraz na życie, osobowymi i majątkowymi;
- kapitałowy, poświęcony obrotowi średnio i długoterminowych instrumentów finansowych[2].

Instytucje finansowe, takie jak banki, domy maklerskie, firmy ubezpieczeniowe, fundusze inwestycyjne oraz operatorzy systemów płatniczych, gromadzą i przetwarzają ogromne ilości danych osobowych, finansowych i handlowych. Są to dane o wysokiej wartości, zarówno dla cyberprzestępców działających w celach finansowych, jak i dla podmiotów zainteresowanych działalnością wywiadowczą lub destabilizacją systemu gospodarczego. Co więcej, cyfryzacja usług finansowych – bankowości internetowej, aplikacji mobilnych, e-płatności – poszerzyła powierzchnię potencjalnych ataków, a także zwiększyła zależność od infrastruktury IT[3]. Do najczęstszych form ataków skierowanych przeciwko sektorowi finansowemu należą:

- Phishing – technika polegająca na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia danych logowania, numerów kart płatniczych lub innych poufnych informacji.
- Malware – złośliwe oprogramowanie wprowadzane do systemów w celu kradzieży danych, przejęcia kontroli nad systemem lub wywołania szkód w infrastrukturze IT.
- Ransomware – oprogramowanie szyfrujące dane i żądające okupu za ich odszyfrowanie. Tego rodzaju ataki często paraliżują działalność operacyjną instytucji finansowych.
- DDoS (Distributed Denial of Service) – ataki polegające na przeciążeniu systemów sieciowych, prowadzące do niedostępności usług online, np. bankowości elektronicznej.

[2] Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1. Charakterystyka systemów infrastruktury krytycznej, Warszawa 2013, s. 37-41.

[3] D. Skoczylas, *Cyberbezpieczeństwo sektora bankowego i infrastruktury rynków finansowych*, Acta Iuris Stetinensis, 43 (2), 2023, s. 109.

- Manipulacje rynkowe i ataki na algorytmy transakcyjne – cyberprzestępcy coraz częściej próbują ingerować w działanie systemów handlu elektronicznego, automatycznych mechanizmów decyzyjnych czy nawet manipulować kursami instrumentów finansowych.

Warto również zwrócić uwagę, że zagrożenie nie zawsze pochodzi z zewnątrz. Równie niebezpieczne są działania osób z wewnątrz organizacji (tzw. insider threats), które mają dostęp do krytycznych systemów i danych[4]. Takie przypadki są trudniejsze do wykrycia i często wiążą się z nadużyciem zaufania oraz lukami w polityce bezpieczeństwa. Oto kilka przykładów największych cyberataków na sektor finansowy:

- Equifax: w 2017 r. hakerzy zaatakowali Equifax, jedną z największych agencji oceny zdolności kredytowej. Ujawniono dane osobowe około 147 milionów klientów, w tym numery ubezpieczenia społecznego i dane finansowe[5].
- Banco de Chile: w 2018 r. chilijski Banco de Chile został zaatakowany przez hakerów, którzy zablokowali systemy banku i skradli dane klientów. Diagram ataku na infrastrukturę ofiary. Pomimo, że wszystkie wskazane przykłady dotyczą rynków zagranicznych, w Polsce sektor finansowy również jest jednym z najczęściej atakowanych przez cyberprzestępców[6].
- Atak na Evolve Bank & Trust: w lipcu 2024 r. Evolve Bank & Trust z siedzibą w Memphis, Tennessee, doświadczył poważnego naruszenia danych, które dotknęło 7,6 miliona osób. Atak został powiązany z grupą ransomware LockBit, która ujawniła wrażliwe dane klientów po tym, jak bank odmówił zapłacenia okupu. Skradzione informacje obejmowały nazwiska, numery ubezpieczenia społecznego, numery kont bankowych oraz dane kontaktowe[7].
- Atak na LoanDepot: LoanDepot, czołowy pożyczkodawca hipoteczny z siedzibą w Irvine w Kalifornii, padł ofiarą ataku, w wyniku którego

[4] L. Liu, O. De Vel, Q.-L. Han, J. Zhang, Y. Xiang, *Detecting and Preventing Cyber Insider Threats: A Survey*, IEEE Communications Surveys & Tutorials, vol. 20, no. 2, 2018, s. 1400.

[5] *Equifax zapłaci za wyciek danych klientów. Ugoda z FTC*, https://businessinsider.com.pl/firmy/zarzadzanie/equifax-zaplaci-za-wyciek-danych-klientow-ugoda-z-ftc/l8hdwqd, [dostęp: 05.04.2025].

[6] *Ransomware sparaliżował bank w Chile* – Bankier.pl, https://www.bankier.pl/wiadomosc/Ransomware-sparalizowal-bank-w-Chile-7958860.html, [dostęp: 05.04.2025].

[7] *Major Cyber Attacks Targeting the Finance Industry* - SOCRadar® Cyber Intelligence Inc., https://socradar.io/major-cyber-attacks-targeting-the-finance-industry, [dostęp: 05.04.2025].

naruszono dane 16,9 miliona klientów. Atak miał miejsce między 3 a 5 stycznia 2024 r. i został przypisany grupie Alphv, znanej również jako Blackcat. Skradzione dane obejmowały nazwiska, adresy, numery kont finansowych, numery telefonów oraz daty urodzenia klientów[8].

- Atak na ByBit: w lutym 2025 r. FBI zidentyfikowało Koreę Północną jako odpowiedzialną za kradzież wirtualnych aktywów o wartości 1,5 miliarda dolarów z giełdy kryptowalut ByBit. Jest to największa tego typu kradzież w historii. Skradzione środki zostały początkowo przetransferowane na wiele adresów bitcoin i innych wirtualnych aktywów, a następnie prawdopodobnie wyprane i zamienione na walutę fiducjarną[9].

Cyberzagrożenia w sektorze finansowym to nie tylko problem instytucji komercyjnych, takich jak banki czy firmy ubezpieczeniowe, ale również organów nadzoru, które pełnią kluczową rolę w zapewnieniu stabilności i transparentności rynku. Jednym z najgłośniejszych przykładów w ostatnich latach był cyberatak wymierzony w Komisję Nadzoru Finansowego (KNF), który unaocznił skalę i powagę ryzyk związanych z bezpieczeństwem cyfrowym w instytucjach publicznych[10].

Do incydentu doszło na przełomie grudnia 2023 i stycznia 2024 r. Atak został zakwalifikowany jako poważny incydent bezpieczeństwa, skutkujący czasowym unieruchomieniem niektórych systemów informatycznych Komisji. Choć oficjalne komunikaty KNF nie zawierały wielu szczegółów, wiadomo, że w ramach środków zaradczych instytucja natychmiast odłączyła swoje systemy od sieci zewnętrznych, co spowodowało zakłócenia w dostępie do usług elektronicznych, w tym do systemu ePUAP. W wyniku tego utrudniona została codzienna komunikacja z interesariuszami i nadzorowanymi podmiotami. Z informacji medialnych i raportów branżowych wynika, że za atakiem mogła stać zorganizowana grupa przestępcza, prawdopodobnie działająca z zagranicy, posługująca się znanymi schematami – w tym oprogramowaniem

[8] *The biggest data breaches of 2024 in financial services*, American Banker, https://www.americanbanker.com/list/the-biggest-data-breaches-of-2024-in-financial-services?, [dostęp: 05.04.2025].

[9] North Korea behind $1.5bn hack of crypto exchange ByBit, says FBI, North Korea, The Guardian, https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi?, [dostęp: 05.04.2025].

[10] *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa – Archiwum, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/, [dostęp: 05.04.2025].

ransomware i kampanią phishingową. Choć nie doszło do potwierdzonego wycieku danych osobowych lub finansowych, eksperci ds. bezpieczeństwa ostrzegali, że nawet czasowa niedostępność systemów nadzorczych może mieć poważne implikacje dla ciągłości działania całego sektora. Bezpośrednie konsekwencje incydentu objęły:

- tymczasowy paraliż komunikacyjny w KNF,
- zakłócenia w procesach nadzoru i obsługi zgłoszeń,
- zwiększoną podatność na dezinformację i ataki wtórne.

Pośrednie skutki miały natomiast charakter reputacyjny i systemowy. Pojawiły się pytania o odporność infrastruktury IT kluczowych instytucji państwowych, a także o zdolność KNF do szybkiej reakcji w sytuacjach kryzysowych. Utrata zaufania do instytucji nadzorczej, nawet chwilowa, może rzutować na stabilność całego systemu finansowego – szczególnie w oczach inwestorów, klientów i międzynarodowych partnerów.

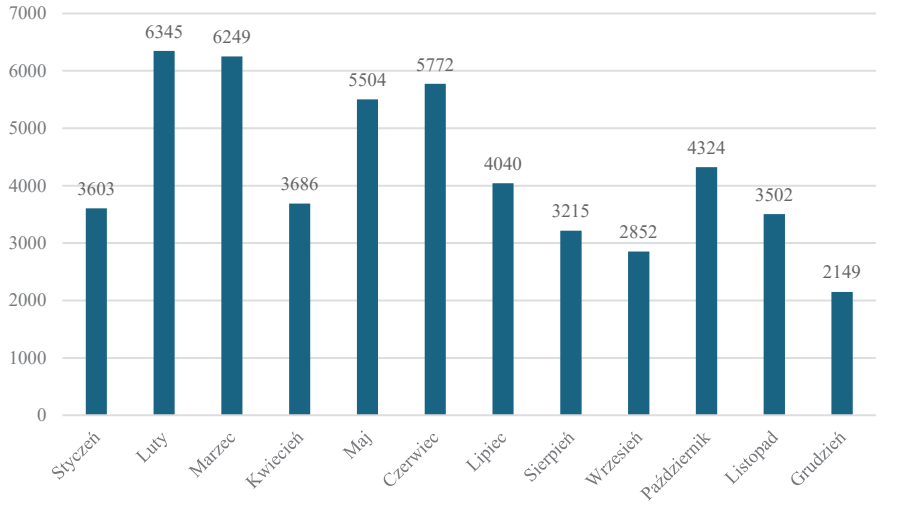
W odpowiedzi na atak, Komisja Nadzoru Finansowego we współpracy z zespołami CSIRT NASK i CERT Polska wdrożyła procedury zarządzania incydentem, przeprowadziła szczegółowe analizy techniczne oraz podjęła działania prewencyjne, mające na celu podniesienie poziomu bezpieczeństwa swoich systemów informatycznych. Zdarzenie to stało się również impulsem do szerszej debaty o konieczności modernizacji infrastruktury cyfrowej w instytucjach publicznych i podjęcia dalszych działań legislacyjnych w zakresie cyberbezpieczeństwa.

Przypadek KNF potwierdza, że nawet najbardziej doświadczone i dobrze zorganizowane instytucje mogą stać się ofiarą cyberataków. Dlatego tak istotne jest ciągłe doskonalenie mechanizmów obronnych, monitorowanie zagrożeń oraz budowanie kultury cyberodporności zarówno w sektorze prywatnym, jak i publicznym.

Rosnące zagrożenia cybernetyczne wobec sektora finansowego wymuszają na instytucjach konieczność inwestowania w nowoczesne systemy bezpieczeństwa, przeprowadzania regularnych audytów, testów penetracyjnych, a także budowania kultury cyberodporności wśród pracowników i klientów. W przeciwnym razie nawet najmniejszy błąd lub luka w zabezpieczeniach może zostać wykorzystana do przeprowadzenia skutecznego i kosztownego ataku.

Charakterystyka cyberataków na sektor finansowy w 2024 roku

Rok 2024 przyniósł bezprecedensowy wzrost liczby cyberataków wymierzonych w sektor finansowy w Polsce. Zgodnie z danymi zawartymi w raporcie CSIRT KNF, liczba zgłoszonych niebezpiecznych domen osiągnęła rekordowy poziom – 51 241 przypadków. W porównaniu z rokiem poprzednim oznacza to wzrost o ponad 70%. Największą grupę, stanowiącą aż 89,4% wszystkich incydentów, tworzyły fałszywe strony inwestycyjne. Ta forma oszustwa była nie tylko najczęściej występująca, ale również najbardziej szkodliwa, skutkując poważnymi stratami finansowymi i społecznymi. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 przedstawiono na rysunku poniżej.



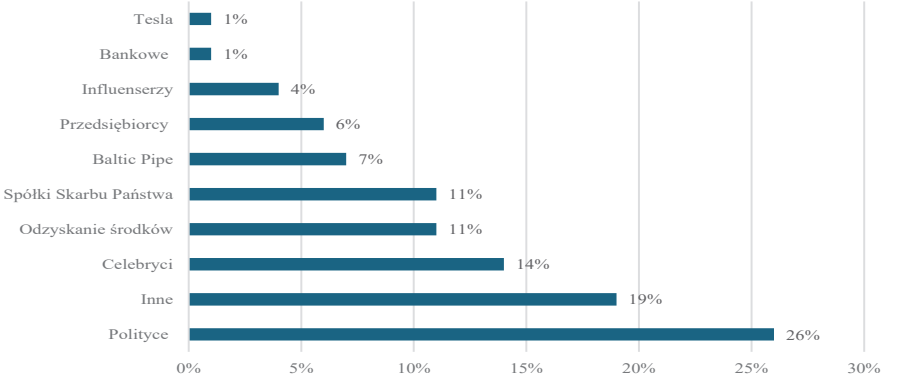
Rysunek 1. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 roku w poszczególnych miesiącach
Źródło: Raport Roczny CISIRT KNF 2024, s. 9.

Fałszywe inwestycje polegały na tworzeniu profesjonalnie wyglądających, lecz całkowicie fikcyjnych platform inwestycyjnych. Cyberprzestępcy wykorzystywali zaawansowane techniki socjotechniczne, aby uwiarygodnić swoje działania – posługiwali się m.in. fałszywymi wykresami, sfałszowanymi opiniami, historiami rzekomych sukcesów oraz mechanizmami rekomendacyjnymi. W kampaniach tych szeroko wykorzystywano reklamy w mediach społecznościowych, które kierowały potencjalne ofiary na spreparowane

strony internetowe. Coraz częściej przestępcy sięgali po technologię deepfake, aby generować materiały wideo z udziałem znanych osób zachęcających do inwestycji, co dodatkowo potęgowało wrażenie autentyczności.

Oprócz fałszywych inwestycji, dużym zagrożeniem okazały się oszustwa ankietowe. CSIRT KNF zidentyfikował ponad cztery tysiące domen związanych z tego typu kampaniami. Ich mechanizm działania polegał na zachęcaniu użytkowników do wypełnienia krótkiej ankiety w zamian za rzekomą nagrodę. Użytkownik w trakcie wypełniania formularza był stopniowo skłaniany do podania danych osobowych oraz informacji o karcie płatniczej. Strony imitowały wygląd znanych marek i instytucji, co miało na celu zwiększenie wiarygodności przekazu. Kluczową rolę odgrywały tu emocje – przestępcy stosowali presję czasu i efekt „strachu przed utratą okazji" (FOMO), aby przyspieszyć reakcję użytkowników.

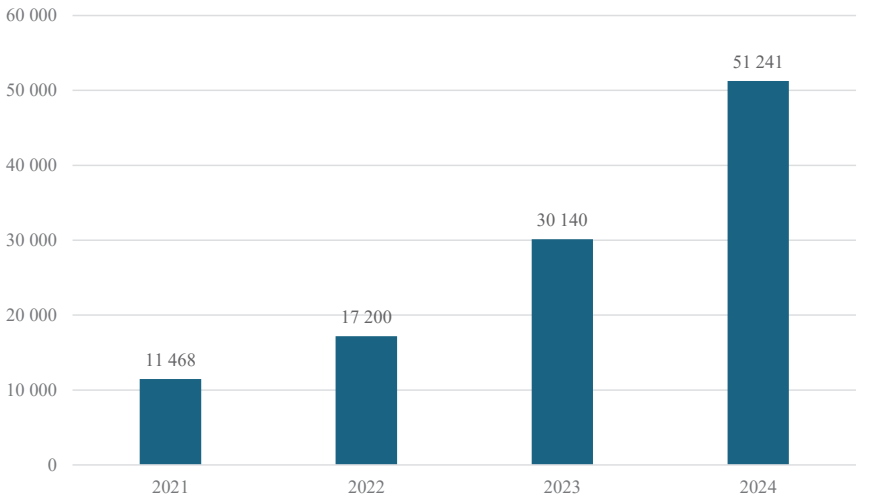
Kolejną kategorią były oszustwa bankowe, w których przestępcy podszywali się pod znane instytucje finansowe. Tworzyli fałszywe strony logowania do bankowości elektronicznej, często różniące się od oryginalnych jedynie minimalnymi szczegółami w adresie URL. Do ofiar trafiały reklamy w mediach społecznościowych, wiadomości SMS oraz e-maile, które przekierowywały na fałszywe witryny. Wykorzystywane wizerunki w reklamach fałszywych inwestycji w 2024 roku przedstawiono na poniższym rysunku.



Rysunek 2. Wykorzystywane wizerunki w reklamach fałszywych inwestycji w 2024 roku

Źródło: Raport Roczny CISIRT KNF 2024, s. 12.

Przestępcy potrafili wykorzystać zarówno techniki phishingowe, jak i manipulację wynikami wyszukiwania w Google, umieszczając swoje spreparowane strony w czołówce wyników. Poniżej na rysunku 3 przedstawiono liczbę zgłoszonych domen phishingowych w latach 2021-2024 przez CSIRT KNF.



Rysunek 3. Liczba zgłoszonych domen phishingowych w latach 2021-2024 przez CSIRT KNF

Źródło: Raport Roczny CISIRT KNF 2024, s. 10.

Z raportu wynika również, że rok 2024 był okresem intensywnych kampanii z użyciem złośliwego oprogramowania. Obserwowano aktywność wielu różnych typów malware, w tym programów typu stealer, takich jak Lumma Stealer czy AgentTesla, których celem było wykradanie danych logowania i poufnych informacji z komputerów użytkowników. Inne zagrożenia obejmowały oprogramowanie typu RAT (*Remote Access Trojan*), jak RemcosRAT czy Xworm, które pozwalało przestępcom na zdalne przejęcie kontroli nad zainfekowanym systemem. Szczególnie niepokojące były przypadki wykorzystania aplikacji mobilnych, dystrybuowanych np. przez fałszywe reklamy na Facebooku. Aplikacje te, często bazujące na technologiach WebAPK lub PWA, udawały oficjalne narzędzia bankowe, a w rzeczywistości wykradały dane osobowe i finansowe użytkowników.

Raport podkreśla także coraz większe zaawansowanie kampanii cyberprzestępczych. Przestępcy szybko dostosowują się do zmieniających się realiów i zabezpieczeń, korzystają z aktualnych wydarzeń społeczno-gospodarczych,

a także coraz częściej personalizują swoje działania w zależności od profilu ofiary. Widać także coraz częstsze wykorzystanie narzędzi opartych na sztucznej inteligencji, które umożliwiają tworzenie jeszcze bardziej przekonujących treści oszukańczych. W świetle powyższych danych, CSIRT KNF wskazuje na potrzebę stałego doskonalenia mechanizmów ochrony przez instytucje finansowe i regulatorów. Rok 2024 był kolejnym dowodem na to, że cyberprzestępczość staje się coraz bardziej profesjonalna i zorganizowana, a jej celem są zarówno dane, jak i bezpośrednie środki finansowe obywateli. Złożoność złośliwego oprogramowania, szybkość działania hakerów, doskonała znajomość wewnętrznych systemów transakcyjnych banków dowodzą wagi problemu, wobec którego stoją instytucje finansowe[11].

Reakcje, strategie i przyszłość cyberbezpieczeństwa w finansach

W obliczu rosnącej liczby i skali cyberzagrożeń sektor finansowy znajduje się dziś w punkcie zwrotnym, który wymaga nie tylko reagowania na incydenty, ale przede wszystkim strategicznego podejścia do budowania trwałej odporności cyfrowej. Odpowiedzią na nasilające się ataki są działania podejmowane na wielu poziomach – od pojedynczych instytucji finansowych, przez krajowe organy nadzoru, po inicjatywy międzynarodowe. Kluczowe znaczenie ma tu spójna i zintegrowana polityka bezpieczeństwa, która obejmuje zarówno aspekt technologiczny, jak i organizacyjny oraz edukacyjny.

Jednym z najważniejszych elementów krajowej odpowiedzi na zagrożenia cybernetyczne jest działalność zespołu CSIRT KNF, pełniącego rolę sektorowego zespołu reagowania na incydenty komputerowe. W 2024 r. zespół ten nie tylko monitorował i analizował bieżące kampanie przestępcze, lecz także aktywnie uczestniczył w budowaniu systemu prewencji poprzez identyfikację niebezpiecznych domen, blokowanie oszukańczych treści i prowadzenie działań edukacyjnych. Współpraca z CSIRT NASK, CERT Polska oraz platformami społecznościowymi, takimi jak Facebook, umożliwiła szybkie reagowanie na nowe zagrożenia oraz ograniczanie ich zasięgu.

Istotnym krokiem w kierunku systemowego podejścia do bezpieczeństwa cyfrowego jest także wdrożenie regulacji europejskich, w tym aktu

[11] G. Strupczewski, *Zagrożenie cybernetyczne instytucji finansowych*, Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych, Nr 24, 2017, s. 80.

DORA (*Digital Operational Resilience Act),* który obowiązywać będzie od stycznia 2025 r. Rozporządzenie to nakłada nowe obowiązki w zakresie zarządzania ryzykiem ICT (technologii informacyjno-komunikacyjnych) na wszystkie instytucje finansowe działające na terenie Unii Europejskiej. DORA wprowadza jednolite standardy raportowania incydentów, testowania odporności cyfrowej, a także nadzoru nad dostawcami usług technologicznych. Jego celem jest wzmocnienie spójności i gotowości całego rynku finansowego na wypadek zakłóceń wywołanych cyberatakami. Na poziomie organizacyjnym wiele instytucji finansowych podejmuje działania mające na celu zwiększenie odporności swoich systemów[12]. Wśród nich znajdują się inwestycje w nowoczesne technologie wykrywania zagrożeń, automatyzacja procesów bezpieczeństwa (np. poprzez SIEM czy SOAR), a także rozwój wewnętrznych zespołów reagowania i współpraca z zewnętrznymi partnerami w zakresie cyberbezpieczeństwa. Coraz większy nacisk kładzie się również na zarządzanie ryzykiem dostawców zewnętrznych, którzy odgrywają coraz istotniejszą rolę w działalności operacyjnej instytucji finansowych.

Nie można pominąć także roli edukacji i podnoszenia świadomości. Kampanie informacyjne, szkolenia dla pracowników, materiały dla klientów indywidualnych – to narzędzia, które pozwalają ograniczyć skuteczność ataków opartych na socjotechnice. CSIRT KNF w swoim raporcie wskazuje, że jednym z kluczowych czynników sukcesu cyberprzestępców jest właśnie nieświadomość użytkowników oraz ich skłonność do zaufania treściom publikowanym w Internecie. Dlatego też działania prewencyjne muszą być prowadzone równolegle z wdrażaniem zabezpieczeń technicznych.

W perspektywie najbliższych lat można spodziewać się dalszej ewolucji zagrożeń, związanej m.in. z wykorzystaniem sztucznej inteligencji do tworzenia treści oszukańczych, automatyzacją ataków oraz rosnącą liczbą podatności w systemach informatycznych. Nowe technologie przyniosą zarówno możliwości, jak i wyzwania, dlatego sektor finansowy musi nieustannie adaptować się do zmieniającego się krajobrazu zagrożeń.

Wnioski płynące z roku 2024 są jednoznaczne – cyberbezpieczeństwo nie jest już kwestią techniczną, lecz strategiczną. Tylko kompleksowe podejście, obejmujące zarówno rozwój technologii ochronnych, jak i działania

[12] A. Krawczyk-Jezierska, *Koszty instytucji finansowych w świetle zagrożeń cybernetycznych*, tom LXXII, nr 8(854), 2019, s. 30.

legislacyjne, organizacyjne i edukacyjne, pozwoli na skuteczne przeciwdziałanie rosnącej fali zagrożeń w cyberprzestrzeni. Budowanie odporności sektora finansowego musi opierać się na współpracy wszystkich interesariuszy: instytucji publicznych, regulatorów, dostawców usług technologicznych oraz samych klientów. Tylko wtedy możliwe będzie utrzymanie zaufania do rynku finansowego jako stabilnego i bezpiecznego filaru gospodarki.

Podsumowanie

Rok 2024 wyraźnie potwierdził, że sektor finansowy pozostaje jednym z najbardziej narażonych obszarów na cyberzagrożenia. Rosnąca skala i złożoność ataków, a także ich coraz bardziej zróżnicowane formy, wymusiły konieczność zintensyfikowania działań prewencyjnych i reagujących. Największym wyzwaniem okazały się kampanie fałszywych inwestycji, które zdominowały krajobraz cyberprzestępczy, prowadząc do poważnych strat finansowych wśród klientów indywidualnych. Ich skuteczność wynikała z umiejętnego łączenia technik socjotechnicznych z nowoczesnymi narzędziami, takimi jak deepfake czy personalizowane kampanie reklamowe.

Istotnym problemem pozostaje fakt, że cyberprzestępcy coraz częściej wykorzystują zaufanie społeczne – podszywają się pod znane osoby, instytucje publiczne czy duże firmy, co znacząco utrudnia wykrycie zagrożenia. Dodatkowo, rosnąca liczba oszustw ankietowych, ataków na bankowość elektroniczną oraz kampanii złośliwego oprogramowania pokazuje, że zagrożenie nie jest ograniczone do jednego typu działania, lecz przybiera wiele form jednocześnie. W związku z tym nie wystarczy już stosowanie klasycznych metod ochrony – potrzebne są rozwiązania kompleksowe, uwzględniające zarówno aspekty techniczne, jak i organizacyjne, a także edukacyjne.

Reakcja sektora finansowego, w tym działania podejmowane przez KNF i CSIRT KNF, wskazują na rosnącą świadomość w zakresie potrzeby budowania odporności cyfrowej. Przykładem tego jest coraz szersze wdrażanie regulacji europejskich, takich jak DORA, które mają na celu ujednolicenie standardów i wymogów dotyczących bezpieczeństwa w całej Unii Europejskiej. Jednocześnie rośnie znaczenie współpracy między instytucjami publicznymi, sektorem prywatnym oraz międzynarodowymi partnerami, co jest nieodzowne w kontekście globalnego charakteru zagrożeń.

Wnioski z analizy raportu CSIRT KNF są jasne – cyberbezpieczeństwo nie może być traktowane jako dodatek do działalności operacyjnej, lecz jako jej integralna część. Tylko wtedy możliwe będzie skuteczne przeciwdziałanie zagrożeniom i ograniczenie ich skutków. Niezbędna jest dalsza rozbudowa infrastruktury ochronnej, regularne testowanie mechanizmów bezpieczeństwa, a przede wszystkim – budowanie kultury świadomości cyfrowej wśród wszystkich uczestników rynku finansowego. Przyszłość cyberbezpieczeństwa w finansach zależy od tego, jak szybko i konsekwentnie sektor dostosuje się do nowych realiów, w których cyberprzestrzeń stała się nieodłącznym i coraz bardziej ryzykownym elementem funkcjonowania gospodarki.

Literatura

1. *Atak teleinformatyczny na polski sektor finansowy,* Rządowe Centrum Bezpieczeństwa – Archiwum, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/.
2. *Equifax zapłaci za wyciek danych klientów. Ugoda z FTC*, https://businessinsider.com.pl/firmy/zarzadzanie/equifax-zaplaci-za-wyciek-danych-klientow-ugoda-z-ftc/l8hdwqd.
3. Hennig R., *Cyberterroryzm vs infrastruktura krytyczna. Cz. V. System finansowy*, Kwartalnik Bellona, 2/2017.
4. Krawczyk-Jezierska A., *Koszty instytucji finansowych w świetle zagrożeń cybernetycznych*, tom LXXII, nr 8(854), 2019.
5. Liu L., De Vel O., Han Q.-L., Zhang J., Xiang Y., *Detecting and Preventing Cyber Insider Threats: A Survey*, IEEE Communications Surveys & Tutorials, vol. 20, no. 2, 2018.
6. *Major Cyber Attacks Targeting the Finance Industry* – SOCRadar® Cyber Intelligence Inc., https://socradar.io/major-cyber-attacks-targeting-the-finance-industry.
7. Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Charakterystyka systemów infrastruktury krytycznej. Warszawa 2013, s. 37-41.
8. North Korea behind $1.5bn hack of crypto exchange ByBit, says FBI, North Korea, The Guardian, https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi?
9. *Ransomware sparaliżował bank w Chile,* Bankier.pl, https://www.bankier.pl/wiadomosc/Ransomware-sparalizowal-bank-w-Chile-7958860.html.
10. Raport Roczny CISIRT KNF 2024.
11. Skoczylas D., *Cyberbezpieczeństwo sektora bankowego i infrastruktury rynków finansowych*, Acta Iuris Stetinensis 43(2), 2023.
12. Strupczewski G., *Zagrożenie cybernetyczne instytucji finansowych*, Rozprawy Ubezpieczeniowe. Konsument na rynku usług finansowych, 24, 2017, s. 80.
13. *The biggest data breaches of 2024 in financial services*, American Banker, https://www.americanbanker.com/list/the-biggest-data-breaches-of-2024-in-financial-services?

dr inż. Karol Chlasta
Akademia Leona Koźmińskiego
ORCID: 0000-0002-6539-566X

https://doi.org/10.29316/9788368103205_3

SZTUCZNA INTELIGENCJA W CYBERBEZPIECZEŃSTWIE – WYZWANIA I MOŻLIWOŚCI

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY – CHALLENGES AND OPPORTUNITIES

Streszczenie

W dobie rosnącej roli sztucznej inteligencji (AI) w cyberbezpieczeństwie, generatywna sztuczna inteligencja (GenAI) staje się zarówno narzędziem obronnym, jak i potencjalnym zagrożeniem. Niniejsza praca przedstawia przegląd metod sztucznej inteligencji, w tym generatywnej sztucznej inteligencji, w kontekście cyberbezpieczeństwa, uwzględniając zarówno nowe techniki ataków, jak i rozwiązania obronne, wspierane przez automatyczne modelowanie tematów. Rozdział zawiera wyniki przeglądu literatury naukowej dotyczącej cyberbezpieczeństwa i sztucznej inteligencji w latach 2017-2024, obejmującego 2420 publikacji z IEEE Xplore Digital Library i SpringerLink. Publikacje koncentrują się głównie na następujących tematach: (1) phishing (407 publikacji; 16,82%), (2) techniki adversarial

Summary

In an era marked by the increasing influence of artificial intelligence (AI) in cybersecurity, generative AI (GenAI) has emerged as both a formidable defensive tool and a potential threat. This chapter examines new AI methods, with a particular focus on generative AI, within the context of cybersecurity, addressing both emerging attack strategies and defensive solutions, as informed by automated topic modelling. The chapter presents a comprehensive review of scientific literature on cybersecurity and AI, spanning the years 2017 to 2024, drawing from a total of 2,420 publications sourced from the IEEE Xplore Digital Library and SpringerLink. The publications primarily address the following topics: (1) phishing (407 publications; 16.82%), (2) adversarial techniques (347 publications; 14.34%), (3) ChatGPT

(347 publikacji; 14,34%), (3) ChatGPT (352 publikacje; 14,55%), (4) duże modele językowe (LLM) (352 publikacje; 14,55%) oraz podatności (77 publikacji; 3,18%). Zidentyfikowane zagrożenia związane z wykorzystaniem LLM w generowaniu phishingu, automatycznym hakowaniu oraz tworzeniu złośliwego oprogramowania zostały szczegółowo podsumowane. Ponadto, zaobserwowano wzrost znaczenia narzędzi opartych na GenAI w obszarze detekcji zagrożeń, analizy kodu oraz automatyzacji cyberobrony. Zdecydowanie widać, że tematy związane z szeroko rozumianą generatywną sztuczną inteligencją (LLM i ChatGPT) stanowią większy zbiór (704 publikacje) niż tradycyjne metody uczenia maszynowego, w tym zagrożenia związane z manipulowaniem danymi wejściowymi do systemów SI (tematyka adversarial obejmuje tylko 347 publikacji). Rozdział podsumowuje również zidentyfikowane regulacje prawne oraz standardy dotyczące cyberbezpieczeństwa, takie jak NIS2, NIST AI Risk Management Framework oraz standardy ISO/IEC 22989, 23053, 23984 i 42001. Praca ukazuje rosnącą i istotną rolę różnych metod generatywnej sztucznej inteligencji w kształtowaniu przyszłości cyberbezpieczeństwa, podkreślając konieczność opracowania nowych strategii ochrony przed nowymi zagrożeniami w zmieniającym się środowisku organizacyjnym, w którym coraz bardziej polegamy na publicznej infrastrukturze chmurowej.

Słowa kluczowe: Generatywna Sztuczna Inteligencja (AI), Duże Modele Językowe (LLM), Zagrożenia oparte na AI, Cyberbezpieczeństwo, Symulacja ataków, Antagonistyczne Uczenie Maszynowe, zarządzanie ryzykiem cyberbezpieczeństwa (NIS2, NIST AI RMF), Normy ISO/IEC bezpieczeństwa AI

(352 publications; 14.55%), (4) large language models (LLMs) (352 publications; 14.55%), and vulnerabilities (77 publications; 3.18%). The risks associated with the use of LLMs in phishing campaigns, automated hacking, and malware generation are systematically summarised. Furthermore, the growing prominence of GenAI-based tools in threat detection, code analysis, and the automation of cyber defence is highlighted. Notably, the body of work dedicated to GenAI, comprising of LLMs and ChatGPT, outnumbers the traditional machine learning studies, with 704 papers on the former compared to just 347 on adversarial topics. The chapter also explores key cybersecurity regulations and standards identified in the literature, including NIS2, the NIST AI Risk Management Framework, and a range of ISO/IEC standards (22989, 23053, 23984, and 42001). This review underscores the increasing and pivotal role of various generative AI methods in shaping the future landscape of cybersecurity, while emphasising the urgent need for new strategies to defend against evolving threats in an environment increasingly dependent on public cloud infrastructure.

Keywords: Generative AI, Large Language Models (LLMs), AI-Driven Threats, Cybersecurity, Offensive Security, Adversarial Methods, Cybersecurity Risk Management (NIS2, NIST AI RMF), ISO/IEC Standards for AI Security

Wstęp

Bezpieczeństwo w cyberprzestrzeni stanowi jedno z kluczowych wyzwań współczesnego świata, szczególnie w kontekście dynamicznego rozwoju technologii informacyjno-komunikacyjnych oraz narastającej skali i złożoności zagrożeń cyfrowych. W dobie transformacji cyfrowej rośnie znaczenie nowoczesnych i zintegrowanych mechanizmów ochrony danych oraz infrastruktury teleinformatycznej, przy jednoczesnym uwzględnieniu wymogów regulacyjnych i międzynarodowych standardów bezpieczeństwa, takich jak ISO/IEC 27001 czy NIST Cybersecurity Framework[1].

Jednym z istotnych czynników wpływających na kształtowanie współczesnego ekosystemu cyberbezpieczeństwa jest rozwój sztucznej inteligencji (AI), która z jednej strony stanowi skuteczne narzędzie wspierające ochronę systemów informatycznych, a z drugiej – może być wykorzystywana jako wektor ataku przez podmioty złośliwe. Szczególne zainteresowanie nauki i przemysłu wzbudzają obecnie modele generatywne, w tym architektury oparte na Generative Adversarial Networks (GAN)[2] oraz bazujące na architekturze Transformer[3]. Wspomniane modele „przeciwnikowe" typu GAN działają na zasadzie „gry" pomiędzy dwiema sieciami neuronowymi[4]: generatorem oraz dyskryminatorem. Generator tworzy dane imitujące zbiór treningowy, natomiast dyskryminator uczy się rozróżniać dane syntetyczne od rzeczywistych. Z kolei architektura Transformer, oparta na mechanizmie samo-uwagi (self-attention), umożliwia równoległe przetwarzanie sekwencji danych, co czyni ją wyjątkowo efektywną w zadaniach, takich jak analiza języka naturalnego (NLP), detekcja anomalii czy klasyfikacja zagrożeń.

Architektury te umożliwiają nie tylko tworzenie realistycznych danych syntetycznych (np. obrazów, tekstów czy dźwięków), ale także znajdują

---

1 *Framework for improving critical infrastructure cybersecurity*, version 1.1, NIST,2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, [dostęp: 10.05.2025].

2 I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, Generative adversarial nets. *Advances in neural information processing systems 27,* 2014.

3 A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, I. Polosukhin, *Advances in neural information processing systems 30*, Attention is all you need, 2017.

4 A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, A. A. Bharath, Generative adversarial networks: An overview. *IEEE signal processing magazine*, 35(1), 2018, 53-65.

zastosowanie w złożonych atakach, takich jak deepfake, spear-phishing z wykorzystaniem metod NLP, czy manipulacją danymi treningowymi w procesie uczenia maszynowego[5].

Postęp w dziedzinie generatywnej sztucznej inteligencji (GenAI) przejawia się w dynamicznej ewolucji architektur: od wprowadzenia Generative Adversarial Networks (GAN) w 2014 r.[6], poprzez pojawienie się architektury Transformer w 2017 r.[7], modelu BERT (2018)[8], GPT-2 (2019)[9], aż po coraz bardziej zaawansowane duże modele językowe, takie jak Claude[10], Gemini[11], GPT-4[12], rozwijane w latach 2022-2024. Można zatem przypuszczać, że GenAI i duże modele językowe (LLM) będą odgrywać coraz bardziej istotną rolę zarówno w obszarze cyberobrony – na przykład poprzez automatyzację detekcji zagrożeń – jak i w działaniach ofensywnych, takich jak generowanie kodu złośliwego oprogramowania, tworzenie treści dezinformacyjnych czy realizacja innych strategii ataków cybernetycznych.

---

5 M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersle, B. Garfinkel, A. Dafoe, P. Scharre, T. Zeitzoff, B. Filar, H. Anderson, H. Roff, G. C. Allen, J. Steinhardt, C. Flynn, S. Ó hÉigeartaigh, SJ Beard, H. Belfield, S. Farquhar, C. Lyle, R. Crootof, O. Evans, M. Page, J. Bryson, R. Yampolskiy, D. Amodei, The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Technical report. University of Oxford, 2018, https://maliciousaireport.com/, [dostęp: 10.05.2025].

6 I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio, *Advances in neural information processing systems 27* Generative adversarial nets, 2014.

7 A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, I. Polosukhin, *Advances in neural information processing systems 30*, Attention is all you need, 2017.

8 J. Devlin, Ch. Ming-Wei, L. Kenton Lee, K. Toutanova Bert, Pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers), 2019, 4171-4186.

9 I. Solaiman, M. Brundage, J. Clark, *Release strategies and the social impacts of language models*, arXiv preprint arXiv:1908.09203, 2019.

10 Anthropic's All Models Overview: https://docs.anthropic.com/en/docs/ about-claude/models/all-models, [dostęp: 10.05.2025].

11 Gemini: A family of highly capable multimodal models, Google, Team, 2024, https://arxiv.org/abs/2312.11805, [dostęp: 10.05.2025].

12 OpenAI (2023) Gpt-4 technical report.

Materiały i metody

Niniejszy rozdział stanowi przegląd literatury naukowej dotyczącej zastosowań sztucznej inteligencji w obszarze cyberbezpieczeństwa, ze szczególnym uwzględnieniem technik generatywnych, takich jak duże modele językowe. Analiza obejmuje publikacje z lat 2017-2024, które zostały pozyskane z dwóch uznanych baz danych: *IEEE Xplore Digital Library* oraz *Springer Link*. W celu opracowania tematycznej mapy publikacji wykorzystano narzędzie *litstudy*[13], które umożliwiło automatyczne modelowanie tematów, analizę n-gramów w streszczeniach artykułów i wizualizację wyników.

Celem przeprowadzonej analizy literaturowej było określenie, w jakim zakresie generatywna sztuczna inteligencja, a w szczególności LLM, od czasu pojawienia się architektury Transformer w 2017 r. znajduje zastosowanie w kontekście cyberbezpieczeństwa. W tym celu autor przeprowadził systematyczne wyszukiwanie w bazach *IEEE Xplore* oraz *Springer Link*, stosując słowa kluczowe: „cybersecurity" oraz „AI". Z bazy IEEE Xplore pozyskano łącznie 1422 publikacje, wyeksportowane w formacie CSV (jeden dokument na plik). Z bazy Springer Link pobrano dodatkowo 1000 dokumentów. Po scaleniu danych uzyskano zbiór zawierający łącznie 2420 artykułów. Bazy te wybrano na podstawie wcześniejszych doświadczeń autora, wskazujących na to, że publikacje dostępne w IEEE Xplore cechują się silniejszym naciskiem na aspekty techniczne (np. detekcja zagrożeń, klasyfikacja danych), podczas gdy Springer Link prezentuje częściej ujęcia społeczno-etyczne, w tym kwestie prywatności, zgodności z regulacjami oraz percepcji technologii AI.

W ramach przygotowania danych do analizy przeprowadzono proces oczyszczania korpusu. Usunięto dwie nieistotne publikacje załadowane w formacie RIS, które nie spełniały kryteriów merytorycznych. Ostateczny korpus danych został załadowany i przetworzony w narzędziu *litstudy*, co umożliwiło wygenerowanie statystyk opisowych (m.in. histogramów częstości występowania n-gramów) oraz eksplorację tematyczną dokumentów przedstawionych na rysunkach 1, 2, 3 i 4.

Do budowy korpusu zastosowano funkcję *build_corpus* z parametrem *ngram_threshold=0.8*, co umożliwiło uwzględnienie popularnych fraz jako spójnych jednostek leksykalnych (np. artificial_intelligence, cyber_security).

[13] H. Stijn, A. Sclocco, H. Dreuning, B. Van Werkhoven, P. Hijma, J. Maassen, R. V van Nieuwpoort, *litstudy: A python package for literature reviews*. SoftwareX, 20, 101207, 2022.

Następnie, wykorzystując funkcję *compute_word_distribution*, przeprowadzono analizę częstości występowania n-gramów w korpusie. Pozwoliło to zidentyfikować kluczowe pojęcia obecne w literaturze, takie jak: „machine_learning", „deep_learning", „attack_detection", „data_privacy" czy „threat_intelligence".

Rezultaty automatycznego modelowania tematów przedstawiono w postaci wizualizacji krajobrazu tematycznego, opartego o landscape plot, który wykorzystuje nieliniowe metody redukcji wymiarowości, takie jak tSNE[14] i UMAP[15], do rozmieszczenia dokumentów na płaszczyźnie dwuwymiarowej. Mapy takie umożliwiają intuicyjne rozpoznanie grup tematycznych, w których blisko siebie zlokalizowane dokumenty reprezentują podobną treść semantyczną. Należy przy tym podkreślić, że odległości między punktami na wizualizacji mają charakter ilustracyjny i nie powinny być interpretowane w sensie metrycznym.

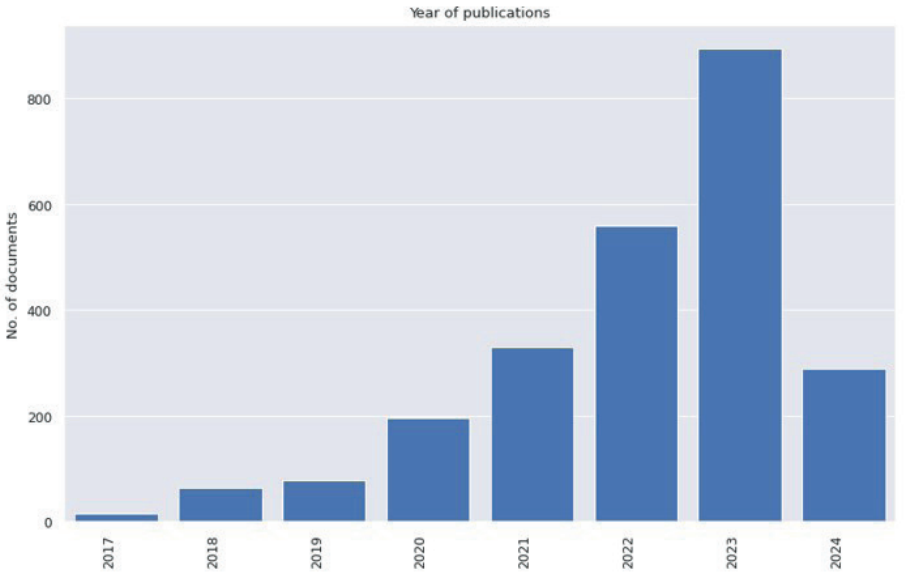
Rezultaty

Zgromadzone wyniki prezentują kompleksowy obraz aktualnego stanu badań na styku sztucznej inteligencji i cyberbezpieczeństwa, podkreślając rosnącą rolę technik generatywnych – zarówno w zakresie detekcji zagrożeń, analiz podatności, symulacji scenariuszy ataków, jak i automatyzacji reakcji na incydenty.

Analiza liczby publikacji w latach 2017-2024 (rysunek 1) ukazuje wyraźny trend wzrostowy. Począwszy od 20 publikacji w 2017 r., ich liczba wzrastała niemal liniowo aż do roku 2020 (200 publikacji), po czym tempo przyrostu uległo znacznemu przyspieszeniu. Szczególnie istotny skok zaobserwowano w latach 2022-2024, gdzie liczba publikacji osiągnęła ponad 400 rocznie. Taki przyrost wskazuje nie tylko na rosnące zainteresowanie tematyką sztucznej inteligencji w kontekście cyberbezpieczeństwa, ale także na zwiększoną świadomość badaczy w zakresie potencjalnych zastosowań obronnych i ofensywnych tych technologii.

[14] L. Van der Maaten, G. Hinton, *Visualizing data using t-sne*. Journal of machine learning research, 9(11), 2008.

[15] L. McInnes, J. Healy, J. Melville, *Umap: Uniform manifold approximation and projection for dimension reduction,* arXiv preprint arXiv:1802.03426, 2018.

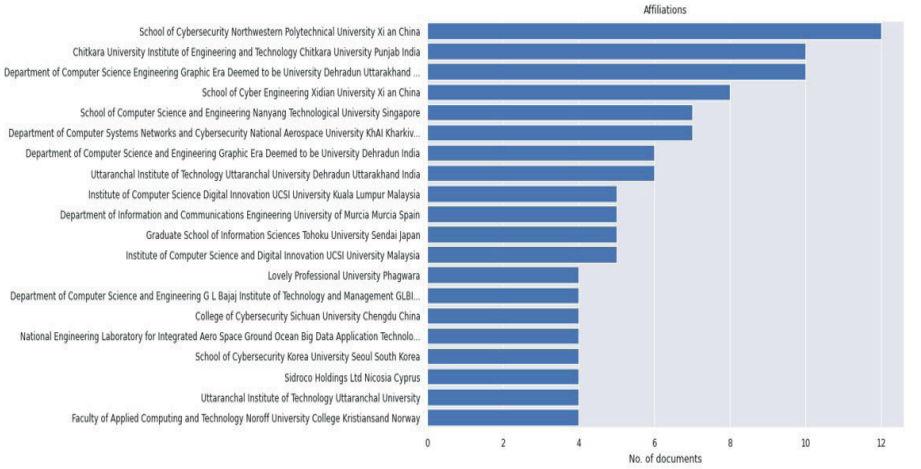


Rysunek 1. Sztuczna inteligencja i cyberbezpieczeństwo, ilość publikacji w latach 2017-2024

Źródło: opracowanie własne.

Analiza danych wskazuje też potencjalnie najaktywniejsze instytucje naukowe w zakresie badań nad zastosowaniami sztucznej inteligencji w cyberbezpieczeństwie. Wśród 20 najczęściej pojawiających się afiliacji dominują ośrodki z Chin i Indii, co odzwierciedla rosnącą rolę Azji w globalnym ekosystemie badawczym. Znaczącą obecność mają również uczelnie i instytuty badawcze z Japonii, Korei Południowej, Singapuru i Malezji. W zestawieniu znalazły się również wybrane europejskie jednostki z Hiszpanii, Norwegii, Cypru oraz Ukrainy (Charków).

Rysunek 2 ukazuje szczegóły 20 najczęściej reprezentowanych afiliacji badawczych w analizowanym korpusie literatury. Widoczna dominacja Azji, zwłaszcza Chin i Indii, może wynikać z dużej liczby publikacji technicznych oraz intensywnego rozwoju krajowych programów AI. Udział Europy, choć mniej liczny, obejmuje ośrodki prowadzące badania nad aspektami etycznymi i regulacyjnymi, co sugeruje zróżnicowanie podejść badawczych zależnie od regionu. Należy zwrócić uwagę na obecność Ukrainy, co może świadczyć o dynamicznym rozwoju kompetencji w obszarze cyberbezpieczeństwa, również wśród naukowców z krajów Europy Wschodniej, gdzie obecnie toczy się wojna.

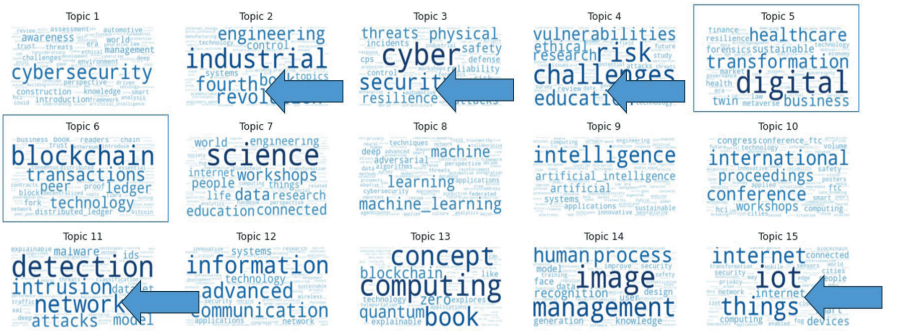


Rysunek 2. Dwadzieścia najczęstszych afiliacji w zebranym zbiorze danych
Źródło: opracowanie własne.

Wyniki automatycznego modelowania tematów w analizowanym korpusie publikacji pozwalają na wyodrębnienie kilku kluczowych obszarów badawczych w dziedzinie cyberbezpieczeństwa. Najsilniej reprezentowane są zagadnienia związane z wykrywaniem intruzów w sieci (intrusion detection) oraz z odpornością systemów informatycznych na różnego rodzaju ataki. W tym kontekście szczególną rolę odgrywają badania poświęcone zarządzaniu ryzykiem, identyfikacji podatności oraz redukcji powierzchni ataku. Istotną część dyskursu zajmują również kwestie bezpieczeństwa infrastruktury przemysłowej oraz zastosowań technologii Internetu Rzeczy (IoT) i przetwarzania brzegowego (edge computing) w kontekście cyberzagrożeń.

Rysunek 3 przedstawia wizualizację tematów uzyskanych za pomocą modelowania nienadzorowanego, gdzie zidentyfikowano kilka wyraźnych klastrów tematycznych. Jeden z najsilniejszych skupia publikacje dotyczące wykrywania intruzów (klaster 11), co potwierdza wagę tego zagadnienia w bieżących badaniach. Widoczne są także klastry związane z bezpieczeństwem fizycznym i infrastrukturą przemysłową (np. klaster 3 – fizyczna ochrona, klaster 15 – IoT), wskazujące na coraz większe zainteresowanie obszarem systemów cyber-fizycznych. Sposób rozmieszczenia dokumentów na rysunku potwierdza również zróżnicowanie podejść – od technicznych po systemowe i organizacyjne.

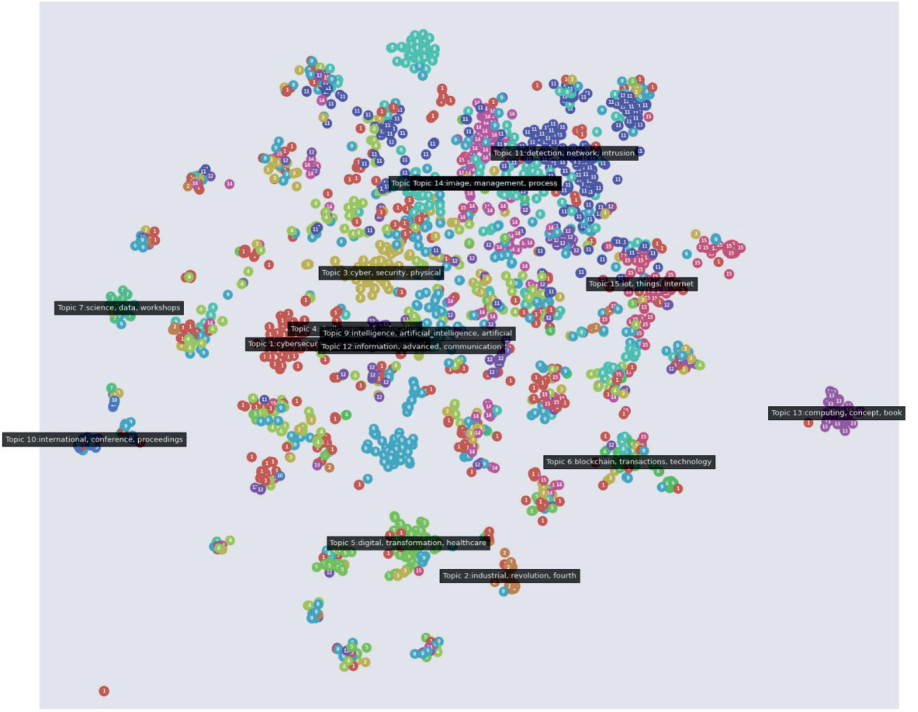
Co interesujące, wśród analizowanych publikacji zauważalna jest obecność tematów związanych z technologią blockchain oraz cyfrową transformacją, szczególnie w sektorze usług zdrowotnych (klaster 5).



Rysunek 3. Automatyczne modelowanie tematów w zbiorze danych
Źródło: opracowanie własne.

Zagadnienia związane z dużymi modelami językowymi, generatywną sztuczną inteligencją oraz dezinformacją nie tworzą jeszcze jednoznacznie wyodrębnionego klastra tematycznego w ramach analizowanego korpusu publikacji. Wydaje się, że publikacje dotyczące tych obszarów są rozproszone w innych obszarach badawczych. Może to świadczyć o ich przekrojowym charakterze, jak również o relatywnie wczesnym etapie integracji metod generatywnej sztucznej inteligencji w badaniach nad cyberbezpieczeństwem.

Natomiast rysunek 4 ilustruje rozkład klastrów tematycznych w przestrzeni dwuwymiarowej zredukowanej przy użyciu technik t-SNE i UMAP. Klaster 1 (kolor czerwony) charakteryzuje się największą dyspersją, co oznacza, że publikacje w jego obrębie są semantycznie heterogeniczne i nie koncentrują się wokół jednego konkretnego zagadnienia. Obecność tematów LLM, GenAI i dezinformacji właśnie w tym klastrze sugeruje ich wieloaspektowość oraz interdyscyplinarny charakter, który przenika zarówno sfery techniczne (np. bezpieczeństwo modeli), jak i społeczne (np. manipulacja informacją). Brak wyraźnego skupienia wskazuje na konieczność dalszych badań w celu lepszego zrozumienia i klasyfikacji tych zjawisk w kontekście cyberbezpieczeństwa.



Rysunek 4. Automatyczne modelowanie tematów w zbiorze danych.
Źródło: opracowanie własne.

Jak wynika z analizy zawartej w tabeli 1, phishing jest najczęściej występującym tematem w badanych publikacjach, odpowiadającym za 16,82% całkowitej liczby prac. Zbliżony udział mają również zagadnienia związane z dużymi modelami językowymi (LLM) oraz narzędziami typu ChatGPT – oba występują z częstotliwością 14,55%. Nieco niższy, choć nadal znaczący odsetek, dotyczy tematyki ataków typu adversarial (14,34%), natomiast kwestie podatności (vulnerabilities) zajmują relatywnie mniejszy udział (3,18%).

Tabela 1. Wyniki analizy tematów (Top 5) w publikacjach dotyczących cyberbezpieczeństwa

Temat	Liczba Publikacji	Procentowy Udział
Phishing	407	16,82%
Adversarial	347	14,34%
ChatGPT	352	14,55%
LLMs	352	14,55%
Vulnerabilities	77	3,18%

Źródło: opracowanie własne.

Tabela 1 przedstawia zestawienie pięciu najczęściej podejmowanych tematów w publikacjach naukowych analizujących zastosowania sztucznej inteligencji w cyberbezpieczeństwie. Dominacja phishingu potwierdza, że zagrożenia związane z inżynierią społeczną nadal są jednym z głównych wyzwań w środowisku cyfrowym. Co interesujące, niemal równy udział tematów związanych z LLM i ChatGPT sugeruje, że badacze rozróżniają specyficzne wyzwania generatywnych chatbotów od ogólnego zagadnienia dużych modeli językowych. Wysoka pozycja tematów związanych z antagonistycznym uczeniem maszynowym (ang. adversarial machine learninig) świadczy o rosnącej świadomości zagrożeń wynikających z manipulowania danymi wejściowymi do systemów SI. Niewielki udział tematów związanych z podatnościami może z kolei świadczyć o niedoreprezentowaniu tej kategorii w analizowanej literaturze lub o trudności klasyfikacyjnej tych prac w ramach bi-gramowego modelowania tematycznego.

Wpływ LLM i GenAI na cyberbezpieczeństwo

W ostatnich latach generatywna sztuczna inteligencja zaczęła odgrywać coraz istotniejszą rolę zarówno w działaniach defensywnych, jak i ofensywnych w cyberprzestrzeni[16]. Modele generatywne, takie jak sieci przeciwnikowe (GAN), architektury typu Transformer oraz duże modele językowe (LLM) – w tym GPT-4 czy Claude – znajdują szerokie zastosowanie w analizie zagrożeń, automatyzacji testów penetracyjnych oraz detekcji podatności w kodzie źródłowy[17]. Jednocześnie, te same mechanizmy są wykorzystywane przez podmioty złośliwe do generowania realistycznych ataków phishingowych, automatycznego przełamywania zabezpieczeń czy tworzenia złożonego złośliwego oprogramowania[18].

Warto podkreślić, że dwuznaczność zastosowań GenAI wymaga nowego podejścia do klasyfikacji zagrożeń – wiele z tych samych narzędzi może być zarówno wsparciem w cyberobronie, jak i komponentem do przeprowadzania

[16] Y. Yigit, W.J. Buchanan, M.G. Tehrani, L. Maglaras, *Review of generative ai methods in cybersecurity*, arXiv preprint arXiv:2403.08701, 2024.

[17] M. Fu, Ch. Tantithamthavorn, Van Nguyen, T. Le, *Chatgpt for vulnerability detection, classification, and repair: How far are we?* In: 2023 30th Asia-Pacific Software Engineering Conference (APSEC) , 632-636. IEEE, 2023.

[18] M. Gupta, A. CharanKumar, A. Kshitiz, E. Parker, L. Praharaj, *From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy,* IEEE Access 11: 80218-80245, 2023.

zautomatyzowanego ataku. Obserwowany rozwój takich technologii zmusza organizacje do ponownego przemyślenia modeli ryzyka i strategii zabezpieczeń, uwzględniających nie tylko skuteczność techniczną, ale również odporność na manipulacje i nadużycia. Pojawia się potrzeba dynamicznych ram regulacyjnych oraz rozwiązań z zakresu cyberodporności, które będą w stanie adaptować organizacje do zmieniającego się charakteru zagrożeń.

Zastosowania sztucznej inteligencji w cyberprzestępczości

Analiza wskazuje, że w ostatnich latach obserwuje się istotną ewolucję złośliwego oprogramowania, katalizowaną przez rozwój dużych modeli językowych. Modele takie jak ChatGPT umożliwiają tworzenie metamorficznego malware[19], dynamicznie modyfikującego swoją strukturę w celu unikania detekcji sygnaturowej i behawioralnej. Przykładowo, malware może zmieniać algorytmy szyfrowania, generować losowo zaciemniony kod przy każdej kompilacji lub rekonfigurować strukturę plików, co znacząco utrudnia analizę i neutralizację. Automatyzacja tych działań przez LLM prowadzi do powstania inteligentnych agentów malware, zdolnych do autonomicznej adaptacji w zależności od środowiska. W połączeniu z powszechnie dostępną infrastrukturą chmurową, złośliwe oprogramowanie może dynamicznie pobierać instrukcje z LLM w czasie rzeczywistym, zyskując wyjątkową elastyczność i trudność wykrycia w systemach produkcyjnych.

Badania[20] dowodzą, że generatywna sztuczna inteligencja może być wykorzystywana do tworzenia zautomatyzowanych narzędzi ransomware, które nie tylko lokalizują i szyfrują dane, lecz także modyfikują swój kod w czasie rzeczywistym, aby unikać detekcji. Szczególnie niepokojące jest osadzanie interpretera Pythona w złośliwym kodzie, umożliwiające dynamiczną komunikację z LLM (np. ChatGPT) w celu generowania nowych fragmentów malware („on-the-fly malware generation"). Powstają również specjalistyczne frameworki, takie jak ThreatGPT, oparte na jailbreakowanych wersjach modeli, które umożliwiają generowanie kodu, scenariuszy ataków, a nawet

[19] P. Madani, *Metamorphic malware evolution: The potential and peril of large language models,* In: 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) , 74-81. IEEE, 2023.

[20] M. Gupta, A. CharanKumar, A. Kshitiz, E. Parker, L. Praharaj, *From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy*, IEEE Access 11: 80218-80245, 2023.

symulację socjotechnicznych interakcji. W połączeniu z lukami sprzętowymi (Meltdown, Spectre), cyberprzestępcy mogą zautomatyzować niemal każdy etap ataku – od wykonania rozpoznania, po jego automatyczne, lub półautomatyczne wykonanie.

Rozwój otwartych modeli językowych (np. Chiński 01.ai[21] oraz publicznych repozytoriów takich jak PentestGPT, ChatGPT_DAN[22] uwidacznia zagrożenia związane z jailbreakami typu „Do Anything Now" (DAN). Umożliwiają one stosunkowo łatwe obchodzenie czasami minimalnych jeszcze zabezpieczeń modeli i wykorzystanie ich jako komponentów złośliwego oprogramowania, np. jak w przypadku wspomnianego ThreatGPT. To w połączeniu z istniejącymi lukami sprzętowymi i wcześniej opisanymi atakami typu ransomware[23] (szyfrującymi dane, np. WannaCry, Ryuk, REvil), czy eraser (NotPetya), tworzą nową klasę zagrożeń.

Podsumowując, LLM-y mogą być więc już obecnie wykorzystywane nie tylko do tworzenia i modyfikacji kodu źródłowego, lecz także do automatyzacji całych łańcuchów ataku, np. poprzez generowanie realistycznych wiadomości phishingowych, czy omijanie systemów ochrony (np. Web Application Firewall). Jako że znacząco ułatwiają one tworzenie zaawansowanych narzędzi ofensywnych i automatyzację działań, zmniejszają one bariery wyjścia i umożliwiają działanie nawet mniej doświadczonym w technologiach informatycznych cyberprzestępcom.

Rozwój mechanizmów obronnych

Wykorzystanie generatywnej sztucznej inteligencji niesie ze sobą również istotne korzyści w dziedzinie cyberbezpieczeństwa. Jednym z kluczowych aspektów jest automatyzacja analizy incydentów bezpieczeństwa. Narzędzia takie jak SecurityLLM i FalconLLM umożliwiają szybkie identyfikowanie wzorców złośliwego kodu w rozległych zbiorach danych[24]. Ponadto, przy pomocy LLMów implementowane są mechanizmy wykrywania deepfake'ów

[21] *Yi Foundation Models*, https://www.01.ai/#yi-foundation-models, [dostęp: 10.05.2025].

[22] *ChatGPT DAN*, https://github.com/0xk1h0/ChatGPT_DAN, [dostęp: 10.05.2025].

[23] *Cloudflare "What are Petya and NotPetya?"*, https://www.cloudflare.com/learning/ security/ ransomware/petya-notpetya-ransomware/, [dostęp: 10.05.2025].

[24] M. A. Ferrag, M. Ndhlovu, N. Tihanyi, L. C. Cordeiro, M. Debbah, T. Lestable, *Revolutionizing cyber threat detection with large language models*, *arXiv preprint arXiv:2306.14263*: 2023, 195-202,

i treści phishingowych, co przyczynia się do ograniczenia skuteczności ataków socjotechnicznych[25].

Sztuczna inteligencja znacząco wspomaga też analizę podatności. Narzędzia pokroju DeepExploit[26] i PentestGPT[27] pozwalają na automatyczne skanowanie i ocenę bezpieczeństwa aplikacji oraz infrastruktury IT. Wraz z postępem technologicznym, coraz większe znaczenie zyskuje automatyczna detekcja kodu malware, realizowana za pomocą systemów AI uczonych na obszernych bazach danych złośliwego oprogramowania[28].

Automatyzacja zadań w cyberbezpieczeństwie obejmuje również analizę logów (LogGPT), automatyczne tworzenie raportów o incydentach oraz wsparcie testów penetracyjnych z wykorzystaniem systemów, takich jak DeepExploit i PentestGPT[29]. Coraz istotniejszą rolę odgrywają także narzędzia wspomagające statyczną i dynamiczną analizę kodu (np. GitHub Copilot, SAST/DAST) oraz systemy do syntetycznego generowania danych na potrzeby uczenia maszynowego (np. PAC-GPT3).

Wzrost liczby defensywnych rozwiązań opartych na GenAI dowodzi, że technologia ta, mimo generowania nowych zagrożeń, stanowi kluczowy element nowoczesnych strategii cyberobrony. Integracja tych systemów z normami zarządzania ryzykiem – takimi jak ISO/IEC 42001 czy dyrektywa NIS2 – jest niezbędna dla zapewnienia zarówno skuteczności operacyjnej, jak

---

[25] S. Enathe VP, Ch. Mouli S, R. Dheepthi, *Llm-enhanced deepfake detection: Dense cnn and multi-modal fusion framework for precise multimedia authentication*. In: 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), IEEE. 2024, 1-6.

[26] A. Sychugov, M. Grekov, *Automated penetration testing based on adversarial inverse reinforcement learning*, In: 2024 International Russian Smart Industry Conference (SmartIndustryCon) , IEEE, 2024, 373-377.

[27] G. Deng, Y. Liu, V. Mayoral-Vilches, P. Liu, Y. Li, Y. Xu, T. Zhang, Y. Liu, M. Pinzger, S. Rass, {PentestGPT}: Evaluating and harnessing large language models for automated penetration testing. In: 33rd USENIX Security Symposium (USENIX Security 24) , 2024, 847–864.

[28] O. Veprytska, V. Kharchenko, AI *powered attacks against ai powered protection: classification, scenarios and risk analysis*, In: 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2022, 1-7.

[29] Q. Jiaxing, S. Huang, Z. Luan, S. Yang, C. Fung, H. Yang, D. Qian, J. Shang, Z. Xiao, Z. Wu, *Loggpt: Exploring chatgpt for log-based anomaly detection*. In: 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), IEEE, 2023, 273-280.

i zgodności z ramami prawnymi i etycznymi. Nowoczesne podejście do bezpieczeństwa informacji wymaga zatem równoległego rozwoju technologicznego oraz wdrożenia mechanizmów kontroli organizacyjnej i audytowalności działań. Wspomniane zastosowania to:

- automatyzacja analizy incydentów (SecurityLLM/FalconLLM),
- generowanie i wykrywanie złośliwego oprogramowania (MalGPT),
- automatyzacja testów penetracyjnych (DeepExploit/PentestGPT),
- automatyzacja analizy logów (LogGPT),
- generowanie i wykrywanie bezpiecznego kodu (SAST/DAST, GitHub Copilot),
- identyfikacja cyberataków: (SecurityLLM/FalconLLM/SecurityBERT),
- generowanie zbiorów danych: PAC-GPT3 do generowania pakietów dla uczenia maszynowego.

Rozwój Standardów Cyberbezpieczeństwa

Wraz z dynamicznym rozwojem i rosnącym znaczeniem generatywnej sztucznej inteligencji i dużych modeli językowych w cyberbezpieczeństwie, imperatywem staje się opracowanie adekwatnych ram regulacyjnych i standardów bezpieczeństwa, koncentrujących się na zarządzaniu ryzykiem związanym z implementacją systemów AI. Kluczowe jest zarówno dostosowanie istniejących norm prawnych i standardów do specyfiki, jak i wypracowanie nowych regulacji dedykowanych temu obszarowi. Niezbędna jest również intensyfikacja współpracy międzynarodowej oraz wymiana doświadczeń w celu skutecznej prewencji zagrożeń wynikających z ewolucji metod sztucznej inteligencji.

Na poziomie Unii Europejskiej, dyrektywa NIS2 oraz norma ISO/IEC 42001 stanowią istotne ramy zarządzania ryzykiem związanym z wdrażaniem SI w organizacjach. Fundamentalnym wyzwaniem pozostaje zabezpieczenie systemów przed potencjalnymi nadużyciami oraz zapewnienie transparentności procesów decyzyjnych realizowanych przez modele generatywne.

W odpowiedzi na zmieniające i zwiększające się ryzyka, obserwuje się implementację nowych regulacji prawnych i standardów bezpieczeństwa. Dyrektywa NIS2 redefiniuje wymogi dotyczące ochrony infrastruktury krytycznej i cyfrowej, natomiast normy ISO/IEC 22989, 23053, 23984 oraz 42001 precyzują zasady zarządzania ryzykiem w kontekście wdrażania AI.

Niniejsza sekcja analizuje kluczowe zmiany w standardach mających implikacje dla cyberbezpieczeństwa. Normy i standardy odgrywają fundamentalną rolę we wspieraniu organizacji w projektowaniu i implementacji bezpiecznych rozwiązań opartych na sztucznej inteligencji. Każda z wymienionych norm ISO odnosi się, w różnym zakresie, do problematyki ryzyka związanego z AI. W kontekście projektowania i wdrażania systemów opartych na AI, zwłaszcza w obszarze cyberbezpieczeństwa, rekomenduje się szczegółowe zapoznanie z wyżej wymienionymi standardami. Zawarte w nich wytyczne i zalecenia mogą zostać przełożone na konkretne mechanizmy kontrolne, stanowiące integralną część dokumentacji polityki bezpieczeństwa. Niezbędna jest systematyczna aktualizacja polityk bezpieczeństwa i ich transpozycja na szczegółowe procedury zarządzania ryzykiem informatycznym, uwzględniająca specyfikę i wykorzystanie nowych metod generatywnych i LLM – w tym zarządzanie kontekstem organizacyjnym oraz wdrożenie własnych, zabezpieczonych i odseparowanych od sieci Internet dużych modeli językowych.

Istotnym wkładem w systematyzację zarządzania ryzykiem związanym z AI jest opracowany przez NIST Artificial Intelligence Risk Management Framework, stanowiący kluczowy dokument dla organizacji zaangażowanych w tworzenie i wdrażanie „bezpiecznej i godnej zaufania" sztucznej inteligencji.

W kontekście regulacji prawnych, dyrektywa NIS2, obowiązująca od 2024 r., wprowadza znaczące zmiany mające na celu podniesienie poziomu bezpieczeństwa sieci i systemów informacyjnych w Unii Europejskiej. Implementuje nowe wymogi dotyczące zarządzania ryzykiem oraz raportowania incydentów, wzmacniając odporność na cyberataki. Sankcje za nieprzestrzeganie dyrektywy mogą sięgać maksymalnie 10 000 000 EUR lub do 2% całkowitego rocznego światowego obrotu danego przedsiębiorstwa, w zależności od tego, która kwota jest wyższa. Dyrektywa obejmuje podmioty istotne (np. dostawców usług cyfrowych, sektory produkcji, przetwórstwa i dystrybucji żywności) oraz niezbędne (w tym administrację publiczną).

Podsumowanie kluczowych, według autora nowych regulacji prawnych i standardów dotyczących sztucznej inteligencji i cyberbezpieczeństwa:

- NIS2: Redefinicja standardów bezpieczeństwa sieci i systemów informacyjnych.
- ISO/IEC 22989:2022: Technologia informacyjna – Sztuczna inteligencja – Pojęcia i terminologia.

- ISO/IEC 23053:2022: Ramy dla systemów SI wykorzystujących uczenie maszynowe.
- ISO/IEC 23984:2023: Technologia informacyjna – Sztuczna inteligencja – Wytyczne dotyczące zarządzania ryzykiem.
- ISO/IEC 42001:2023: Technologia informacyjna – Sztuczna inteligencja – System zarządzania.
- NIST Artificial Intelligence Risk Management Framework.

Należy zauważyć, że NIST Artificial Intelligence Risk Management Framework jest w początkowej fazie rozwoju, a wiele organizacji publikuje własne wytyczne i zasady dotyczące AI, co wskazuje na potrzebę dalszej systematyzacji i standaryzacji regulacji w tym obszarze.

Podsumowanie

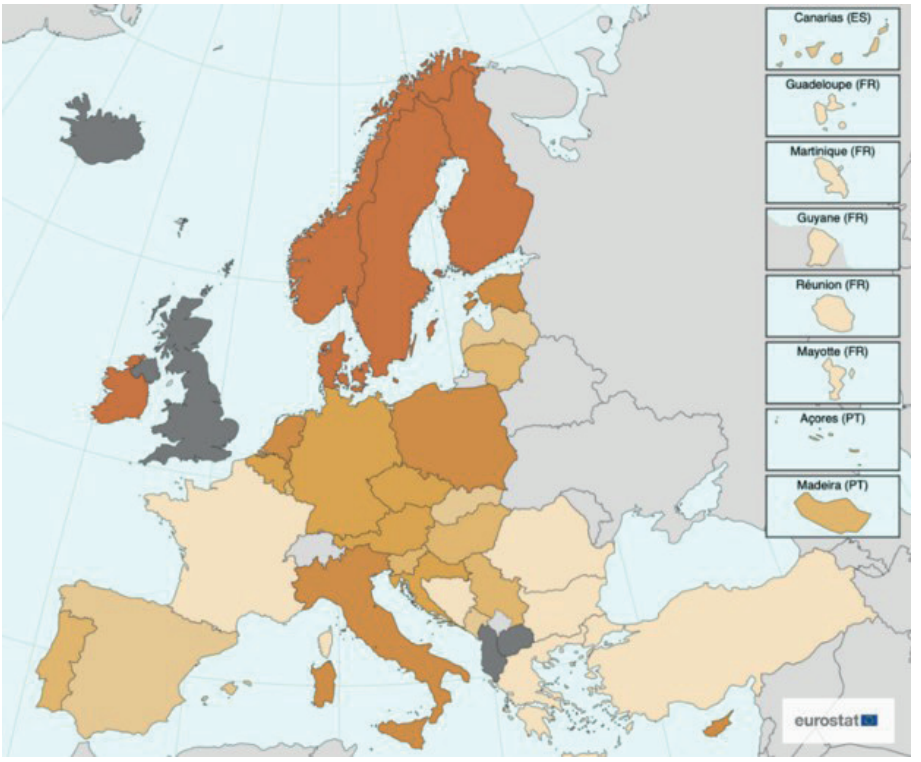
W niniejszym rozdziale przedstawiono wybrane aspekty rozwoju sztucznej inteligencji i jej wpływu na bezpieczeństwo systemów informatycznych, zwracając szczególną uwagę na jej nowe generatywne odmiany. Zaprezentowano przegląd literatury z lat 2017-2024, obejmujący automatyczne modelowanie tematów oraz analizę trendów w publikacjach naukowych dotyczących sztucznej inteligencji i cyberbezpieczeństwa. Dokonano przeglądu ponad 2420 publikacji naukowych z zasobów IEEE Xplore Digital Library i SpringerLink. Wykonana analiza ilustruje wykładniczy wzrost zainteresowania badawczego tematyką sztucznej inteligencji i cyberbezpieczeństwa.

Zdaniem autora, w obliczu rosnącej liczby ataków wykorzystujących sztuczną inteligencję, organizacje powinny inwestować w technologie zabezpieczające systemy oparte na AI oraz rozwijać kompetencje pracowników w zakresie analizy zagrożeń i reagowania na incydenty przy użyciu tych samych metod.

Współpraca publiczno-prywatna oraz wymiana informacji o zagrożeniach będą kluczowe dla skutecznej ochrony. Istotne będzie też dostosowanie istniejących norm zarządzania ryzykiem do specyfiki generatywnej sztucznej inteligencji i LLM oraz opracowanie nowych standardów zarządzania ryzykiem związanych z jej szerokim wdrażaniem. W wyniku analizy ustalono, że współczesne zagrożenia cybernetyczne coraz częściej wykorzystują zaawansowaną sztuczną inteligencję i inżynierię społeczną. Phishing i zautomatyzowane techniki hakowania, np. oferowane przez PentestGPT, stają się bardziej

wyrafinowane, umożliwiając tworzenie bardziej przekonujących wiadomości i skuteczniejszych wektorów ataku. Generowanie złośliwych ładunków, inspirowanych podejściem WannaCry, NotPetya, Ryuk czy Revili ransomware staje się łatwiejsze, co ilustruje potencjał AI w działaniach ofensywnych cyberbezpieczeństwa. Szczególnie groźne stają się techniki polimorficznego malware, skutecznie unikające detekcji, tworzonego przy użyciu (jailbreakowanych) modeli LLM (np. metoda DAN). Ponadto, sztuczna inteligencja znajduje zastosowanie w dekonstrukcji algorytmów kryptograficznych, w tym AES i CHAM, podważając bezpieczeństwo fundamentalnych mechanizmów ochrony danych. Te zjawiska wskazują na zacieranie się granic między defensywą, a ofensywą w cyberprzestrzeni oraz rosnącą rolę nowych metod w tym ekosystemie.

W odpowiedzi na rosnące zagrożenia cybernetyczne, coraz większe znaczenie zyskują zautomatyzowane metody detekcji i analizy anomalii w systemach IT. Przykładem jest wykorzystanie skryptów PowerShell do monitorowania infrastruktury, np. identyfikowania zapytań do baz danych Microsoft SQL obciążających procesor, mogących wskazywać na nieoptymalne działanie lub atak. Rozwijają się również rozwiązania do automatycznej analizy danych o zagrożeniach z wielu źródeł, wspierające szybkie reagowanie i podejmowanie decyzji w zakresie cyberbezpieczeństwa. Integralną częścią proaktywnej ochrony aplikacji są techniki SAST i DAST, pozwalające wykrywać podatności na etapie kodowania i działania aplikacji. Wspólne zastosowanie tych narzędzi zwiększa odporność systemów i ogranicza powierzchnię ataku.



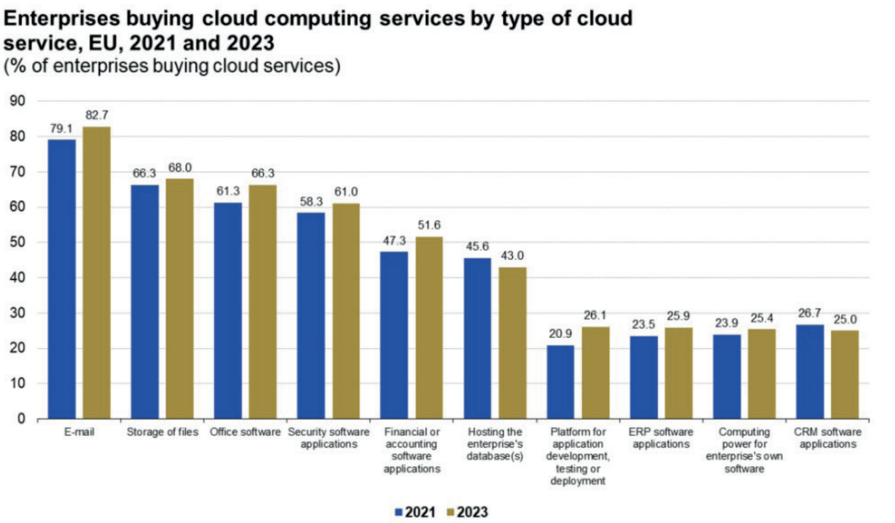
Rysunek 5. Adopcja chmury obliczeniowej w Unii Europejskiej w latach 2021-2023
Źródło: Raport Eurostat (2023) "EU Survey on ICT and e-commerce usage in enterprises".

W tym miejscu warto wspomnieć, że w Polsce w latach 2021-2023 odnotowano zauważalny wzrost wykorzystania publicznej chmury obliczeniowej. W tym czasie na polskim rynku IT nastąpiły znaczące zmiany, w tym powstanie regionu Google Cloud (2021 r.), strefy lokalnej Amazon Web Services (2022 r.) oraz regionu Microsoft Azure (2023 r.) w Warszawie, co według autora mogło przyczynić się do wzrostu zainteresowania chmurą obliczeniową w naszym kraju.

Rysunek 5 przedstawia wyniki badania usług IT i handlu elektronicznego Eurostat (2023 r.) w Unii Europejskiej przeprowadzonego przez Eurostat. Statystyki uzyskano z badań przeprowadzonych przez krajowe urzędy statystyczne w pierwszych miesiącach 2023 r. na próbie około 161 000 przedsiębiorstw zatrudniających 10 lub więcej pracowników lub osób samozatrudnionych (spośród 1,5 miliona takich organizacji w całej UE). Wśród nich 83% stanowiły małe przedsiębiorstwa (10-49 pracowników), 14% średnie (50-249)

i 3% duże (250 lub więcej). Badanie to ukazuje, że w 2023 r. 55,7% polskich przedsiębiorstw korzystało z usług chmury obliczeniowej, co stanowi wzrost o 10,5 punktu procentowego w porównaniu do 2021 r. Polska zajmuje obecnie 10. miejsce w UE pod względem wykorzystania chmury obliczeniowej. Najwyższy odsetek przedsiębiorstw korzystających z usług cloud computing odnotowano w Finlandii (78,3%), Szwecji (71,6%), Danii (69,5%) i na Malcie (66,7%), a najniższy w Grecji (23,6%), Rumunii (18,4%) i Bułgarii (17,5%).

Z badania wiemy też, że zaawansowane usługi przetwarzania w chmurze zakupiło 83,6% dużych przedsiębiorstw, w porównaniu do 77,4% średnich i 74,2% małych przedsiębiorstw korzystających z tych usług. Najczęściej kupowanymi usługami w chmurze obliczeniowej w 2023 r. były proste usługi poczty e-mail (82,7%), przechowywania plików (68%) i oprogramowanie biurowe (66,3%), a także aplikacje zabezpieczające (61,0%), finansowe lub księgowe (51,6%) oraz hosting baz danych (43,0%). Około jedna czwarta firm zakupiła platformy obliczeniowe do tworzenia, testowania lub wdrażania aplikacji (26,1%), oprogramowanie ERP (25,9%), moc obliczeniową do uruchamiania własnego oprogramowania (25,4%) lub oprogramowanie CRM (25,0%), co widać na przytaczanym rysunku 6.



Rysunek 6. Konsumpcja usług chmury obliczeniowej w Unii Europejskiej w latach 2021 i 2023

Źródło: Raport Eurostat (2023) "EU Survey on ICT and e-commerce usage in enterprises".

Autor uważa, że redefiniuje to typowe „granice organizacyjne", które wymagają ochrony. Można więc założyć, że w tak zmieniającym się środowisku, w związku z nowymi metodami i narzędziami SI (GenAI/LLM) większość danych organizacji w UE będzie wkrótce generowanych i przetwarzanych poza tradycyjnymi centrami danych, koncentrując potencjalnie ataki na API systemów i urządzeniach tzw. „przetwarzania brzegowego" tych organizacji. Przetwarzanie brzegowe to model rozproszonych obliczeń, przesuwający obliczenia i przechowywanie danych bliżej ich źródeł, w bardziej rozproszony sposób, co oczywiście dla zespołów cyberbezpieczeństwa generuje nowe wyzwania.

Wracając do wyników, dokonano przeglądu ponad 2420 publikacji naukowych z zasobów IEEE Xplore Digital Library i SpringerLink, koncentrują się one głównie na tematyce (1) phishingu (407 publikacji, 16,82%), (2) adversarial (347 publikacji, 14,34%), (3) ChatGPT (352 publikacji, 14,55%), (4) LLMs (352 publikacji, 14,55%) i podatności (77 publikacji, 3,18%).

Widać wyraźnie, że obecność tematów związanych z szeroko rozumianą generatywną sztuczną inteligencją (LLM i ChatGPT) jest sumarycznie większa (704 dokumenty) niż nacisk kładziony na bardziej tradycyjne metody uczenia maszynowego, w tym zagrożenia związane z manipulowaniem danymi wejściowymi do systemów AI. Tematyka Adversarial to tylko 347 dokumentów.

Sztuczna inteligencja wykazuje rosnący potencjał w cyberbezpieczeństwie, zarówno w obronie, jak i ataku. Wraz z rozwojem tych technologii, organizacje muszą dostosować strategie ochrony przed nowymi zagrożeniami. Kluczowe będzie także opracowanie i wdrożenie nowych regulacji prawnych oraz standardów bezpieczeństwa uwzględniających AI. Czego więc możemy się spodziewać w przyszłości?

- Duże modele językowe mogą zostać zinfiltrowane ze względu na potencjalne niedostateczne zabezpieczenie baz danych.
- Narzędzia oparte na generatywnej sztucznej inteligencji mają potencjał znaczącej zmiany sposobu prowadzenia operacji dezinformacyjnych poprzez masowe tworzenie fałszywych treści.
- Ułatwiona dostępność nowych narzędzi wspiera rozproszone ataki, takie jak DoS, wycieki danych, podmiany stron internetowych i próby zakłócenia infrastruktury krytycznej.
- Zmieniające się środowisko cyberprzestrzeni w Polsce – wzrost znaczenia usług chmury publicznej i przetwarzania brzegowego.

W związku z tym konieczne staje się wdrażanie nowych standardów bezpieczeństwa, uwzględniających nowe metody AI, oraz zmieniające się środowisko działania organizacji (wspomniana adopcja chmury publicznej i przetwarzania brzegowego). Czeka nas również wdrożenie dyrektywy NIS2 i nowych standardów takich jak ISO/IEC 22989:2022, ISO/IEC 23053:2022, ISO/IEC 23984:2023, ISO/IEC 42001:2023, czy NIST Artificial Intelligence Risk Management Framework.

Autor serdecznie dziękuje Wiktorowi Szymanikowi za cenne uwagi, które przyczyniły się do rozwoju niniejszego rozdziału.

Literatura

1. Creswell, Antonia; Tom White, Vincent Dumoulin, Kai Arulkumaran, Biswa Sengupta & Anil A Bharath, *Generative adversarial networks: An overview,* IEEE signal processing magazine 35(1), 2018.
2. Deng, Gelei; Yi Liu, Víctor Mayoral-Vilches, Peng Liu, Yuekang Li, Yuan Xu, Tianwei Zhang, Yang Liu, Martin Pinzger & Stefan Rass, *{PentestGPT}: Evaluating and harnessing large language models for automated penetration testing*. In: 33rd USENIX Security Symposium (USENIX Security 24), 2024.
3. Devlin, Jacob; Ming-Wei Chang, Kenton Lee & Kristina Toutanova, *Bert: Pre-training of deep bidirectional transformers for language understanding*. In: Proceedings of the 2019 conference of the North American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers), 2019.
4. Eurostat, *Cloud computing – statistics on the use by enterprises from the 2023 EU survey on ICT usage and e-commerce in enterprises*. Technical report. Eurostat 2023, https://ec.europa.eu/eurostat/statisticsexplained/index.php
5. Ferrag, Mohamed Amine; Mthandazo Ndhlovu, Norbert Tihanyi, Lucas C Cordeiro, Merouane Debbah & Thierry Lestable, Revolutionizing cyber threat detection with large language models. *arXiv preprint arXiv:2306.14263*, 2023.
6. Fu, Michael; Chakkrit Kla Tantithamthavorn, Van Nguyen & Trung Le, *Chatgpt for vulnerability detection, classification, and repair: How far are we?,* In: 2023 30th Asia-Pacific Software Engineering Conference (APSEC), IEEE, 2023.
7. Goodfellow, Ian J; Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville & Yoshua Bengio, *Generative adversarial nets,* Advances in neural information processing systems 27, 2014.
8. Google, Team, *Gemini: A family of highly capable multimodal models 2024*, https://arxiv.org/abs/2312.11805
9. Gupta, Maanak; CharanKumar Akiri, Kshitiz Aryal, Eli Parker & Lopamudra Praharaj, *From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy*. IEEE Access 11, 2023.

10. Heldens, Stijn; Alessio Sclocco, Henk Dreuning, Ben Van Werkhoven, Pieter Hijma, Jason Maassen & Rob V van Nieuwpoort, *litstudy: A python package for literature reviews*. SoftwareX 20, 2022.
11. Madani, Pooria, *Metamorphic malware evolution: The potential and peril of large language models*. In: 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), IEEE, 2023.
12. McInnes, Leland; John Healy & James Melville, *Umap: Uniform manifold approximation and projection for dimension reduction*. arXiv preprint arXiv:1802.03426, 2018.
13. Miles Brundage, Shahar Avin, Jack Clark Helen Toner Peter Eckersley Ben Garfinkel Allan Dafoe Paul Scharre Thomas Zeitzoff Bobby Filar Hyrum Anderson Heather Roff Gregory C. Allen Jacob Steinhardt Carrick Flynn Seán Ó SJ Beard Haydn Belfield Sebastian Farquhar Clare Lyle Rebecca Crootof Owain Evans Michael Page Joanna Bryson Roman Yampolskiy Dario Amodei, *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Technical report. University of Oxford 2018, https://maliciousaireport.com/.
14. *Framework for improving critical infrastructure cybersecurity*, version 1.1, NIST 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP. 04162018.pdf.
15. Qi, Jiaxing; Shaohan Huang, Zhongzhi Luan, Shu Yang, Carol Fung, Hailong Yang, Depei Qian, Jing Shang, Zhiwen Xiao & Zhihui Wu, *Loggpt: Exploring chatgpt for log-based anomaly detection*. In: 2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), IEEE, 2023.
16. Solaiman, Irene; Miles Brundage, Jack Clark, Amanda Askell, Ariel Herbert-Voss, Jeff Wu, Alec Radford, Gretchen Krueger, Jong Wook Kim, Sarah Kreps, *Release strategies and the social impacts of language models*. arXiv preprint arXiv:1908.09203, 2019.
17. Sychugov, Alexey & Mikhail Grekov, *Automated penetration testing based on adversarial inverse reinforcement learning*. In: 2024 International Russian Smart Industry Conference (SmartIndustryCon), IEEE, 2024.
18. Van der Maaten, Laurens & Geoffrey Hinton, *Visualizing data using t-sn*e. Journal of machine learning research 9(11), 2008.
19. Vaswani, Ashish; Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser & Illia Polosukhin, *Attention is all you need*. Advances in neural information processing systems 30. 2017.
20. Veprytska, Olena & Vyacheslav Kharchenko, *Ai powered attacks against ai powered protection: classification, scenarios and risk analysis*. In: 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), IEEE, 2022.
21. VP, Samesh Enathe; R Dheepthi*, Llm-enhanced deepfake detection: Dense cnn and multi-modal fusion framework for precise multimedia authentication*. In: 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), IEEE, 2024.

mgr inż. Ewa Brodacz
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0002-6469-9159

dr inż. Ewa Stamirowska-Krzaczek
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0002-6653-9055

dr inż. Justyna Siwiela-Tomaszczyk
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0002-2303-9285

Angelika Stopa
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0004-2908-3273

Michał Wrześniewski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0007-5021-8568

https://doi.org/10.29316/9788368103205_4

CYBERZAGROŻENIA W ŁAŃCUCHU DOSTAW ŻYWNOŚCI – WPŁYW CYBERATAKÓW NA SEKTOR ROLNO-SPOŻYWCZY I BEZPIECZEŃSTWO WEWNĘTRZNE PAŃSTWA

CYBER THREATS IN THE FOOD SUPPLY CHAIN – THE IMPACT OF CYBERATTACKS ON THE AGRI-FOOD SECTOR AND NATIONAL INTERNAL SECURITY

Streszczenie

W rozdziale przeanalizowano wpływ cyberzagrożeń na sektor rolno-spożywczy oraz

Summary

This chapter analyzes the impact of cyber threats on the agri-food sector and their

ich konsekwencje dla bezpieczeństwa wewnętrznego państwa. Przedstawiono strukturę współczesnego łańcucha dostaw żywności i opisano główne technologie wykorzystywane w rolnictwie cyfrowym, takie jak Internet rzeczy (IoT), systemy SCM, automatyzacja oraz blockchain. Omówiono kluczowe zagrożenia cybernetyczne, w tym ataki ransomware, sabotaż infrastruktury krytycznej, manipulację danymi oraz szpiegostwo przemysłowe. Wskazano ekonomiczne, społeczne, polityczne, środowiskowe i zdrowotne skutki cyberataków na sektor spożywczy. Zaproponowano strategie budowania odporności sektora, w tym wdrażanie międzynarodowych norm bezpieczeństwa (ISO/IEC 27001, NIST), szyfrowanie danych, szkolenia pracowników i implementację technologii blockchain. Rozdział omawia również dobre praktyki międzynarodowe oraz rekomendacje dla Polski. Podkreślono, że cyberbezpieczeństwo sektora żywnościowego powinno być integralnym elementem strategii bezpieczeństwa narodowego.

Słowa kluczowe: bezpieczeństwo żywnościowe, cyberzagrożenia, sektor rolno-spożywczy, ransomware, blockchain, bezpieczeństwo narodowe

consequences for national internal security. It presents the structure of the modern food supply chain and describes the main technologies used in digital agriculture, such as the Internet of Things (IoT), supply chain management (SCM) systems, automation, and blockchain. Key cybersecurity threats are discussed, including ransomware attacks, sabotage of critical infrastructure, data manipulation, and industrial espionage. The chapter identifies the economic, social, political, environmental, and health impacts of cyberattacks on the food sector. It proposes strategies to enhance sector resilience, including the implementation of international security standards (ISO/IEC 27001, NIST), data encryption, employee training, and blockchain deployment. The chapter also reviews international best practices and provides recommendations for Poland. It emphasizes that cybersecurity in the food sector should be an integral part of national security strategies.

Keywords: food security, cyber threats, agri-food sector, ransomware, blockchain, national security

Wstęp

Współczesne państwa opierają swoją odporność wewnętrzną na wielu filarach. Jednym z kluczowych jest bezpieczeństwo żywnościowe. Stabilny dostęp do żywności, zarówno pod względem ilości, jakości oraz dostępności ekonomicznej, wpływa bezpośrednio na spokój społeczny, stabilność gospodarczą jak i polityczną suwerenność kraju[1]. W dobie globalizacji i postępującej digitalizacji sektor rolno-spożywczy stał się celem cyberataków, które mogą destabilizować dostawy żywności na masową skalę.

[1] J. Clapp, *Food, Politics, and Society: Toward a Critical Research Agenda*, Global Food Security, nr 28, art. 100476, 2021,

Łańcuch dostaw żywności, obejmujący produkcję, przetwórstwo, logistykę, dystrybucję i sprzedaż detaliczną, jest obecnie silnie zależny od technologii informatycznych[2]. Internet rzeczy (IoT), systemy zarządzania łańcuchem dostaw (SCM), blockchain oraz systemy automatyzacji i robotyzacji bez wątpienia usprawniły wiele procesów w sektorze rolno-spożywczym, ale również każdy z tych systemów, mimo korzyści, może stać się potencjalnym celem ataków ze strony cyberprzestępców czy nawet wrogich państw[3].

Narastające zagrożenia cybernetyczne w sektorze rolno-spożywczym to nie tylko problem technologiczny – mogą one realnie wpłynąć na stabilność państwa: od gwałtownych wzrostów cen żywności, poprzez destabilizację społeczną, aż po strategiczne osłabienie suwerenności gospodarczej[4]. Ataki ransomware, sabotaż infrastruktury krytycznej, manipulacja danymi logistycznymi czy cyberatak na inteligentne systemy rolnicze mogą prowadzić do przerw w dostawach podstawowych produktów żywnościowych, wzrostu inflacji, a w skrajnych przypadkach – nawet do kryzysów humanitarnych.

Celem niniejszego rozdziału jest analiza kluczowych cyberzagrożeń w łańcuchu dostaw żywności oraz ocena ich konsekwencji dla gospodarki i bezpieczeństwa narodowego. Ponadto wskazane zostaną możliwe strategie zabezpieczenia sektora rolno-spożywczego oraz przykłady dobrych praktyk na poziomie międzynarodowym.

Niniejszy rozdział został opracowany na podstawie analizy literatury przedmiotu oraz dostępnych danych i raportów dotyczących cyberzagrożeń w sektorze rolno-spożywczym. W procesie badawczym zastosowano metodę przeglądu systematycznego, uwzględniając publikacje naukowe, raporty rządowe, dokumenty organizacji międzynarodowych oraz studia przypadków rzeczywistych incydentów cybernetycznych.

Dobór materiału opierał się na następujących kryteriach:

- publikacje z recenzowanych czasopism naukowych wydanych w latach 2010-2024,
- raporty i wytyczne renomowanych instytucji, takich jak FAO, ENISA, CISA, FDA, OECD, NIST,

[2] B. Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World (Updated Edition)*, W. W. Norton & Company, New York 2020.

[3] National Academies of Sciences, Engineering and Medicine, *Science Breakthroughs to Advance Food and Agricultural Research by 2030*, National Academies Press, Washington 2020.

[4] L. Bodin, L. A. Gordon, *Cybersecurity Risk Management for Critical Infrastructure: A Food Supply Chain Perspective*, Journal of Risk Research, nr 23(7-8), 2020, s. 1048-1060.

- studia przypadków głośnych ataków cybernetycznych na sektor rolno-spożywczy (m.in. atak na JBS Foods),
- opracowania dotyczące zastosowania technologii blockchain, IoT, SCM oraz systemów automatyzacji w rolnictwie i przetwórstwie.

Analiza obejmowała identyfikację kluczowych typów zagrożeń, ocenę ich potencjalnych skutków dla bezpieczeństwa wewnętrznego państw oraz przegląd istniejących strategii prewencji i reagowania. Zastosowano podejście jakościowe, ukierunkowane na syntetyzowanie aktualnego stanu wiedzy oraz formułowanie rekomendacji dla polityk publicznych.

Współczesny łańcuch dostaw żywności i jego podatność na cyberzagrożenia

Struktura łańcucha dostaw żywności

Łańcuch dostaw żywności obejmuje pięć głównych etapów: produkcję, przetwórstwo, logistykę, dystrybucję i sprzedaż detaliczną. Każdy z tych elementów jest w coraz większym stopniu zinformatyzowany i zależny od infrastruktury cyfrowej[5]. Współczesne gospodarstwa rolne wykorzystują precyzyjne systemy zarządzania plonami i zasobami, zakłady przetwórcze polegają na zautomatyzowanych liniach produkcyjnych, a firmy logistyczne oraz sieci handlowe zarządzają zapasami w czasie rzeczywistym.

Rosnąca kompleksowość łańcucha dostaw zwiększa jego podatność na cyberzagrożenia. Rozwój handlu elektronicznego w branży spożywczej oraz rosnące znaczenie platform e-commerce jeszcze bardziej potęgują to ryzyko – jak pokazuje analiza Goik i Ciupak[6], wzrost częstotliwości zakupów żywności online i rozproszenie danych logistycznych wymagają nowego podejścia do bezpieczeństwa cyfrowego w tym obszarze. Wzajemne powiązania pomiędzy różnymi podmiotami (rolnicy, przetwórcy, dystrybutorzy, detaliści) oznaczają, że skuteczny cyberatak na jeden element systemu może doprowadzić do efektu domina i zakłóceń w całym sektorze[7].

---

[5] M. M. Aung, Y. S. Chang, *Traceability in a food supply chain: Safety and quality perspectives*, Food Control, nr 39, 2014, s. 172-184.

[6] D. Goik, M. Ciupak, *Dostawy żywności w systemie e-commerce – ich przyszłość i uwarunkowania*, Problemy Drobnych Gospodarstw Rolnych, nr 2, 2018, s. 23-33.

[7] A. Miremadi, A. Moeini, B. Ajirloo, *IoT-Based Smart Agriculture: Cybersecurity Issues and Challenges*, Journal of Ambient Intelligence and Humanized Computing, 2022.

Technologie wykorzystywane w sektorze rolno-spożywczym

Internet rzeczy (IoT) i inteligentne systemy zarządzania rolnictwem. Internet rzeczy w rolnictwie (Agri-IoT) obejmuje wykorzystanie czujników, dronów, autonomicznych pojazdów i innych urządzeń umożliwiających precyzyjne zarządzanie uprawami, nawadnianiem czy hodowlą zwierząt[8]. Chociaż technologie te zwiększają wydajność i zmniejszają zużycie zasobów, są one narażone na cyberataki, takie jak przejęcie kontroli nad urządzeniami czy manipulacja danymi.

Oprogramowanie do zarządzania łańcuchem dostaw (SCM). Nowoczesne systemy SCM umożliwiają monitorowanie i koordynowanie przepływu surowców i produktów w czasie rzeczywistym. Naruszenia w tych systemach mogą prowadzić do poważnych zakłóceń dostaw, manipulacji zamówieniami, czy fałszowania dokumentacji logistycznej[9].

Automatyzacja i robotyzacja w produkcji żywności. Zakłady przetwórstwa żywności coraz częściej wykorzystują roboty do pakowania, sortowania i kontroli jakości produktów. Zautomatyzowane linie produkcyjne, sterowane cyfrowo, są jednak podatne na ataki typu ransomware lub sabotaż, co może całkowicie sparaliżować produkcję[10].

Blockchain jako potencjalne zabezpieczenie przed fałszerstwami. Blockchain, jako rozproszona baza danych, może zwiększyć przejrzystość i bezpieczeństwo łańcucha dostaw żywności, umożliwiając śledzenie produktów „od pola do stołu”[11]. Jak zauważa Kosior[12], technologia ta może w istotny sposób podnieść wiarygodność informacji o pochodzeniu i jakości żywności, szczególnie w kontekście szybkiej identyfikacji źródeł zagrożeń. Niemniej jednak nie jest ona wolna od słabości – m.in. błędów implementacyjnych

[8] S. Wolfert i in., *Big Data in Smart Farming – A review*, Agricultural Systems, nr 153, 2017, s. 69-80.

[9] H. Min, G. Zhou, *Supply chain modeling: past, present and future*, Computers & Industrial Engineering, nr 43(1-2), 2002, s. 231-249.

[10] F. Tian, Z. Li, Y. Liu, *Food Supply Chain Digitalization: Opportunities and Challenges*, Computers and Electronics in Agriculture, nr 186, 2021, art. 106184.

[11] F. Casino, T. K. Dasaklis, C. Patsakis, *A systematic literature review of blockchain-based applications: Current status, classification and open issues*, Telematics and Informatic,s nr 36, 2019, s. 55-81.

[12] K. Kosior, *Potencjał technologii blockchain w zapewnianiu bezpieczeństwa i jakości żywności*, Żywność. Nauka. Technologia. Jakość, nr 25(4), 2018, s. 22-31.

czy luk w warstwie użytkowej, które mogą zostać wykorzystane przez cyberprzestępców.

Główne luki bezpieczeństwa w systemach cyfrowych sektora spożywczego

Sektor rolno-spożywczy często nie posiada zaawansowanych mechanizmów ochrony cybernetycznej, co czyni go atrakcyjnym celem dla atakujących [13]. Główne luki bezpieczeństwa obejmują:

- niski poziom aktualizacji oprogramowania i firmware'u urządzeń IoT,
- brak szkoleń z zakresu cyberhigieny wśród rolników i pracowników sektora,
- ograniczone inwestycje w cyberbezpieczeństwo w porównaniu z innymi sektorami krytycznymi,
- uzależnienie od zewnętrznych dostawców technologii, co zwiększa ryzyko łańcuchowe.

Główne zagrożenia cybernetyczne w sektorze rolno-spożywczym

Ataki ransomware – paraliżowanie systemów przetwórczych i logistycznych. Jednym z najpoważniejszych zagrożeń dla sektora rolno-spożywczego są ataki typu ransomware. Polegają one na szyfrowaniu systemów informatycznych firmy i żądaniu okupu za ich odblokowanie. Skutki takich ataków są katastrofalne: zatrzymanie produkcji, zakłócenie logistyki, utrata danych produkcyjnych i finansowych.

Przykładem jest atak ransomware na JBS Foods w 2021 r. największego na świecie producenta mięsa, który doprowadził do czasowego zamknięcia zakładów przetwórczych w USA, Kanadzie i Australii[14]. Koszty związane z okupem oraz zakłóceniem łańcucha dostaw szacowano na dziesiątki milionów dolarów. Zestawienia incydentów opracowane przez CSIS[15] wskazują, że liczba cyberataków na sektor spożywczy rośnie, a ich skala coraz częściej obejmuje całe kraje. Ataki ransomware nie tylko wpływają na produkcję i dostawy

[13] N. Kshetri, *Blockchain's roles in strengthening cybersecurity and protecting privacy*, Telecommunications Policy nr 42(4), 2018, s. 327-339.

[14] L. H. Newman, *Hackers Hit the World's Largest Meat Supplier With Ransomware*, *Wired Magazine*, 2021.

[15] Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents*, Washington 2021.

żywności, ale mogą również wywoływać panikę konsumencką i destabilizować rynki rolno-spożywcze[16].

Ataki na infrastrukturę krytyczną. Łańcuch dostaw żywności jest uzależniony od infrastruktury krytycznej, takiej jak dostawy wody, energii elektrycznej i chłodnictwa. Cyberataki na te elementy mogą spowodować masowe straty w sektorze rolnym i spożywczym.

W 2021 r. odnotowano cyberatak na zakład uzdatniania wody w Oldsmar na Florydzie, gdzie hakerzy próbowali zwiększyć poziom ługu sodowego w wodzie do niebezpiecznego poziomu[17]. Choć nie był to atak na sektor spożywczy per se, pokazuje on potencjalne zagrożenia dla bezpieczeństwa żywności i zdrowia publicznego poprzez manipulację infrastrukturą wodną.

Manipulacja danymi i sabotaż łańcucha dostaw. Cyberprzestępcy mogą manipulować danymi w systemach zarządzania łańcuchem dostaw: zmieniać daty przydatności do spożycia, fałszować certyfikaty jakości lub zmieniać trasy dostaw, prowadząc do strat finansowych i ryzyka zdrowotnego dla konsumentów[18]. Sabotaż logistyczny może polegać na przekierowywaniu dostaw na fałszywe adresy lub celowym opóźnianiu transportu łatwo psujących się produktów.

Ataki na inteligentne rolnictwo. Automatyczne systemy nawadniania, nawożenia czy karmienia zwierząt są podatne na przejęcie przez cyberprzestępców. Skutki takich ataków mogą być katastrofalne, np. zatrzymanie podlewania upraw w okresie suszy lub przedawkowanie nawozów, prowadzące do ich zniszczenia[19]. Ataki na inteligentne gospodarstwa mogą mieć także charakter długofalowy – trudny do wykrycia sabotaż, powodujący stopniowe obniżanie plonów i jakości produktów.

Kradzież danych i szpiegostwo przemysłowe. Sektor rolno-spożywczy gromadzi cenne dane: o metodach uprawy, recepturach produktów, dostawcach czy klientach. Kradzież tych danych może służyć zarówno celom komercyjnym, jak i strategicznym. Szpiegostwo przemysłowe w rolnictwie

[16] A. Clopton, *Ransomware: Paralyzing Critical Infrastructure*, Journal of Cybersecurity nr 8(1), 2022, art. 1-14.

[17] U.S. Department of Homeland Security, *CISA Insights: Mitigating Attacks Against Critical Infrastructure*, Washington 2021.

[18] H. Boyes i in., *The Industrial Internet of Things (IIoT): An Analysis Framework*, Computers in Industry nr 101, 2018, s. 1-12.

[19] S. Wolfert i in., *Big Data…, op. cit.*

i przemyśle spożywczym jest coraz częściej notowane, a jego skutki obejmują zarówno bezpośrednie straty finansowe, jak i długofalowe poważne ryzyko utraty konkurencyjności[20].

Skutki cyberataków dla bezpieczeństwa wewnętrznego państwa

Skutki ekonomiczne: wzrost cen żywności i straty w sektorze rolnym i spożywczym. Cyberataki na sektor rolno-spożywczy mogą prowadzić do znaczących strat finansowych. Zakłócenia w produkcji i logistyce powodują wzrost cen produktów spożywczych, a także zmniejszenie podaży na rynku[21]. W przypadku długotrwałych zakłóceń, takich jak ataki ransomware na przetwórnie lub dostawców żywności, skutkiem może być gwałtowna inflacja cen podstawowych produktów. Ponadto straty finansowe ponoszą przedsiębiorstwa sektora – koszty obejmują okup, przestoje produkcyjne, odszkodowania, a także inwestycje w odbudowę i zabezpieczenie systemów[22]. Średni koszt przestoju w sektorze spożywczym może sięgać milionów dolarów dziennie.

Skutki społeczne: panika konsumentów, braki żywnościowe, destabilizacja rynków. W przypadku poważnych zakłóceń w dostawach żywności może dojść do paniki konsumenckiej – podobnie jak obserwowano to podczas pandemii COVID-19 przy brakach papieru toaletowego czy produktów pierwszej potrzeby[23]. Wzrost niepewności prowadzi do wykupywania zapasów, co tylko pogłębia braki i potęguje niestabilność. Zakłócenia w sektorze spożywczym mogą także powodować destabilizację rynków pracy (np. w rolnictwie sezonowym), wzrost bezrobocia w sektorach powiązanych oraz ogólne obniżenie poziomu życia ludności[24]. Jak zauważa IFRC[25], brak dostępu do żywności wynikający z zakłóceń systemowych – w tym cyfrowych – może prowadzić do napięć społecznych i humanitarnych kryzysów. Według UNDRR[26], zakłócenia w sektorach podstawowych, takich jak żywność, mogą prowadzić

[20] D. Manheim, *Cybersecurity and Agriculture: Threats and Impacts*, Journal of Agricultural and Environmental Ethics, nr 31(4), 2018, s. 581-600.

[21] OECD, *Strengthening Agricultural Resilience in the Face of Multiple Risks*, Paryż 2020.

[22] N. Kshetri, *Blockchain's roles…,* op. cit.

[23] D. Laborde i in., *COVID-19 risks to global food security*, Science, nr 369(6503), 2020, s. 500-502.

[24] J. Clapp, *Food, Politics…,* op. cit.

[25] International Federation of Red Cross and Red Crescent Societies (IFRC), *World Disasters Report 2021: Hunger and Food Insecurity*, Genewa 2021.

[26] United Nations Office for Disaster Risk Reduction (UNDRR), *Global Assessment Report on Disaster Risk Reduction*, Genewa 2019.

do tzw. kaskadowych skutków społecznych i destabilizacji funkcjonowania całych regionów.

Skutki polityczne: zagrożenia dla suwerenności żywnościowej. Bezpieczeństwo żywnościowe jest nieodłącznym elementem suwerenności narodowej. Długotrwałe lub powtarzające się cyberataki na sektor rolno-spożywczy mogą zmusić państwa do zwiększonego importu żywności lub zawierania niekorzystnych umów handlowych[27]. Osłabienie własnych zdolności produkcyjnych i logistycznych prowadzi do utraty kontroli nad podstawowymi zasobami strategicznymi, co może być wykorzystywane jako element presji politycznej przez inne państwa lub grupy interesów[28].

Skutki środowiskowe: skutki ataków na systemy nawożenia, pestycydy i gospodarkę wodną. Cyberataki na systemy zarządzania nawożeniem i gospodarką wodną mogą mieć poważne konsekwencje środowiskowe. Niewłaściwe dawkowanie nawozów lub pestycydów może prowadzić do skażenia gleby i wód gruntowych, zniszczenia plonów oraz długofalowego pogorszenia jakości środowiska rolniczego[29]. Uszkodzenie lub sabotaż systemów nawadniania może prowadzić do strat w produkcji rolniczej, a w skrajnych przypadkach – do pustynnienia terenów rolnych.

Skutki zdrowotne: ryzyko zatruć żywności i przerwania dostaw podstawowych produktów. Manipulacja danymi dotyczącymi bezpieczeństwa żywności (takimi jak daty przydatności do spożycia lub parametry przechowywania) może zwiększać ryzyko zatruć żywności[30]. Dodatkowo przerwanie dostaw podstawowych produktów, takich jak mleko, chleb czy mięso, prowadzi do niedoborów żywieniowych w populacji. Ataki mogą również wpływać na ograniczenie dostępu do specjalistycznych produktów żywieniowych dla osób chorych (np. żywność bezglutenowa, żywność medyczna), co stwarza dodatkowe zagrożenia dla zdrowia publicznego.

---

[27] FAO, *The State of Food Security and Nutrition in the World 2021*, Food and Agriculture Organization of the United Nations, Rzym 2021.

[28] D. Barkin, *Food Sovereignty: A Critical Dialogue*, Globalizations, nr 16(7), 2019, s. 1047-1065..

[29] Y. Zhang, R. Deng, J. Weng, *Smart farming cyber security: A review*, Computers and Electronics in Agriculture, nr 140, 2017, s. 297-310.

[30] R. Smith, A. Young, *Food safety vulnerabilities and cybersecurity risks*, British Food Journal, nr 123(12), 2021, s. 4047-4063.

Strategie zabezpieczenia sektora rolno-spożywczego przed cyberatakami

Budowanie odporności cybernetycznej poprzez wdrażanie norm i standardów bezpieczeństwa (np. NIST, ISO/IEC 27001). Podstawowym elementem zabezpieczania sektora rolno-spożywczego jest implementacja uznanych norm bezpieczeństwa informacyjnego. W polskim kontekście działania te wpisują się w założenia ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r., która – jak wskazuje Terlikowski (2018 r.) – wyznacza ramy funkcjonowania krajowych i sektorowych zespołów reagowania na incydenty oraz identyfikuje zagrożenia cyfrowe jako jeden z kluczowych elementów bezpieczeństwa wewnętrznego państwa[31]. Standardy, takie jak ISO/IEC 27001 definiują wymagania dla systemów zarządzania bezpieczeństwem informacji, obejmując audyty ryzyk, zarządzanie incydentami i ciągłość działania[32]. W kontekście polskim szczególnie istotne wydają się wnioski Najwyższej Izby Kontroli (2022 r.), która wskazuje, że mimo istnienia wielu mechanizmów nadzoru nad bezpieczeństwem żywności, systemy te charakteryzują się poważnymi brakami organizacyjnymi i kompetencyjnymi[33]. Ich uzupełnienie – także w zakresie cyberbezpieczeństwa – stanowi jeden z kluczowych warunków zwiększenia odporności sektora na zagrożenia cyfrowe. Dodatkowo wytyczne amerykańskiego Narodowego Instytutu Standaryzacji i Technologii (NIST), takie jak Cybersecurity Framework[34], dostarczają praktycznych narzędzi oceny ryzyk i projektowania planów odporności cybernetycznej w sektorach krytycznych, w tym w łańcuchu dostaw żywności.

Ulepszanie systemów szyfrowania danych i ochrony infrastruktury krytycznej. Wdrożenie zaawansowanych technik szyfrowania transmisji danych (np. szyfrowanie end-to-end) oraz ochrony baz danych może znacząco utrudnić przechwycenie wrażliwych informacji[35]. Konieczne jest również stosowanie segmentacji sieci, ochrony przed atakami typu DDoS oraz zabezpieczenia

[31] T. Terlikowski, *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów*, Zeszyty Naukowe SGSP, nr 71(2), 2018, s. 137-150.

[32] ISO/IEC, *ISO/IEC 27001:2013 Information Security Management Systems – Requirements*, International Organization for Standardization, Genewa 2013.

[33] Najwyższa Izba Kontroli, *System kontroli bezpieczeństwa żywności w Polsce – stan obecny i pożądane kierunki zmian*, Warszawa 2022.

[34] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Gaithersburg 2018.

[35] W. Stallings, *Cryptography and Network Security: Principles and Practice* (7 ed.), Pearson, Boston 2017.

systemów SCADA i ICS, które zarządzają automatyzacją w produkcji i przetwórstwie żywności[36]. Jak podkreśla U.S. Department of Homeland Security[37], sektor żywnościowy powinien być traktowany na równi z innymi sektorami infrastruktury krytycznej w zakresie ochrony przed cyberatakami. Wymaga to wdrażania dedykowanych procedur zarządzania ryzykiem oraz reagowania na incydenty w czasie rzeczywistym.

Współpraca sektora publicznego i prywatnego w zakresie monitorowania cyberzagrożeń. Ze względu na złożoność i transgraniczny charakter zagrożeń, niezbędna jest ścisła współpraca między sektorem prywatnym, instytucjami państwowymi i organizacjami międzynarodowymi[38]. Tworzenie wspólnych centrów reagowania na incydenty (CSIRT), platform wymiany informacji o zagrożeniach (ISAC) oraz publicznych baz danych zagrożeń cybernetycznych (np. MITRE ATT&CK) pozwala na szybsze wykrywanie i neutralizowanie zagrożeń.

Programy szkoleniowe dla rolników, producentów i dystrybutorów żywności. Jednym z najczęstszych wektorów ataku jest człowiek – tzw. czynnik ludzki. W sektorze rolno-spożywczym, gdzie często brakuje zaawansowanej wiedzy informatycznej, edukacja w zakresie podstaw cyberbezpieczeństwa jest kluczowa[39].

Programy szkoleniowe powinny obejmować:

- rozpoznawanie prób phishingu,
- stosowanie silnych haseł,
- aktualizowanie oprogramowania,
- bezpieczne korzystanie z urządzeń IoT.

Implementacja technologii blockchain w śledzeniu dostaw żywności. Blockchain może zwiększyć odporność łańcucha dostaw poprzez transparentność transakcji i niezmienność zapisów danych[40]. Przykładowo: rejestracja każdej partii żywności od produkcji do sprzedaży w rozproszonej sieci bloków danych pozwala na szybkie wykrywanie fałszerstw i sabotażu. Dodatkowo

[36] M. Krotofil, D. Gollmann, *Industrial control systems security: What is happening?*, Industrial Control Systems Security (ICSS) Workshop**,** 2013.

[37] U.S. Department of Homeland Security, *CISA Insights…,* op. cit.

[38] L. Bodin, L. A. Gordon, *Cybersecurity Risk Management…,* op. cit.

[39] SANS Institute, *Security Awareness Report: Managing Human Risk*, 2020.

[40] F. Casino i in., *A systematic literature review…,* op. cit.

zastosowanie smart kontraktów może automatyzować procesy kontroli jakości i płatności.

Przykłady dobrych praktyk i międzynarodowe regulacje.

Polityki cyberbezpieczeństwa w sektorze rolno-spożywczym w USA, UE i Azji. W USA bezpieczeństwo sektora rolno-spożywczego jest jednym z priorytetów w narodowej strategii cyberbezpieczeństwa. Ustawa Food Safety Modernization Act (FSMA) rozszerzyła uprawnienia FDA w zakresie monitorowania i zapobiegania zagrożeniom dla łańcucha dostaw żywności[41]. W 2022 r. Departament Rolnictwa (USDA) opublikował wytyczne dla rolników dotyczące cyberhigieny oraz rozpoczął wdrażanie programów pilotażowych w zakresie cyberodporności gospodarstw rolnych. Dodatkowo inicjatywa Cybersecurity and Infrastructure Security Agency (CISA) wspiera sektor spożywczy poprzez analizy zagrożeń i rekomendacje dotyczące ochrony infrastruktury krytycznej[42].

W UE sektor rolno-spożywczy został zaliczony do sektorów krytycznych w ramach dyrektywy NIS2[43]. Dyrektywa nakłada obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych przez przedsiębiorstwa spożywcze w celu minimalizowania ryzyka cyberzagrożeń. Zgodnie z przewodnikiem dla branży spożywczej (Dyrektywa 2022/2555), producenci żywności są zobowiązani m.in. do przeprowadzania regularnych analiz ryzyka, opracowywania planów ciągłości działania, monitorowania zabezpieczeń u swoich dostawców, a także zgłaszania istotnych incydentów do odpowiednich organów w ciągu 24 godzin od ich wykrycia. Przedsiębiorstwa muszą również prowadzić rejestry działań związanych z cyberbezpieczeństwem, w tym dokumentować szkolenia i audyty[44]. Dodatkowo Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) opracowuje regularne raporty dotyczące zagrożeń w sektorze spożywczym i wytyczne dotyczące budowania odporności cybernetycznej w rolnictwie cyfrowym[45].

[41] U.S. Food and Drug Administration, *Food Safety Modernization Act (FSMA)*, Washington 2011.

[42] CISA, *Cybersecurity Best Practices for the Food and Agriculture Sector*, Washington 2021.

[43] European Union, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, 2022.

[44] Dyrektywa 2022/2555, *Przewodnik dla branży spożywczej – Bezpieczeństwo żywności w praktyce*, Wydawnictwo Wiedza i Praktyka, Warszawa 2024.

[45] ENISA, *Threat Landscape for the Food Sector*, Luksemburg 2022.

W Japonii strategia „Society 5.0" obejmuje budowę bezpiecznego rolnictwa cyfrowego, a rząd finansuje programy wsparcia dla rolników wdrażających bezpieczne systemy IoT[46]. W Chinach rozwój „inteligentnego rolnictwa" jest powiązany z inwestycjami w systemy blockchain i AI zabezpieczające łańcuch dostaw żywności[47].

Przykłady udanych inicjatyw zabezpieczających łańcuch dostaw żywności.

Food Safety Modernization Act (USA). FSMA zmieniła podejście do bezpieczeństwa żywności z reaktywnego na proaktywne, nakładając obowiązek analiz zagrożeń i wdrażania planów prewencyjnych przez producentów i dystrybutorów[48]. W kontekście cyberzagrożeń oznacza to także konieczność oceny ryzyka w systemach cyfrowych.

IBM Food Trust to platforma blockchain umożliwiająca śledzenie produktów żywnościowych od producenta do konsumenta w sposób niezmienny i transparentny[49]. W projekt zaangażowane są takie firmy jak Walmart czy Nestlé, co znacząco poprawia bezpieczeństwo dostaw i szybkość reakcji na potencjalne zagrożenia.

Australian Food and Grocery Council – Cybersecurity Guidelines. Australia przyjęła w 2020 r. wytyczne dla przemysłu spożywczego dotyczące cyberbezpieczeństwa, obejmujące m.in. ochronę systemów SCADA oraz zarządzanie incydentami w łańcuchu dostaw[50].

Rekomendacje dla Polski i innych krajów w zakresie wzmacniania cyberbezpieczeństwa sektora żywnościowego:

- uwzględnienie sektora rolno-spożywczego w krajowych strategiach cyberbezpieczeństwa,
- obowiązkowe audyty cyberbezpieczeństwa dla dużych producentów i przetwórców żywności,
- wspieranie inwestycji w bezpieczne technologie cyfrowe w rolnictwie i logistyce,

[46] Cabinet Office Japan, *Society 5.0 Strategy: Outline and Implementation*, Tokio 2020.

[47] L. Zhou, Y. Zhang, W. Ma, *Smart agriculture: Cybersecurity issues and challenges*, International Journal of Agricultural Sustainability, 2022.

[48] U.S. Food and Drug Administration, *Food Safety Modernization Act (FSMA)…,* op. cit.

[49] IBM, *IBM Food Trust: Blockchain for Food Transparency*, 2021.

[50] Australian Food and Grocery Council, *Cybersecurity Guidelines for the Food and Grocery Industry*, Canberra 2020.

- edukacja i szkolenia z zakresu cyberhigieny dla rolników, przetwórców i handlowców,
- tworzenie krajowych i regionalnych platform wymiany informacji o zagrożeniach.

Podsumowanie

Dzisiejszy łańcuch dostaw żywności, choć bardzo wydajny i oparty na globalnych powiązaniach, staje się coraz bardziej narażony na ataki cybernetyczne. Postępująca cyfryzacja – obejmująca m.in. Internet rzeczy, systemy SCM, automatyzację oraz blockchain – z jednej strony przyspiesza i porządkuje procesy, z drugiej jednak otwiera nowe ścieżki potencjalnych zagrożeń. Warto zaznaczyć, że technologie takie jak blockchain mogą zwiększać bezpieczeństwo danych i ograniczać możliwość fałszerstw, jednak nie stanowią pełnej ochrony przed zaawansowanymi formami cyberataków.

Analiza przeprowadzona w niniejszym rozdziale wskazuje na kilka istotnych wniosków:

- Kluczowe zagrożenia obejmują ataki ransomware, sabotaż infrastruktury krytycznej, manipulację danymi logistycznymi, przejęcie kontroli nad inteligentnymi systemami rolniczymi oraz kradzież danych.
- Wpływ cyberataków na sektor rolno-spożywczy jest wielowymiarowy: od strat finansowych i wzrostu cen żywności, poprzez destabilizację społeczną, aż po zagrożenia polityczne, środowiskowe i zdrowotne.
- Bezpieczeństwo cybernetyczne sektora żywnościowego stało się bezpośrednim elementem bezpieczeństwa wewnętrznego państwa. Utrata kontroli nad produkcją i dystrybucją żywności może prowadzić do utraty suwerenności gospodarczej i wzrostu podatności kraju na presję zewnętrzną.
- Odpowiednie strategie zabezpieczające obejmują wdrażanie międzynarodowych standardów bezpieczeństwa (ISO/IEC 27001, NIST), poprawę ochrony danych, współpracę publiczno-prywatną, programy edukacyjne dla pracowników sektora oraz wdrażanie technologii blockchain.
- Dobre praktyki międzynarodowe pokazują, że skuteczna prewencja wymaga zarówno regulacji prawnych, jak i inwestycji technologicznych oraz budowy świadomości zagrożeń na wszystkich poziomach łańcucha dostaw.

- Rekomendacje dla Polski i innych krajów obejmują stworzenie krajowych programów cyberodporności sektora rolno-spożywczego, obowiązkowe audyty bezpieczeństwa, oraz rozbudowę programów edukacyjnych dla rolników i przetwórców.

W obliczu rosnącego zagrożenia cyberatakami, państwa powinny traktować bezpieczeństwo żywnościowe nie tylko jako element polityki rolnej, lecz przede wszystkim jako fundament bezpieczeństwa narodowego. Rozwój technologii cyfrowych musi iść w parze z rozwojem narzędzi ochrony przed cyberzagrożeniami, aby zapewnić stabilność dostaw żywności i co za tym idzie – ochronę obywateli.

Potrzeba dalszych badań w tym obszarze jest pilna – szczególnie w zakresie oceny skuteczności nowych technologii ochronnych, tworzenia modeli predykcyjnych zagrożeń oraz strategii zarządzania ryzykiem cybernetycznym w sektorze żywnościowym.

Polska, podobnie jak inne kraje, powinna rozwijać zintegrowane strategie prewencji i edukacji. Przykładem dobrych praktyk regionalnych może być Alliance for a Green Revolution in Africa (AGRA), która od 2021 r. publikuje raporty *Food Security Monitor*, analizujące czynniki destabilizujące bezpieczeństwo żywnościowe, w tym także wybrane aspekty zagrożeń cyfrowych w państwach Afryki Subsaharyjskiej[51]. Na poziomie strategicznym podkreśla się również konieczność budowania odporności cybernetycznej jako integralnego elementu zapewniania bezpieczeństwa żywnościowego, co znajduje wyraz m.in. w opracowaniach Agricultural and Food Security Council[52].

Literatura

1. Agricultural and Food Security Council, *Ensuring Food Security through Cyber Resilience*, 2020.
2. Alliance for a Green Revolution in Africa (AGRA), *Food Security Monitor*, 2021.
3. Aung M. M., Chang Y. S., *Traceability in a food supply chain: Safety and quality perspectives*, „Food Control" nr 39, 172-184, 2014.
4. Australian Food and Grocery Council, *Cybersecurity Guidelines for the Food and Grocery Industry*, Canberra 2020.

[51] Alliance for a Green Revolution in Africa, *Food Security Monitor*, Nairobi 2021.

[52] Agricultural and Food Security Council, *Ensuring Food Security through Cyber Resilience*, 2020.

5. Barkin D., *Food Sovereignty: A Critical Dialogue*, „Globalizations" nr 16(7), 1047-1065, 2019.
6. Bodin L., Gordon L. A., *Cybersecurity Risk Management for Critical Infrastructure: A Food Supply Chain Perspective*, „Journal of Risk Research" nr 23(7-8), 1048-1060, 2020.
7. Boyes H., Hallaq B., Cunningham J., Watson T., *The Industrial Internet of Things (IIoT): An Analysis Framework*, „Computers in Industry" nr 101, 1-12, 2018.
8. Cabinet Office Japan, *Society 5.0 Strategy: Outline and Implementation*, Tokio 2020.
9. Casino F., Dasaklis T. K., Patsakis C., *A systematic literature review of blockchain-based applications: Current status, classification and open issues*, „Telematics and Informatics" nr 36, 55-81, 2019.
10. Center for Strategic and International Studies (CSIS), *Significant Cyber Incidents*, Washington 2021.
11. CISA, *Cybersecurity Best Practices for the Food and Agriculture Sector*, Cybersecurity and Infrastructure Security Agency, Washington 2021.
12. Clapp J., *Food, Politics, and Society: Toward a Critical Research Agenda*, „Global Food Security" nr 28, art. 100476, 2021.
13. Clopton A., *Ransomware: Paralyzing Critical Infrastructure*, „Journal of Cybersecurity" nr 8(1), art. 1-14, 2022,
14. ENISA, *Threat Landscape for the Food Sector*, European Union Agency for Cybersecurity, 2022.
15. European Union, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, 2022.
16. FAO, *The State of Food Security and Nutrition in the World 2021*, Food and Agriculture Organization of the United Nations, Rzym 2021.
17. Food and Agriculture Organization of the United Nations (FAO), *Digital Technologies in Agriculture and Rural Areas*, 2020.
18. U.S. Food and Drug Administration, *Food Safety Modernization Act (FSMA)*, Washington 2011.
19. Goik D., Ciupak M., *Dostawy żywności w systemie e-commerce – ich przyszłość i uwarunkowania*, „Problemy Drobnych Gospodarstw Rolnych" nr 2, 2018.
20. IBM, *IBM Food Trust: Blockchain for Food Transparency*, 2021.
21. International Federation of Red Cross and Red Crescent Societies (IFRC), *World Disasters Report 2021: Hunger and Food Insecurity*, Genewa 2021.
22. International Food Policy Research Institute (IFPRI), *Building Resilient Food Systems*, 2020.
23. ISO/IEC, *ISO/IEC 27001:2013 Information Security Management Systems – Requirements*, International Organization for Standardization, Genewa 2013.
24. Kosior K., *Potencjał technologii blockchain w zapewnianiu bezpieczeństwa i jakości żywności*, „Żywność. Nauka. Technologia. Jakość" nr 25(4), 2018.
25. Krotofil M., Gollmann D., *Industrial control systems security: What is happening?*, „Industrial Control Systems Security (ICSS) Workshop", 2013.
26. Kshetri N., *Blockchain's roles in strengthening cybersecurity and protecting privacy*, „Telecommunications Policy" nr 42(4), 1027-1038, 2017.

27. Laborde D., Martin W., Swinnen J., Vos R., *COVID-19 risks to global food security*, „Science" nr 369(6503), 2020.
28. Manheim D., *Cybersecurity and Agriculture: Threats and Impacts*, „Journal of Agricultural and Environmental Ethics" nr 31(4), 2018.
29. Min H., Zhou G., *Supply chain modeling: past, present and future*, „Computers & Industrial Engineering" nr 43(1-2), 2002.
30. Miremadi A., Moeini A., Ajirloo B., *IoT-Based Smart Agriculture: Cybersecurity Issues and Challenges*, „Journal of Ambient Intelligence and Humanized Computing", 2022.
31. Najwyższa Izba Kontroli, *System kontroli bezpieczeństwa żywności w Polsce – stan obecny i pożądane kierunki zmian*, Warszawa 2022.
32. National Academies of Sciences, Engineering and Medicine, *Science Breakthroughs to Advance Food and Agricultural Research by 2030*, Washington 2020.
33. Newman L. H., *Hackers Hit the World's Largest Meat Supplier With Ransomware*, „Wired Magazine", 2021.
34. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg 2018.
35. OECD, *Strengthening Agricultural Resilience in the Face of Multiple Risks*, Paris 2020.
36. SANS Institute, *Security Awareness Report: Managing Human Risk*, 2020.
37. Schneier B., *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (Updated Edition), W. W. Norton & Company, New York 2020.
38. Smith R., Young A., *Food safety vulnerabilities and cybersecurity risks*, „British Food Journal" nr 123(12), 2021.
39. Stallings W., *Cryptography and Network Security: Principles and Practice* (7 ed.), Pearson, Boston 2017.
40. Terlikowski T., *Bezpieczeństwo cyberprzestrzeni wyzwaniem naszych czasów*, „Zeszyty Naukowe SGSP" nr 71(2), 2018.
41. Tian F., Li Z., Liu Y., *Food Supply Chain Digitalization: Opportunities and Challenges*, „Computers and Electronics in Agriculture" nr 186, art. 106184, 2021.
42. U.S. Department of Homeland Security, *CISA Insights: Mitigating Attacks Against Critical Infrastructure*, Washington 2021.
43. United Nations Office for Disaster Risk Reduction (UNDRR), *Global Assessment Report on Disaster Risk Reduction*, Genewa 2019.
44. Wolfert S., Ge L., Verdouw C., Bogaardt M. J., *Big Data in Smart Farming – A review*, „Agricultural Systems" nr 153, 2017.
45. World Economic Forum, *The Future of the Last-Mile Ecosystem*, Geneva 2020.
46. Zhang Y., Deng R., Weng J., *Smart farming cyber security: A review*, „Computers and Electronics in Agriculture" nr 140, 2017.
47. Zhou L., Zhang Y., Ma W., *Smart agriculture: Cybersecurity issues and challenges*, „International Journal of Agricultural Sustainability", 2022.

dr Iwona Lasek-Surowiec
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0002-7231-7993

dr hab. Julia Nowicka
Akademia Sztuki Wojennej
ORCID: 0000-0002-0778-0519

dr Tetiana Strutynska
Przykarpacki Uniwersytet Narodowy im. Wasyla Stefanyka
w Iwano-Frankiwsku
ORCID: 0000-0003-3328-628X

mgr Wiktoria Marcinek
ORCID: 0009-0009-0959-6182

https://doi.org/10.29316/9788368103205_5

ROLA SANKCJI UNIJNYCH W KONFLIKCIE ROSYJSKO-UKRAIŃSKIM 2022-2025. ASPEKTY PRAWNE I MIĘDZYNARODOWE

THE ROLE OF EU SANCTIONS IN THE RUSSIAN-UKRAINIAN CONFLICT 2022-2025. LEGAL AND INTERNATIONAL ASPECTS

Streszczenie

Celem rozdziału jest analiza roli, jaką pełnią sankcje Unii Europejskiej jako instrument prawa międzynarodowego oraz polityki zagranicznej na przykładzie konfliktu rosyjsko-ukraińskiego po 2022 r. Autorka skupia się na podstawach prawnych środków

Summary

The aim of the chapter is to analyze the role of European Union sanctions as an instrument of international law and foreign policy, using the example of the Russia–Ukraine conflict after 2022. The author focuses on the legal foundations of restrictive measures

restrykcyjnych przyjmowanych przez UE wobec Rosji, ich zgodności z międzynarodowymi normami prawnymi oraz efektywności z perspektywy politycznej, gospodarczej i strategicznej. Główna hipoteza badawcza zakłada, że sankcje unijne – mimo, że nie przyniosły natychmiastowego zakończenia agresji – stanowią legalne i skuteczne narzędzie oddziaływania międzynarodowego, przyczyniające się do osłabienia potencjału militarnego i gospodarczego Rosji, a także wzmacniające pozycję UE jako aktora globalnego. W rozdziale zastosowano metodę analizy dogmatyczno-prawnej, dokumentacyjnej i ilościowej, a także elementy studium przypadku – w szczególności dotyczącego kolejnych pakietów sankcji przyjmowanych przez Unię Europejską w latach 2022-2025. Wnioski wskazują, że sankcje unijne wobec Rosji, mimo braku bezpośredniego efektu politycznego, przyczyniły się do strategicznego osłabienia agresora i ograniczenia jego zdolności do eskalacji konfliktu. Dodatkowo, działania UE miały istotne znaczenie dla zachowania jedności wspólnoty międzynarodowej i podkreśliły konieczność dalszej profesjonalizacji oraz instytucjonalizacji polityki sankcyjnej.

Słowa kluczowe: sankcje, UE, Federacja Rosyjska, Ukraina, konflikt zbrojny

adopted by the EU against Russia, their compliance with international legal norms, and their effectiveness from political, economic, and strategic perspectives. The main research hypothesis assumes that EU sanctions – although they have not led to the immediate cessation of aggression – constitute a lawful and effective tool of international influence, contributing to the weakening of Russia's military and economic potential, while also strengthening the EU's position as a global actor. The chapter employs dogmatic-legal, documentary, and quantitative methods, as well as elements of case study analysis - particularly with regard to successive sanctions packages adopted by the European Union between 2022 and 2025. The findings suggest that, despite the absence of a direct political breakthrough, EU sanctions against Russia have contributed to the strategic weakening of the aggressor and have limited its capacity to escalate the conflict. Moreover, the EU's actions have played an important role in maintaining international unity and highlighted the need for further professionalization and institutionalization of the Union's sanctions policy.

Keywords: sanctions, European Union, Russian Federation, Ukraine, armed conflict

Wstęp

Konflikt zbrojny pomiędzy Federacją Rosyjską a Ukrainą, którego nowy etap rozpoczął się 24 lutego 2022 r., stanowi jedno z najpoważniejszych naruszeń prawa międzynarodowego i publicznego od czasu zakończenia II wojny światowej. Agresja Federacji Rosyjskiej przeciwko suwerennemu państwu, będącemu stroną Karty Narodów Zjednoczonych (KNZ)[1], stanowi jaskrawe

[1] *Karta Narodów Zjednoczonych, Statut Międzynarodowego Trybunału Sprawiedliwości i Porozumienie ustanawiające Komisję Przygotowawczą Narodów Zjednoczonych* (Dz. U. z 1947 r. Nr 23, poz. 90 z późn. zm.).

pogwałcenie fundamentalnych zasad prawa międzynarodowego, w szczególności zakazu użycia siły w stosunkach międzynarodowych, wynikającej z art. 2 ust. 4 KNZ. W obliczu tej bezprecedensowej sytuacji społeczność międzynarodowa, a w szczególności Unia Europejska (UE), podjęła działania mające na celu przeciwdziałanie skutkom tej agresji, wyrażające się m.in. w zastosowaniu środków restrykcyjnych (sankcji) wobec Federacji Rosyjskiej oraz podmiotów powiązanych z reżimem odpowiedzialnym za działania wojenne na terytorium Ukrainy.

Od marca 2014 r. Unia Europejska stopniowo wprowadza środki ograniczające wobec Federacji Rosyjskiej w odpowiedzi na kolejne naruszenia prawa międzynarodowego i suwerenności Ukrainy. Sankcje te były reakcją na nielegalną aneksję Krymu w 2014 r., a następnie na rozpoczęcie pełnoskalowej inwazji zbrojnej na Ukrainę w lutym 2022 r. oraz bezprawne przyłączenie do Federacji Rosyjskiej ukraińskich obwodów: donieckiego, ługańskiego, zaporoskiego i chersońskiego. Do maja 2025 r. UE przyjęła szesnaście pakietów sankcyjnych, których głównym celem jest wywarcie maksymalnej presji politycznej i gospodarczej na Rosję, aby ograniczyć jej zdolność do prowadzenia wojny oraz skłonić ją do zakończenia agresji. Unijne środki mają charakter selektywny, tymczasowy i proporcjonalny – są regularnie weryfikowane pod kątem skuteczności i zgodności z celami polityki zagranicznej UE. Mogą zostać zmodyfikowane, złagodzone lub zniesione, jeśli Federacja Rosyjska podejmie wiarygodne działania prowadzące do ich realizacji. Równolegle Unia nałożyła także środki ograniczające wobec państw wspierających rosyjską agresję, w tym wobec Białorusi, Iranu i Korei Północnej[2].

UE, jako organizacja międzynarodowa o charakterze ponadnarodowym, odgrywa istotną rolę jako kreator i egzekutor środków sankcyjnych, stanowiących jeden z instrumentów reakcji na poważne naruszenia prawa międzynarodowego. Sankcje te obejmują między innymi zamrożenie aktywów, zakaz wjazdu na terytorium UE, ograniczenia w zakresie eksportu i importu towarów oraz usług strategicznych (m.in. technologii podwójnego zastosowania), a także zakazy udziału na rynkach kapitałowych[3].

[2] *EU sanctions against Russia*, https://www.consilium.europa.eu/en/policies/sanctions-against-russia/, [dostęp: 30.04.2025].

[3] *Timeline – EU sanctions against Russia*, https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/, [dostęp: 30.04.2025].

Konstrukcja prawna sankcji unijnych, ich zgodność z międzynarodowymi standardami prawnymi oraz efektywność jako narzędzia wpływu politycznego i gospodarczego w stosunkach międzynarodowych, stanowią przedmiot intensywnych analiz naukowych i politycznych. W literaturze przedmiotu podkreśla się, że środki restrykcyjne, choć niewątpliwie nie mają charakteru środka przymusu w rozumieniu rozdziału VII KNZ, są wyrazem polityki „twardego prawa miękkiego oddziaływania" (*hard law of soft power*)[4], pozwalającym UE na oddziaływanie na zachowania państw trzecich oraz podmiotów niepaństwowych bez użycia środków militarnych. Działania te są uzasadniane nie tylko względami prawnymi, lecz również etycznymi i politycznymi, odwołującymi się do wartości, na których opiera się system traktatowy Unii – takich jak demokracja, państwo prawa, prawa człowieka oraz zasada pokojowego rozwiązywania sporów.

W tym kontekście pojawia się potrzeba pogłębionej analizy roli sankcji unijnych jako narzędzia prawa międzynarodowego i prawa UE w reakcji na agresję rosyjską. Celem niniejszego rozdziału jest zatem zbadanie zarówno podstaw prawnych sankcji UE, mechanizmów ich wdrażania, jak i ich zgodności z normami prawa międzynarodowego.

Niniejszy rozdział ma zatem na celu nie tylko przedstawienie aktualnego stanu prawnego i faktycznego w zakresie sankcji unijnych wobec Rosji, ale również ocenę ich skuteczności, spójności z zasadami prawa międzynarodowego oraz wpływu na rozwój instrumentarium polityki zagranicznej UE w dobie kryzysów bezpieczeństwa i erozji ładu międzynarodowego opartego na prawie. Analiza opiera się na źródłach prawa pierwotnego i wtórnego UE, dokumentach organizacji międzynarodowych, literaturze przedmiotu oraz orzecznictwie sądów unijnych, a także na dostępnych raportach i ocenach skutków sankcji publikowanych przez ośrodki analityczne oraz instytucje unijne i międzynarodowe.

Podstawy prawne środków sankcyjnych UE wobec Rosji

W odpowiedzi na zagrożenia dla pokoju i bezpieczeństwa międzynarodowego, UE może przyjmować środki restrykcyjne w ramach wspólnej

[4] E. Hoca, A. Korbayram, *The Methods of Hard Power and Soft Power in International Law*. 10.31410/ERAZ.2023.543, s. 544-545, 2023.

polityki zagranicznej i bezpieczeństwa (WPZiB). Podstawą prawną dla ustanawiania środków sankcyjnych UE przeciw Rosji w związku z wojną w Ukrainie są art. 29 Traktatu o Unii Europejskiej (TUE) oraz art. 215 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE)[5]. Zgodnie z zasadą lojalnej współpracy, o której mowa w art. 4 ust. 3 TUE[6], państwa członkowskie są zobowiązane do zapewnienia skuteczności przyjętych decyzji oraz do powstrzymania się od działań, które mogłyby zagrozić ich realizacji. W ramach WPZiB sankcje przyjmowane są jednomyślnie przez Radę UE[7], co w praktyce oznacza konieczność osiągnięcia konsensusu politycznego wśród wszystkich państw członkowskich – często o zróżnicowanych interesach strategicznych i gospodarczych w relacjach z Rosją.

Rada Unii Europejskiej na podstawie decyzji przyjętej na mocy art. 29 TUE ustanawia wspólne stanowisko w zakresie środków ograniczających (sankcji) wobec państw trzecich, podmiotów lub osób fizycznych. Działanie to stanowi element realizacji celów WPZiB, w tym ochrony wartości Unii, wspierania pokoju oraz wzmacniania bezpieczeństwa międzynarodowego.

W celu nadania sankcjom skutku prawnego wewnątrz Unii, na podstawie art. 215 TFUE, Rada – na wspólny wniosek Wysokiego Przedstawiciela ds. WPZiB oraz Komisji Europejskiej (KE) – przyjmuje odpowiednie rozporządzenia, mające bezpośrednie zastosowanie we wszystkich państwach członkowskich. Oznacza to, że nie wymagają one implementacji do prawa krajowego, co znacząco zwiększa ich efektywność i zapewnia jednolitą egzekucję w całej Unii[8].

---

[5] Art. 29 TUE umożliwia Radzie UE przyjmowanie decyzji w ramach WPZiB, w tym dotyczących sankcji wobec państw trzecich, osób lub podmiotów; art. 215 TFUE pozwala na przyjmowanie rozporządzeń wykonawczych przez Radę (na wniosek Wysokiego Przedstawiciela i Komisji Europejskiej), które nadają sankcjom moc prawną obowiązującą we wszystkich państwach członkowskich.

[6] *„Zgodnie z zasadą lojalnej współpracy Unia i państwa członkowskie, z poszanowaniem i wzajemną pomocą, wykonują zadania wynikające z Traktatów. Państwa członkowskie podejmują wszelkie środki ogólne lub szczególne, odpowiednie do zapewnienia wykonania zobowiązań wynikających z Traktatów lub aktów instytucji Unii. Państwa członkowskie ułatwiają Unii wykonywanie jej zadań i powstrzymują się od wszelkich środków, które mogłyby zagrażać osiągnięciu celów Unii."*

[7] art. 31 ust. 1 Traktatu o Unii Europejskiej (wersja skonsolidowana) (Dz. U. UE. C. z 2016 r. Nr 202).

[8] *Traktat o funkcjonowaniu Unii Europejskiej* (wersja skonsolidowana) (Dz. U. UE. C. z 2016 r. Nr 202, z późn. zm.).

Rozporządzenia te najczęściej dotyczą zamrażania aktywów, zakazów podróży, zakazów eksportu i importu określonych towarów i technologii, ograniczeń w dostępie do rynku kapitałowego czy zakazów świadczenia usług finansowych, konsultingowych czy prawnych. Po raz pierwszy zastosowano w UE mechanizm środków ograniczających w 2014 r. Pierwszym z aktów prawnych w przedmiotowym zakresie było Rozporządzenie Rady (UE) nr 833/2014 – ustanawiające środki ograniczające w związku z działaniami Rosji destabilizującymi sytuację w Ukrainie, które obejmuje m.in. embargo na broń, restrykcje eksportowe na towary podwójnego zastosowania, ograniczenia w sektorze energetycznym i finansowym[9] oraz Rozporządzenie Rady (UE) nr 269/2014 – dotyczące środków wobec osób fizycznych i prawnych odpowiedzialnych za podważanie integralności terytorialnej, suwerenności i niezależności Ukrainy, przewidujące m.in. zamrożenie aktywów oraz zakazy podróży.

Oba te rozporządzenia były wielokrotnie nowelizowane, począwszy od lutego 2022 r., w ramach tzw. pakietów sankcyjnych UE. Sankcje te obejmują dziś m.in. zakaz importu rosyjskiej ropy i węgla, odłączenie rosyjskich banków od systemu SWIFT, sankcje wobec rosyjskich propagandystów oraz ograniczenia w eksporcie zaawansowanych technologii. Są elementem zintegrowanego podejścia Unii do polityki zagranicznej, łączącego środki prawne, dyplomatyczne, gospodarcze i wojskowe, a ich przyjmowanie i przedłużanie wymaga jednomyślności Rady, co czyni je również narzędziem testującym solidarność polityczną państw członkowskich.

Reasumując, środki te obejmują m.in. ograniczenia w handlu towarami o znaczeniu strategicznym (technologie wysokiego ryzyka, surowce energetyczne), zakazy finansowania rosyjskich przedsiębiorstw państwowych,

[9] Consolidated text: *Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, Access initial legal act (Legal status of the document In force) ELI: http://data.europa.eu/eli/reg/2014/833/2025-02-25, dostęp 5 maja 2025 r.; Rozporządzenie 833/2014 było podstawą dla kolejnych pakietów sankcji, które rozszerzały jego zakres, w tym:
Rozporządzenia 2022/328 z 25 lutego 2022 r. (wprowadziło dodatkowe ograniczenia, m.in. zakaz świadczenia usług finansowych i technicznych dla rosyjskiego sektora naftowego oraz ograniczenia w dostępie do unijnego rynku kapitałowego dla rosyjskich instytucji finansowych i rządu Rosji), Rozporządzenie 2022/879 z 3 czerwca 2022 r. (rozszerzyło sankcje o zakaz świadczenia na rzecz Rosji usług księgowych, rachunkowych, audytowych, doradztwa podatkowego, doradztwa biznesowego i w zakresie zarządzania oraz usług public relations), czy Rozporządzenie 2024/1428 z 17 maja 2024 r. (wprowadziło kolejne zmiany, dostosowując środki ograniczające do aktualnej sytuacji geopolitycznej).

restrykcje w zakresie usług doradczych, prawnych, audytorskich oraz zakaz świadczenia usług w sektorze naftowym i gazowym. Kluczowym aspektem tych regulacji jest również zamrażanie aktywów oraz zakaz udostępniania środków finansowych osobom fizycznym i prawnym znajdującym się na tzw. czarnej liście UE[10].

Z perspektywy prawnej sankcje unijne wobec Federacji Rosyjskiej dzielą się na dwie główne kategorie: sankcje indywidualne i sektorowe.

Każda z kategorii sankcji opiera się na odpowiednio sprecyzowanej podstawie prawnej w decyzji Rady i rozporządzeniu implementacyjnym, co pozwala zapewnić zarówno ich skuteczność, jak i zgodność z zasadą legalizmu oraz wymogami proporcjonalności.

Zestawienie sankcji znajduje się w poniżej.

Tabela 1. Sankcje UE wobec Rosji (2014-2025)

Kategoria	Zakres przedmiotowy sankcji
Sankcje indywidualne	Zamrożenie aktywów i zakaz wjazdu dla osób fizycznych i prawnych uznanych za odpowiedzialne za: agresję wobec Ukrainy, okupację Krymu i Donbasu, deportacje dzieci, zbrodnie wojenne, dezinformację, wsparcie finansowe dla reżimu Putina. Obejmuje m.in. W. Putina, S. Ławrowa, gubernatorów, dowódców wojskowych, członków Dumy, propagandystów, oligarchów, krewnych elit.
Sankcje sektorowe: finansowe	Odłączenie głównych rosyjskich banków (Sberbank, VTB, Bank Rossija itd.) od SWIFT. Zakaz wszelkich transakcji z Bankiem Centralnym Rosji, Narodowym Funduszem Dobrobytu i Ministerstwem Finansów FR. Zakaz inwestowania w rosyjskie papiery wartościowe, obrót euroobligacjami, nowymi obligacjami państwowymi. Zakaz świadczenia usług powierniczych, księgowych, audytorskich i doradczych w sektorze finansowym. Zakaz świadczenia usług kryptowalutowych dla rosyjskich osób i firm.
Sankcje – w zakresie energetyki	Zakaz importu ropy (transportowanej drogą morską), produktów rafinowanych, węgla, LNG i LPG z Rosji. Zakaz świadczenia usług związanych z eksploracją, wydobyciem, rafinacją i transportem surowców energetycznych. Zakaz dostarczania technologii i sprzętu dla sektora energetycznego (np. dla projektów arktycznych i głębinowych). Zakaz reeksportu rosyjskiego LNG przez terminale UE do państw trzecich.

[10] *Council Regulation (EU) 2025/395 of 24 February 2025 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine* ST/5462/2025/INIT, OJ L, 2025/395, 24.2.2025, ELI: http://data.europa.eu/eli/reg/2025/395/oj, [dostęp: 10.05.2025].

Kategoria	Zakres przedmiotowy sankcji
Sankcje transportowe	Całkowity zakaz lądowania, startu i przelotu nad UE dla rosyjskich statków powietrznych, w tym prywatnych odrzutowców oligarchów. Zakaz dostępu rosyjskich statków (handlowych, kontenerowych, tankowców) do portów UE. Zakaz wjazdu rosyjskich przewoźników drogowych na teren UE. Zakaz eksportu technologii i części zamiennych do samolotów, dronów, rakiet, a także komponentów do systemów nawigacyjnych.
Sankcje w – zakresie obrony i przemysłu	Zakaz eksportu wszelkiego sprzętu wojskowego i podwójnego zastosowania (technologie komunikacyjne, mikroprocesory, półprzewodniki, optoelektronika, komponenty radarowe). Zakaz dostarczania dronów i ich części (w tym czujników, kamer, żyroskopów). Zakaz świadczenia usług naprawczych, doradczych i transferu technologii w sektorze zbrojeniowym. Zakaz udziału w rosyjskich projektach zbrojeniowych.
Sankcje w zakresie handlu surowcami	Zakaz importu surowców i produktów z Rosji: stal i żelazo, aluminium, węgiel, drewno, cement, guma, złoto, diamenty, nawozy, produkty rafinowane, tworzywa sztuczne, alkohole, kosmetyki, papierosy, kawior, owoce morza. Zakaz eksportu towarów luksusowych (zegarki, auta, jachty), technologii przemysłowych, narzędzi i obrabiarek, maszyn CNC, elektroniki przemysłowej. Zakaz współpracy w przemyśle chemicznym i górniczym.
Sankcje w zakresie usług	Zakaz świadczenia usług w zakresie: księgowości, audytu, konsultingu, doradztwa prawnego, doradztwa podatkowego, architektury i inżynierii, reklamy, badań rynku, doradztwa IT, usług trustowych i związanych z kryptowalutami. Zakaz doradztwa strategicznego dla podmiotów rosyjskich oraz firm zależnych od rosyjskiego kapitału.
Sankcje w zakresie mediów i propagandy	Zakaz retransmisji, emisji i działalności medialnej dla prorosyjskich mediów: RT, Sputnik, Rossiya RTR, Rossiya 24, TV Centre, REN TV, NTV, VGTRK i inne. Zakaz świadczenia usług reklamowych, produkcyjnych i PR-owych dla rosyjskich nadawców. Dezaktywacja licencji medialnych i zakaz dystrybucji online.
Sankcje w zakresie terytoriów okupowanych	Zakaz importu towarów z okupowanych terytoriów Ukrainy (Krym, Donieck, Ługańsk, Zaporoże, Chersoń). Zakaz eksportu towarów i technologii do tych regionów. Zakaz inwestycji i świadczenia usług turystycznych oraz doradczych. Ograniczenia dla firm operujących na tych terenach i pośredników.

Kategoria	Zakres przedmiotowy sankcji
Zamrożenie aktywów państwowych	Zamrożenie ponad 200 mld EUR aktywów Banku Centralnego Rosji i jednostek państwowych. UE rozważa wykorzystanie nadzwyczajnych zysków z tych aktywów na odbudowę Ukrainy i pomoc militarną.
Środki zabezpieczające przed obejściem sankcji	Sankcje wobec firm i osób z państw trzecich (Turcja, Kazachstan, ZEA, itd.) wspierających Rosję w obchodzeniu sankcji. Zakaz reeksportu towarów o znaczeniu strategicznym dla armii rosyjskiej. Obowiązek zawierania w kontraktach klauzul zakazujących reeksportu do Rosji. Lista towarów „wrażliwych" obejmuje elektronikę, chipy, drony, technologie wojskowe.

Źródło: opracowanie własne na podstawie https://www.sanctionsmap.eu/#/main, [dostęp: 10.05.2025].

Zgodność sankcji unijnych wobec Rosji z prawem międzynarodowym

Sankcje międzynarodowe – zarówno te przyjmowane przez organizacje uniwersalne, jak i regionalne – stanowią instrument oddziaływania politycznego i prawnego, który nie ma charakteru użycia siły w rozumieniu KNZ[11].

W świetle dominującego stanowiska w literaturze prawa międzynarodowego, środki sankcyjne (*restrictive measures* lub *countermeasures*) mogą być stosowane w odpowiedzi na tzw. poważne naruszenia prawa międzynarodowego (*serious breaches of peremptory norms*) i mają na celu wymuszenie zmiany zachowania podmiotu dopuszczającego się naruszeń[12].

Sankcje przyjmowane przez UE wobec Federacji Rosyjskiej po 24 lutego 2022 r. stanowią odpowiedź na rażące naruszenie norm o charakterze bezwzględnie obowiązującym (*ius cogens),* takich jak zakaz użycia siły, zakaz aneksji terytorium siłą oraz obowiązek poszanowania suwerenności i integralności terytorialnej państw. Tym samym, działania UE wpisują się w ogólnie akceptowane ramy dopuszczalnych reakcji wspólnoty międzynarodowej wobec bezprawia międzynarodowego, przewidzianych m.in. w artykułach

[11] art. 2 ust. 4 KNZ.

[12] Więcej: ILC, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, art. 40-41 https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf, [dostęp: 5 maja 2025].

o odpowiedzialności państw za czyny międzynarodowo bezprawne, przyjętych przez Komisję Prawa Międzynarodowego ONZ w 2001 r.[13]

Z perspektywy międzynarodowej kluczowe znaczenie dla oceny sankcji unijnych mają zasady legalności, proporcjonalności i niedyskryminacji. Sankcje nie mogą mieć charakteru arbitralnego, a ich stosowanie powinno opierać się na obiektywnie weryfikowalnych przesłankach, uzasadniających odpowiedzialność danego podmiotu (państwowego lub niepaństwowego). UE, przyjmując sankcje wobec Rosji, każdorazowo wskazuje motywy prawne i polityczne danej decyzji – odwołując się do dokumentacji ONZ, stanowisk OBWE, dowodów naruszeń prawa humanitarnego oraz rezolucji Parlamentu Europejskiego[14].

W doktrynie prawa międzynarodowego uznaje się również, że środki sankcyjne nie powinny prowadzić do nieuzasadnionych cierpień ludności cywilnej, a ich celem nie może być „zbiorowa kara"[15]. W przypadku UE nie wprowadza się sankcji humanitarnych (np. ograniczeń w dostępie do żywności czy leków), co odróżnia ją np. od kompleksowych sankcji przyjmowanych przez Radę Bezpieczeństwa ONZ w latach 90. XX w. Działania UE mają zatem charakter selektywny i ukierunkowany, zgodnie z zasadą *targeted sanctions*[16].

Chociaż wyłączną kompetencję do podejmowania sankcji z mocą wiążącą dla całej społeczności międzynarodowej posiada Rada Bezpieczeństwa ONZ na podstawie Rozdziału VII Karty NZ, to organizacje regionalne i państwa

---

[13] T. Ruys*, Sanctions*, *Retorsions and Countermeasures: Concepts and International Legal Framework* (April 8, 2016). Forthcoming in Larissa van den Herik (ed.), Research Handbook on UN sanctions and international law (Edward Elgar Publishing) (2016), available at https://ssrn.com/abstract=2760853 or http://dx.doi.org/10.2139/ssrn.2760853, [dostęp: 04.05.2025].

[14] OBWE, *Raport Misji Obserwacyjnej OBWE na Ukrainie*, różne edycje od 2014 r., raport z 2022 r.: https://www.osce.org/ukraine-smm/reports, [dostęp: 10 maja 2025]; *Decyzja Rady (WPZiB) 2022/327 z dnia 25 lutego 2022 r. w sprawie zmiany decyzji 2014/512/WPZiB dotyczącej środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*; Parlament Europejski, *Rezolucja z dnia 2 marca 2022 r. w sprawie rosyjskiej agresji na Ukrainę* (2022/2564(RSP), P9_TA(2022)0052.

[15] A. Hofer, *Unilateral Sanctions As A Challenge To The International Legal Order*, https://research-portal.uu.nl/ws/portalfiles/portal/234166919/10.4324_9781003387589-4_chapterpdf.pdf, s. 74-75, [dostęp: 12.05.2025].

[16] Rada Bezpieczeństwa ONZ, *Rezolucja nr 661 (1990)* w sprawie Iraku i Kuwejtu, S/RES/661 (1990), przyjęta 6 sierpnia 1990 r., wprowadzająca kompleksowe sankcje wobec Iraku, w tym ograniczenia importu żywności i leków; zob. też: Komitet Praw Człowieka ONZ, *Uwagi ogólne nr 31*, CCPR/C/21/Rev.1/Add.13 (2004), par. 8.

indywidualnie są uprawnione do podejmowania środków jednostronnych lub wielostronnych – o ile nie naruszają one obowiązujących norm traktatowych ani nie stanowią obejścia zakazów prawa międzynarodowego. W związku z impasem decyzyjnym w Radzie Bezpieczeństwa – ze względu na prawo weta Federacji Rosyjskiej jako stałego członka, UE – działając w porozumieniu z partnerami międzynarodowymi – wzięła na siebie część odpowiedzialności za przeciwdziałanie dalszej destabilizacji ładu międzynarodowego[17].

Warto przy tym zaznaczyć, że sankcje unijne są zgodne z celami KNZ, w szczególności z art. 1 ust. 1 i 2, który wskazuje na konieczność utrzymywania międzynarodowego pokoju i bezpieczeństwa, a także rozwijania przyjaznych stosunków między narodami, opartych na zasadzie równouprawnienia i samostanowienia. Tym samym środki te mają charakter legitymizowany i defensywny – nie zaś agresywny lub ofensywny.

Osoby fizyczne i prawne objęte sankcjami unijnymi mają możliwość zaskarżenia decyzji Rady do Trybunału Sprawiedliwości Unii Europejskiej (TSUE), co jest istotnym elementem zapewnienia zgodności sankcji z zasadą państwa prawa[18].

Analogiczne standardy stosowane są wobec sankcji nakładanych na rosyjskich oligarchów, polityków i przedsiębiorstwa państwowe. W latach 2022-2025 liczne podmioty rosyjskie zaskarżały decyzje Rady UE do TSUE, domagając się ich unieważnienia. W zdecydowanej większości przypadków skargi te były oddalane, ponieważ Rada wykazała istnienie wystarczająco wiarygodnych przesłanek wskazujących na powiązania tych osób z działaniami wspierającymi agresję na Ukrainę[19].

---

[17] Patrz: A. Kociołek-Pęksa, J. Menkes, *Problematyka sankcji i countermeasures w prawie międzynarodowym publicznym – wymiar filozoficznoprawny*, Szkoła Główna Handlowa w Warszawie, http://repozytorium.uni.wroc.pl/Content/89896, [dostęp: 09.05.2025].
B. Ziemblicki , *Sankcje gospodarcze z perspektywy prawa międzynarodowego*, [w:], Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego, 2024, Vol. XXII, s. 1-19.

[18] art. 263 TFUE.

[19] Wyrok Sądu (pierwsza izba w składzie powiększonym) z dnia 20 grudnia 2023 r. w sprawie T313/22, *Roman Arkadyevich Abramovich przeciwko Radzie Unii Europejs*kiej Dokument 62022TJ0313, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:62022TJ0313_RES; Wyrok Trybunału (dziesiąta izba) z dnia 13 marca 2025 r. w sprawie C-271/24, *Igor Shuvalov przeciwko Radzie Unii Europejskiej,* https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:62024CJ0271, [dostęp: 01.05.2025].

Analiza skutków i efektywności sankcji unijnych wobec Rosji w latach 2022-2025

Ocena skuteczności sankcji gospodarczych i politycznych stosowanych przez UE wobec Federacji Rosyjskiej, licząc od pełnoskalowego ataku na Ukrainę z lutego 2022 r., musi opierać się na złożonej analizie zarówno bezpośrednich skutków ekonomicznych, jak i długofalowego oddziaływania na zachowanie państwa objętego restrykcjami.

Przyjmuje się, że o efektywności sankcji decydują cztery główne kryteria[20]:

- celowość (*policy change/behavioral change*) – czy sankcje służą osiągnięciu jasno zdefiniowanego celu politycznego,
- skuteczność gospodarcza (*economic impact*) – czy sankcje wywierają istotny wpływ na kluczowe sektory gospodarki objętego nimi państwa,
- odporność na obchodzenie *(resilience against sanctions circumvention)* – czy podjęto odpowiednie środki przeciwdziałające próbom obejścia sankcji,
- koszty uboczne (*humanitarian and political side effects*) – czy sankcje nie powodują nadmiernych szkód dla państw stosujących środki restrykcyjne oraz dla ludności cywilnej w państwie objętym sankcjami.

W okresie od 24 lutego 2022 r. do 2025 r. Unia Europejska przyjęła 16 pakietów sankcyjnych, obejmujących setki podmiotów i sektory strategiczne. W wyniku tych działań odnotowano szereg istotnych skutków ekonomicznych[21].

Przede wszystkim nastąpiła izolacja finansowa Rosji, m.in. z związku z zamrożeniem rezerw walutowych Banku Centralnego Rosji (ok. 300 mld USD), wykluczeniem kluczowych banków z systemu SWIFT oraz zakaz operowania na europejskich rynkach finansowych, co znacząco utrudniło

[20] Patrz: G. C. Hufbauer, J. J. Schott, K. A. Elliott, B. Oegg, *Economic Sanctions Reconsidered*, 3rd Edition, Peterson Institute for International Economics, Washington, DC November 2007, https://dl1.cuni.cz/pluginfile.php/863435/mod_resource/content/0/Gary%20Clyde%20Hufbauer%2C%20Jeffrey%20J.%20Schott%2C%20Kimberly%20Ann%20Elliott%2C%20Barbara%20Oegg-Economic%20Sanctions%20Reconsidered%20(2008).pdf, [dostęp: 10.05.2025]; A. Bojinović Fenko, J. Brsakoska Bazerkoska, *The EU as a Global Actor: The Significanceof Changes in the World Order From 2004 to 2024 as Regards EU Actorness*, DOI: 10.33067/SE.2.2024.1, https://journalse.com/pliki/pw/2-2024-Bojinovic.pdf, [dostęp: 09.05.2025].

[21] https://www.consilium.europa.eu/pl/infographics/impact-sanctions-russian-economy/, [dostęp: 01.05.2025].

stabilizację rosyjskiego rubla i zwiększyło koszty transakcyjne dla rosyjskich przedsiębiorstw[22]. Wykluczenie banków rosyjskich i białoruskich z systemu SWIFT jest istotnym narzędziem sankcyjnym, skutkującym ograniczeniem ich zdolności do realizacji transakcji międzynarodowych. Objęcie tym środkiem 23 banków z Federacji Rosyjskiej oraz 4 z Republiki Białorusi oznacza, że instytucje te zostały pozbawione możliwości przesyłania i odbierania płatności za pośrednictwem tej kluczowej infrastruktury finansowej[23]. W praktyce oznacza to, że banki objęte sankcjami tracą możliwość swobodnego pozyskiwania walut obcych, ponieważ transfer środków między instytucjami finansowymi zazwyczaj wymaga udziału banków zagranicznych, pełniących rolę pośredników. Dodatkowo, niemożność przesyłania aktywów poza granice kraju prowadzi do pogłębienia trudności finansowych zarówno w Rosji, jak i na Białorusi, ograniczając ich integrację z międzynarodowym systemem finansowym.

Utrata dostępu do rynków kapitałowych UE doprowadziła do pogłębienia deficytu budżetowego w latach 2023-2024. Osłabiony został sektor energetyczny, m.in. w związku ze stopniowym embargiem UE na import rosyjskiej ropy naftowej (w tym produktów rafinowanych) oraz zakaz świadczenia usług transportowych i ubezpieczeniowych dla dostaw morskich, co z kolei spowodowało konieczność przekierowania eksportu Rosji na rynki azjatyckie z dużym dyskontem cenowym. W efekcie dochody z sektora naftowo-gazowego, stanowiącego ponad 40% budżetu Rosji, uległy zmniejszeniu o około 25-30% rocznie w porównaniu z okresem sprzed wojny[24].

Sankcje znacząco uderzyły w przemysł zbrojeniowy i wysokich technologii. Zakaz eksportu do Rosji komponentów elektronicznych, mikroprocesorów, technologii lotniczych, dronowych i morskich utrudnił produkcję nowoczesnego uzbrojenia i sprzętu wojskowego. Rosja zmuszona była do

[22] A. Moiseienko, *Frozen Russian State Assets: The Key to Enforcing the Largest Financial Debt of Our Times, VerfBlog,* 2025/4/04, https://verfassungsblog.de/frozen-russian-state-assets/, DOI: 10.59704/8b6611ae95a1a8be, [dostęp: 12.05.2025].

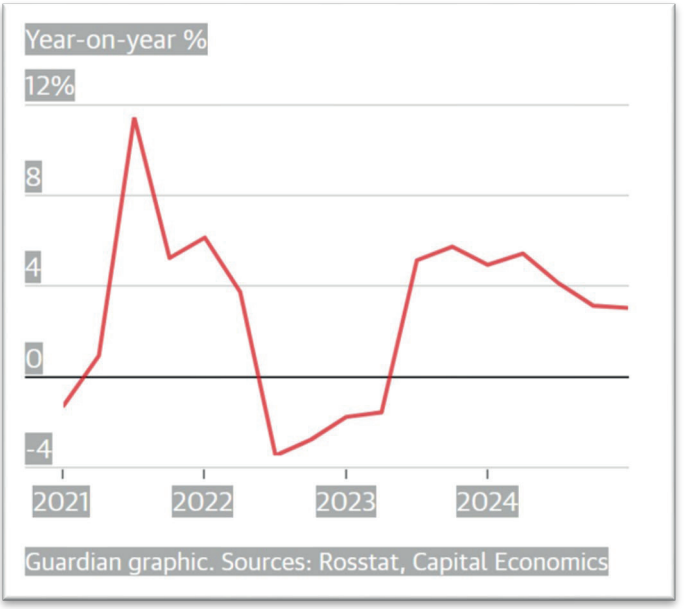
[23] System SWIFT (*Society for Worldwide Interbank Financial Telecommunication*) pełni funkcję globalnej platformy komunikacyjnej, umożliwiającej wymianę informacji między bankami oraz innymi instytucjami finansowymi na całym świecie. Zrzesza on ponad 11 tysięcy podmiotów w skali globalnej i jest powszechnie wykorzystywany do obsługi transakcji transgranicznych, https://www.swift.com/?utm, [dostęp: 07.05.2025].

[24] Według danych IEA, w styczniu 2023 roku dochody Rosji z eksportu ropy i gazu spadły o około 30% w porównaniu z tym samym miesiącem poprzedniego roku. W lutym 2023 roku dochody podatkowe ze sprzedaży ropy i gazu zmniejszyły się o 46% w ujęciu rocznym, https://www.iea.org/data-and-statistics, [dostęp: 08.05.2025].

pozyskiwania technologii z krajów trzecich (np. Chiny, Iran, Korea Północna) oraz adaptacji technologii cywilnych, co obniżyło jakość i skuteczność niektórych systemów uzbrojenia[25].

Negatywne skutki dla rosyjskiej gospodarki miało też wycofanie się wielu przedsiębiorstw się z rynku rosyjskiego, ograniczając dostępność nowoczesnych technologii i know-how, a jednocześnie pogłębiając proces autarkizacji rosyjskiej gospodarki. Brak inwestycji zagranicznych i sankcje wtórne wpłynęły na obniżenie potencjału innowacyjnego i konkurencyjności rosyjskich firm.

Poniższy rysunek pokazuje jak zmieniła się wartość PKB Rosji po ataku na Ukrainę 24 lutego 2022 r.



Rysunek 1. Zmiana wartości PKB w Federacji Rosyjskiej po agresji na Ukrainę 24 lutego 2022 r.

Źródło: https://www.theguardian.com/world/2025/feb/22/what-have-three-years-of-putins-war-done-to-both-nations-economies, [dostęp: 10.05.2025].

[25] M. Bergmann, M. Snegovaya, T. Dolbaia, N. Fention, Contributor: S. Bendett, *Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry*, April 2023, A Report of the CSIS Europe, Russia, and Eurasia Program, https://www.csis.org/analysis/out-stock-assessing-impact-sanctions-russias-defense-industry, [dostęp: 09.05.2025].; N. Fenton, A. Kolyandr, *Down But Not Out: The Russian Economy Under Western Sanctions*, https://www.csis.org/analysis/down-not-out-russian-economy-under-western-sanctions, [dostęp: 09.05.2025].

Według danych KE od lutego 2022 r. UE zakazała eksportu do Rosji towarów o wartości ponad 48 mld euro i importu z Rosji do UE towarów o wartości 91,2 mld euro. Oznacza to, że w porównaniu z 2021 r. embargo dotyczy obecnie 54% eksportu i 58% importu[26].

Mimo istotnych trudności gospodarczych sankcje unijne nie doprowadziły do zasadniczej zmiany polityki Kremla wobec Ukrainy. Władze rosyjskie wzmocniły kontrolę nad mediami, represjonowały opozycję i prowadziły politykę „oblężonej twierdzy", przedstawiając sankcje jako dowód „zachodniej agresji"[27]. Jednocześnie jednak wzrosło niezadowolenie części elit gospodarczych i technokratycznych z powodu utraty dostępu do rynków i kapitału. Presja gospodarcza zmusiła władze rosyjskie do uzależnienia się od wsparcia Chin, co osłabiło suwerenność decyzyjną Moskwy w relacjach międzynarodowych[28].

Od początku obowiązywania sankcji państwa członkowskie UE oraz KE odnotowały liczne przypadki prób obchodzenia restrykcji, w szczególności poprzez reeksport towarów objętych zakazem z państw trzecich (np. Armenia, Kazachstan, Serbia), tworzenie fikcyjnych podmiotów pośredniczących czy wykorzystywanie jurysdykcji nieregulowanych (*offshore*) do transferu aktywów[29].

W odpowiedzi UE przyjęła mechanizmy przeciwdziałające obchodzeniu sankcji, w tym obowiązek raportowania podejrzanych transakcji, tzw. *clause anti-circumvention* w rozporządzeniach, a także współpracę z krajami trzecimi w ramach dyplomacji sankcyjnej (ang. *sanctions diplomacy*)[30].

---

[26] https://www.consilium.europa.eu/pl/policies/sanctions-against-russia-explained/, [dostęp: 12.05.2025].

[27] A. Legucka, *Orędzie Putina - rok wojny w oblężonej twierdzy*, Polski Instytut Spraw Międzynarodowych, https://www.pism.pl/publikacje/oredzie-putina-rok-wojny-w-oblezonej-twierdzy?, [dostęp: 08.05.2025].

[28] P. Dzierżanowski, M. Przychodniak, *Gospodarcze wsparcie ChRL dla Rosji po inwazji na Ukrainę*, Warszawa, styczeń 2025, s. 5-28, https://www.pism.pl/publikacje/gospodarcze-wsparcie-chrl-dla-rosji-po-inwazji-na-ukraine?, [dostęp: 13.05.2025].

[29] S. Djankov, A. Golovchenko, *Who benefits from Russia's war in Ukraine*, 6 January 2025, https://cepr.org/voxeu/columns/who-benefits-russias-war-ukraine, [dostęp: 10.05.2025].

[30] *Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014*, Banking and Finance, Last update: 28 April 2025, https://finance.ec.europa.eu/system/files/2024-01/faqs-sanctions-russia-consolidated_en.pdf?utm_source, [dostęp: 10.05.2025].

Choć sankcje unijne nie doprowadziły do natychmiastowej zmiany polityki Rosji ani zakończenia wojny, ich efektywność należy oceniać w szerszym kontekście strategicznym. Doszło do powstrzymania dalszej eskalacji działań zbrojnych poprzez osłabienie potencjału gospodarczego i militarnego Rosji oraz długofalowego jej osłabienia jako aktora geopolitycznego poprzez utratę zaufania inwestorów, wizerunku wiarygodnego partnera handlowego oraz wzrost zależności od państw azjatyckich.

Z perspektywy prawa i polityki międzynarodowej, sankcje unijne należy więc traktować jako narzędzie strategicznego oddziaływania, którego skuteczność nie ogranicza się wyłącznie do efektu natychmiastowego, ale rozciąga się w czasie i ma charakter systemowy.

Wnioski *de lege ferenda* i rekomendacje dla polityki sankcyjnej Unii Europejskiej

Doświadczenia z lat 2022-2025 dowodzą, że polityka sankcyjna UE wobec Federacji Rosyjskiej wymaga równoczesnego zachowania spójności instytucjonalnej oraz zdolności adaptacyjnej. Spójność ta odnosi się do jednolitości decyzji Rady przy zachowaniu wspólnotowego interesu w dziedzinie polityki zagranicznej i bezpieczeństwa, natomiast elastyczność umożliwia szybką reakcję na zmieniające się okoliczności geopolityczne i prawne.

De lege ferenda zasadne jest więc wzmocnienie koordynacji międzyinstytucjonalnej – w szczególności pomiędzy Radą, KE oraz Europejską Służbą Działań Zewnętrznych – w zakresie analizy skutków oraz kontroli wykonania sankcji. Ponadto wskazane byłoby ustanowienie trwałego organu doradczego ds. polityki sankcyjnej, składającego się z przedstawicieli instytucji unijnych, ekspertów prawa międzynarodowego i przedstawicieli państw członkowskich, którego zadaniem byłoby monitorowanie efektywności i zgodności środków restrykcyjnych z normami prawa międzynarodowego.

W związku z licznymi próbami obchodzenia sankcji przez podmioty rosyjskie za pośrednictwem krajów trzecich i mechanizmów pośrednich, niezbędne jest zintensyfikowanie polityki przeciwdziałania (*sanctions circumvention).* W tym kontekście rekomenduje się wprowadzenie unijnego mechanizmu szybkiego reagowania na naruszenia i obejścia sankcji, który umożliwiałby niezwłoczne aktualizowanie list sankcyjnych i identyfikowanie kanałów ryzyka, zacieśnienie współpracy z krajami trzecimi w ramach tzw.

„dyplomacji sankcyjnej" i zawieranie porozumień dwustronnych w zakresie wzajemnej pomocy prawnej, wymiany informacji oraz blokowania przepływów finansowych. Kolejną rekomendacją jest rozszerzenie katalogu sankcji wtórnych (*secondary sanctions*) wobec podmiotów ułatwiających obchodzenie sankcji, przy jednoczesnym zachowaniu proporcjonalności i zgodności z zasadą dobrej wiary. W celu zwiększenia legitymizacji polityki sankcyjnej UE na forum międzynarodowym, a także w oczach opinii publicznej, zaleca się wprowadzenie bardziej transparentnych procedur decyzyjnych i kontrolnych.

De lege ferenda wskazane byłoby ustanowienie obowiązku publikacji szczegółowych uzasadnień dla każdej decyzji sankcyjnej wraz z odwołaniem do norm prawa międzynarodowego i dokumentacji faktycznej oraz zapewnienie prawa do skutecznej obrony i przejrzystości procedur dla osób fizycznych i prawnych objętych sankcjami, w tym obowiązkowego dostępu do akt sprawy w określonym terminie. Powinny być przeprowadzane regularne przeglądy i ewaluacje skutków sankcji, z udziałem niezależnych ekspertów i organizacji międzynarodowych, takich jak OBWE czy Rada Europy.

W świetle wydarzeń lat 2022-2025 sankcje przestały być jedynie incydentalnym narzędziem reakcji kryzysowej i stały się trwałym komponentem polityki zagranicznej Unii Europejskiej. W związku z tym konieczne jest wzmocnienie ram prawnych oraz zdolności operacyjnych w tym zakresie. Proponuje się w związku z tym opracowanie kompleksowego kodeksu sankcyjnego UE (tzw. *EU Sanctions Framework*), który zawierałby jednolite zasady klasyfikacji sankcji, procedury ich wprowadzania, egzekwowania i znoszenia, jak również wprowadzenie instrumentów wsparcia dla państw członkowskich i przedsiębiorców w zakresie zgodności z przepisami sankcyjnymi *(compliance*), w tym szkoleń, wytycznych oraz wsparcia informatycznego. Wartościowym rozwiązaniem byłoby stworzenie unijnej platformy monitorowania skutków sankcji w wymiarze społecznym, gospodarczym i politycznym, również z uwzględnieniem oddziaływania na państwa trzecie.

Podsumowanie

Reasumując, sankcje UE są narzędziem w ramach WPZiB w celu przestrzegania prawa międzynarodowego, zapobiegania kryzysom międzynarodowym, wspierania rozwiązywania konfliktów, zwalczania terroryzmu i zwalczania rozprzestrzeniania broni. Sankcje są użytecznym narzędziem wspierania

państw trzecich konsolidujących demokrację i praworządność oraz pociągania gwałcicieli do odpowiedzialności za ich zbrodnie.

Polityka sankcyjna UE w odpowiedzi na agresję Rosji przeciwko Ukrainie w latach 2022-2025 stanowiła przełomowy etap w ewolucji zewnętrznych instrumentów prawa Unii. Zastosowane środki nie tylko potwierdziły zdolność UE do działania w sytuacjach zagrożenia pokoju i bezpieczeństwa międzynarodowego, ale również ukazały potrzebę dalszej profesjonalizacji, instytucjonalizacji i umiędzynarodowienia polityki sankcyjnej.

Z punktu widzenia prawa międzynarodowego, unijne sankcje wobec Rosji były zgodne z podstawowymi normami prawnymi, takimi jak zakaz agresji, prawo do samoobrony oraz odpowiedzialność państwa za czyny bezprawne. Ich skuteczność, choć nie absolutna, przyczyniła się do strategicznego osłabienia potencjału agresora oraz utrzymania jedności wewnątrz wspólnoty międzynarodowej.

Z tego względu, sankcje powinny pozostać integralnym narzędziem polityki UE, ale zarazem podlegać ciągłej ewaluacji i udoskonaleniu w duchu praworządności, przejrzystości i skuteczności.

Literatura

1. Dokumenty i raporty dot. zgodności środków restrykcyjnych z prawem międzynarodowym 2022-2025, OBWE.
2. Karta Narodów Zjednoczonych, Charter of the United Nations. https://www.un.org/en/about-us/un-charter
3. Orzeczenia w sprawach rosyjskich podmiotów zaskarżających sankcje UE, 2022–2024, Trybunał Sprawiedliwości Unii Europejskiej.
4. Rozporządzenie Rady (UE) nr 269/2014 z dnia 17 marca 2014 r. w sprawie środków ograniczających wobec osób i podmiotów odpowiedzialnych za podważanie integralności terytorialnej Ukrainy, Rada Unii Europejskiej.
5. Rozporządzenie Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. w sprawie środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie, Rada Unii Europejskiej.
6. Traktat o Unii Europejskiej, Dz.U. C 326 z 26.10.2012.
7. Traktat o funkcjonowaniu Unii Europejskiej, Dz.U. C 326 z 26.10.2012.

Netografia

1. Komunikaty prasowe nt. pakietów sankcji wobec Rosji, 2022-2025, Rada Unii Europejskiej, https://www.consilium.europa.eu.
2. Sanctions Map EU. (2025). Consolidated list of EU sanctions. https://www.sanctionsmap.eu.

3. *Omijanie sankcji unijnych przez Rosję: mechanizmy i kierunki*, Ośrodek Studiów Wschodnich, 2023-2024, https://www.osw.waw.pl.
4. Wsparcie gospodarcze Chin dla Rosji po inwazji na Ukrainę,, Polski Instytut Spraw Międzynarodowych, 2024, https://www.pism.pl.
5. *What have three years of Putin's war done to both nations' economies?*, 22.02.2025, The Guardian, https://www.theguardian.com/world/2025/feb/22/what-have-three-years-of-putins-war-done-to-both-nations-economies.

dr Marcin Oskierko
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0003-3450-6037

Adrian Łysomirski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0005-9997-6648

mgr inż. Daniel Stankowski
ORCID: 0000-0002-4316-1221

mgr inż. Marcin Kołodyński
ORCID: 0009-0007-0044-0769

https://doi.org/10.29316/9788368103205_6

WARUNKI PRAWNE WJAZDU I POBYTU OBYWATELI UKRAINY W POLSCE PO ROZPOCZĘCIU DZIAŁAŃ WOJENNYCH W UKRAINIE

LEGAL CONDITIONS FOR ENTRY AND RESIDENCE OF UKRAINIAN CITIZENS IN POLAND AFTER THE START OF HOSTILITIES IN UKRAINE

Streszczenie

Celem rozdziału jest analiza regulacji prawnych obowiązujących w Polsce po 24 lutego 2022 r., w związku z bezprecedensowym napływem obywateli Ukrainy uciekających przed wojną. Autorzy koncentrują się na omówieniu przepisów tzw. „specustawy”,

Summary

The aim of the chapter is to analyze the legal regulations in force in Poland after February 24, 2022, in connection with the unprecedented influx of Ukrainian citizens fleeing the war. The authors focus on discussing the provisions of the so-called “special act”,

uchwalonej w celu zapewnienia systemowego wsparcia uchodźcom wojennym oraz legalizacji ich pobytu na terytorium Rzeczypospolitej Polskiej. Wobec podjętej tematyki warto postawić następujące pytania badawcze: Jakie przesłanki determinują uznanie pobytu obywatela Ukrainy w Polsce za legalny z mocy prawa? W jaki sposób polska specustawa harmonizuje z regulacjami unijnymi w zakresie ochrony czasowej? Czy obowiązujące rozwiązania prawne można uznać za wystarczające w kontekście skali i zróżnicowania fali migracyjnej? Jakie znaczenie administracyjne i praktyczne ma dokument Diia.pl w systemie legalizacji pobytu cudzoziemców? Hipoteza badawcza zakłada, że wdrożenie specustawy w połączeniu z unijnym mechanizmem ochrony czasowej stanowi skuteczne i elastyczne narzędzie reagowania na masowy napływ uchodźców z Ukrainy. Wprowadzone rozwiązania prawne pozwoliły na szybkie objęcie ochroną setek tysięcy osób uciekających z terytorium ogarniętego konfliktem zbrojnym, gwarantując im dostęp do legalnego pobytu, rynku pracy, edukacji czy opieki zdrowotnej.
Rozdział oparty został na analizie aktów prawnych prawa krajowego i unijnego, komentarzy eksperckich, dokumentów urzędowych oraz danych statystycznych udostępnionych przez instytucje państwowe i organizacje międzynarodowe. Zastosowano metodę egzegezy prawniczej oraz analizę porównawczą.

Słowa kluczowe: specustawa, obywatel Ukrainy, ochrona czasowa, legalizacja pobytu, uchodźcy, cudzoziemcy, wojna w Ukrainie, Diia.pl.

adopted in order to provide systemic support to war refugees and legalize their stay on the territory of the Republic of Poland. In view of the subject matter, it is worth asking the following research questions: What are the prerequisites for recognizing the stay of a Ukrainian citizen in Poland as legal by virtue of law? How does the Polish special act harmonize with EU regulations on temporary protection? Can the existing legal solutions be considered sufficient in the context of the scale and diversity of the migration wave? What is the administrative and practical significance of the Diia.pl document in the system of legalization of the stay of foreigners? The research hypothesis assumes that the implementation of the special act in combination with the EU temporary protection mechanism is an effective and flexible tool for responding to the mass influx of refugees from Ukraine. The introduced legal solutions have made it possible to quickly protect hundreds of thousands of people fleeing the territory engulfed by armed conflict, guaranteeing them access to legal residence, the labor market, education, and health care. The chapter is based on the analysis of legal acts of national and EU law, expert commentaries, official documents, and statistical data made available by state institutions and international organizations. The method of legal exegesis and comparative analysis were used.

Keywords: special act, citizen of Ukraine, temporary protection, legalization of stay, refugees, foreigners, war in Ukraine, Diia.pl.

Wstęp

Dnia 24 lutego 2022 r. doszło do eskalacji trwającej od 2014 r. agresji Federacji Rosyjskiej wobec Ukrainy. W tym dniu rosyjskie siły zbrojne przekroczyły granicę Ukrainy, rozpoczynając pełnoskalową inwazję. Skutkiem tych działań był bezprecedensowy exodus ludności cywilnej – największy w Europie od zakończenia II wojny światowej. Mieszkańcy terenów objętych działaniami militarnymi, masowo opuszczali swoje miejsca zamieszkania. Zgodnie z danymi przedstawionymi przez Wysokiego Komisarza Narodów Zjednoczonych ds. Uchodźców (UNHCR), do końca czerwca 2022 r. terytorium Ukrainy opuściło blisko 5,5 miliona osób poszukujących ochrony międzynarodowej[1].

Największy odsetek osób opuszczających Ukrainę w wyniku rosyjskiej inwazji kierował się ku granicy z Polską. O wyjątkowej skali tego zjawiska świadczy fakt, iż w ciągu zaledwie dwóch tygodni od rozpoczęcia działań zbrojnych, do Polski przybył pierwszy milion uchodźców i uchodźczyń wojennych. Według szacunków, od 24 lutego do końca czerwca 2022 r., odnotowano ponad 4,3 miliona przekroczeń granicy ukraińsko-polskiej, przy czym warto zaznaczyć, że dane te obejmują również osoby, które mogły przekraczać granicę wielokrotnie. Nie oznacza to jednak, że taka liczba osób pozostała na terytorium Polski. Znacząca część migrantów kontynuowała podróż do innych państw europejskich lub zdecydowała się na powrót do Ukrainy. Wśród powracających znajdowali się m.in. mężczyźni podejmujący decyzję o włączeniu się do działań obronnych oraz osoby, które mimo wcześniejszej ewakuacji, wracały z powodów rodzinnych, osobistych bądź logistycznych – zarówno na krótko, jak i na dłużej[2]. Zgodnie z danymi opublikowanymi przez Unię Metropolii Polskich, na koniec marca 2022 r. liczba obywateli i obywatelek Ukrainy przebywających na terytorium Polski wynosiła około 3,2 miliona osób. Warto jednak zaznaczyć, że nie wszyscy przybyli w związku z eskalacją konfliktu zbrojnego – już na początku stycznia 2022 r. populacja ukraińska w Polsce liczyła około 1,5 miliona. Blisko 70% tej społeczności

[1] Ukraine Refugee Situation, https://data.unhcr.org/en/situations/ukraine, [dostęp: 12.03.2025].

[2] M. Duszczyk, P. Kaczmarczyk, *Imigranci i uchodźcy wojenni a sytuacja demograficzna Polski,* [w:] *Gościnna Polska 2022+. Jak mądrze wesprzeć Polskę i Polaków w pomocy osobom uciekającym przed wojną w Ukrainie?*, WiseEuropa, Warszawa 2022, s. 19.

zamieszkiwało dwanaście największych ośrodków miejskich w kraju oraz przyległe do nich obszary metropolitalne, w tym powiaty sąsiadujące z miastami wojewódzkimi[3].

W początkowym okresie konfliktu zbrojnego w Ukrainie struktura demograficzna uchodźców przybywających do Polski wskazywała na znaczący udział dzieci, które stanowiły blisko połowę tej populacji. Należy podkreślić, że przedstawione dane obejmują wyłącznie osoby zarejestrowane w systemie PESEL do końca maja 2022 r., których liczba przekroczyła 1,15 miliona. W grupie dorosłych uchodźców wyraźną przewagę liczebną miały kobiety, stanowiące ponad 90% tej kategorii[4].

Celem rozdziału jest przedstawienie oraz ocena obowiązujących uregulowań prawnych dotyczących wjazdu, pobytu i zakresu ochrony przysługującej obywatelom Ukrainy i wybranym kategoriom cudzoziemców w Polsce po wybuchu wojny, z uwzględnieniem aspektów prawa krajowego i unijnego.

Zasady przekraczania granic strefy Schengen oraz ich zmiany w kontekście wojny w Ukrainie

Ogólne zasady dotyczące przekraczania granic zostały uregulowane w Kodeksie Granicznym Schengen, który stanowi zbiór norm prawnych określających funkcjonowanie przestrzeni pozbawionej kontroli na granicach wewnętrznych, przy jednoczesnym ustanowieniu mechanizmów umożliwiających swobodny przepływ osób w jej obrębie.

Zgodnie z postanowieniami Kodeksu granicznego Schengen, realizacja kontroli granicznej na granicach zewnętrznych, leży nie tylko w interesie państwa członkowskiego bezpośrednio odpowiedzialnego za jej przeprowadzenie, lecz także w interesie wszystkich państw członkowskich, które zdecydowały się na zniesienie kontroli na granicach wewnętrznych. Ustanowienie wspólnego mechanizmu kontroli granicznej stanowi zatem element ochrony całej przestrzeni Schengen i przyczynia się do zapewnienia bezpieczeństwa wewnętrznego Unii Europejskiej. Kontrola graniczna odgrywa kluczową rolę w przeciwdziałaniu zjawiskom nielegalnej migracji oraz handlu ludźmi,

[3] A. Sobestjańska, A. Sopińska, *Miejska gościnność: wielki wzrost, wyzwania i szanse. Raport o uchodźcach z Ukrainy w największych polskich miastach*, Unia Metropolii Polskich im. P. Abramowicza, Warszawa 2022, s. 9.

[4] M. Duszczyk, P. Kaczmarczyk, *Imigranci i uchodźcy wojenni…,* op. cit., s. 21-22.

a także w zapobieganiu potencjalnym zagrożeniom dla bezpieczeństwa wewnętrznego, porządku publicznego, zdrowia publicznego oraz stosunków międzynarodowych państw członkowskich. Zakres tej kontroli nie ogranicza się wyłącznie do formalnej odprawy osób na przejściach granicznych oraz do fizycznej ochrony granicy w jej linii ciągłej, lecz obejmuje również działania analityczne, takie jak ocena ryzyka dla bezpieczeństwa wewnętrznego oraz identyfikacja zagrożeń, które mogą wpływać na integralność i bezpieczeństwo granic zewnętrznych Unii Europejskiej[5].

Przekraczanie granic zewnętrznych dozwolone jest jedynie na przejściach granicznych i w ustalonych godzinach ich otwarcia. Na przejściach granicznych, które nie są czynne całą dobę, udostępnia się widoczne informacje o godzinach ich otwarcia. Na zasadzie odstępstwa można dopuścić wyjątki od obowiązku przekraczania granic zewnętrznych jedynie na przejściach granicznych i w ustalonych godzinach ich otwarcia: dla osób lub grup osób – w przypadku, gdy istnieje szczególny wymóg sporadycznego przekraczania granic zewnętrznych poza przejściami granicznymi lub poza ustalonymi godzinami ich otwarcia – pod warunkiem, że posiadają zezwolenia wymagane na mocy prawa krajowego oraz że nie zachodzi sprzeczność z interesem porządku publicznego i bezpieczeństwa wewnętrznego państw członkowskich, dla osób lub grup osób w przypadku nieprzewidzianej sytuacji wyjątkowej oraz zgodnie z przepisami szczególnymi[6] zawartymi w art. 19 i 20 w związku z załącznikami VI i VII. Przekroczenie granicy zewnętrznej Unii Europejskiej w sposób niezgodny z obowiązującymi przepisami – tj. poza wyznaczonymi przejściami granicznymi lub poza godzinami ich funkcjonowania – podlega sankcjonowaniu przez państwa członkowskie. Wprowadzane przez nie środki represyjne powinny cechować się skutecznością, proporcjonalnością oraz charakterem prewencyjnym, tak aby zapewnić realne przeciwdziałanie naruszeniom reżimu granicznego i utrzymać integralność wspólnej przestrzeni bezpieczeństwa.

Zasady dotyczące wjazdu obywateli państw trzecich na terytorium państw członkowskich Unii Europejskiej pozwalają na wjazd w czasie nieprzekraczającym 90 dni w dowolnym okresie 180 dni. Aby wjazd obywatela państwa trzeciego na terytorium państw członkowskich był uznany za legalny,

[5] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen)*, Dz. Urz. UE L 77/1 z 23.03.2016, pkt.6 i 8 preambuły.

[6] Szerzej zob. *Kodeks graniczny Schengen*, załącznik VI i VII.

konieczne jest spełnienie określonych wymogów wjazdowych, które obejmują następujące warunki: posiadanie ważnego dokumentu podróży uprawniającego posiadacza do przekroczenia granicy i spełniającego kryterium ważności przez przynajmniej trzy miesiące po planowanej dacie wyjazdu z terytorium państw członkowskich oraz został wydany w okresie ostatnich 10 lat. Ponadto podróżni muszą posiadać ważną wizę, jeżeli jest wymagana, chyba, że posiadają ważny dokument pobytowy lub ważną wizę długoterminową. Uzasadnią cel i warunki planowanego pobytu oraz posiadają wystarczające środki utrzymania, zarówno na czas trwania planowanego pobytu, na powrót do ich państwa pochodzenia lub na tranzyt do państwa trzeciego. Ponadto nie są osobami, wobec których dokonano wpisu do celów odmowy wjazdu w SIS oraz nie są uważani za stanowiących zagrożenie dla porządku publicznego, bezpieczeństwa wewnętrznego, zdrowia publicznego lub stosunków międzynarodowych żadnego z państw członkowskich, a w szczególności nie dokonano wobec nich, na tej samej podstawie, wpisu do celów odmowy wjazdu w krajowych bazach danych państw członkowskich[7].

Rozpoczęcie działań wojennych na terytorium Ukrainy zapoczątkowało istotne zmiany w regulacjach dotyczących zasad wjazdu i pobytu obywateli ukraińskich na obszarze Unii Europejskiej. Komisja Europejska w opublikowanym komunikacie ustaliła środki operacyjne dotyczące zarządzania granicami zewnętrznymi w celu ułatwienia przekraczania granicy między UE a Ukrainą[8]. Środki te obejmowały: uproszczenie kontroli granicznych dla niektórych kategorii osób, w tym osób wymagających szczególnego traktowania, takich jak dzieci, oraz innych kategorii, takich jak pracownicy transportu, którzy znaleźli się w Ukrainie podczas wykonywania swoich obowiązków, możliwość organizowania kontroli granicznych poza przejściami granicznymi, szczególne ustalenia dotyczące przekraczania granic przez służby ratownicze, policję, straż pożarną i straż graniczną, jak i marynarzy, niezależnie od ich narodowości, utworzenie uprzywilejowanych korytarzy w celu zapewnienia wjazdu i powrotu organizacjom udzielającym pomocy humanitarnej ludności na terytorium Ukrainy oraz zniesienie ceł i wprowadzenie środków ułatwiających wjazd zwierząt domowych podróżujących ze swoimi właścicielami z Ukrainy.

[7] Ibidem, art. 6.

[8] *Komunikat Komisji zawierający wytyczne operacyjne dotyczące zarządzania granicami zewnętrznymi w celu ułatwienia przekraczania granicy między UE a Ukrainą 2022/C 104 I/01*, Dz. Urz. UE C 104 I z 4.3.2022.

Osoby objęte zakresem ochrony na podstawie przepisów specustawy

W założeniu ustawa miała stanowić odpowiedź na konieczność zorganizowania systemowego wsparcia dla osób zmuszonych do opuszczenia terytorium Ukrainy w związku z trwającymi tam działaniami wojennymi. W swojej obecnej wersji, tzw. specustawa obejmuje regulacjami określone grupy osób, którym przysługuje szczególna pomoc, zgodnie z zapisami zawartymi w kolejnych jej przepisach:

- Grupę objętą pomocą na mocy specustawy stanowią obywatele Ukrainy, którzy przybyli do Polski w związku z prowadzonymi na terytorium ich państwa działaniami wojennymi[9]. W pierwotnym brzmieniu przepisów ustawodawca przewidział, że wsparcie przysługuje wyłącznie osobom, które przekroczyły granicę polsko-ukraińską bezpośrednio z terytorium Ukrainy. Tym samym, z zakresu uprawnień do pomocy wyłączone zostały osoby, które opuściły Ukrainę przez inne państwa sąsiednie – takie jak Słowacja, Węgry, Rumunia czy Mołdawia – i dopiero później przybyły na terytorium Rzeczypospolitej Polskiej z zamiarem dłuższego pobytu. Taka redakcja przepisu skutkowała szeregiem niepożądanych konsekwencji, w tym próbami ponownego przekroczenia granicy ukraińsko-polskiej przez niektóre osoby, które w ten sposób usiłowały spełnić formalne warunki niezbędne do uzyskania pomocy. Wymóg dotyczący „bezpośredniego" wjazdu na terytorium Rzeczypospolitej Polskiej został zniesiony na mocy pierwszej nowelizacji ustawy z dnia 23 marca 2022 r.[10], także przepisów ustawy – Prawo o szkolnictwie wyższym i nauce[11]. Chociaż znowelizowane przepisy formalnie weszły w życie z dniem 26 marca 2022 r., zgodnie z ich treścią mają one zastosowanie wstecz, obejmując sytuacje zaistniałe od 24 lutego 2022 r. Celem takiego rozwiązania było umożliwienie objęcia wsparciem również tych obywateli Ukrainy, którzy przybyli do Polski przed datą wejścia w życie aktu prawnego, bez konieczności podejmowania przez nich dodatkowych

[9] Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz. U. z 2025 r. poz. 337).

[10] Ustawa z 23 marca 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz. U. 2022 r. poz. 683).

[11] Ustawa z dnia z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1897).

działań migracyjnych oraz bez narażania ich na wykluczenie z systemu pomocy[12].

- Zgodnie z postanowieniami ustawy, uprawnienia do skorzystania z przewidzianych w niej form wsparcia zostały rozszerzone również na małżonków obywateli Ukrainy, którzy sami nie posiadają obywatelstwa ukraińskiego, pod warunkiem, że przybyli do Polski z terytorium Ukrainy i nie są obywatelami Rzeczypospolitej Polskiej ani żadnego innego państwa członkowskiego Unii Europejskiej. Przepis ten zawiera kilka istotnych elementów merytorycznych, warunkujących jego zastosowanie. Po pierwsze, regulacja ta wprowadza wyjątek od podstawowej zasady dotyczącej zakresu podmiotowego specustawy, umożliwiając objęcie jej przepisami określonej grupy cudzoziemców niebędących obywatelami Ukrainy. Mowa tu wyłącznie o małżonkach obywateli tego państwa. Zakres zastosowania przepisu ma charakter wąski – nie dotyczy bowiem innych członków najbliższej rodziny, takich jak dzieci, rodzice czy partnerzy pozostający w nieformalnych związkach, jeżeli nie legitymują się obywatelstwem ukraińskim. Co więcej, uprawnienia wynikające z ustawy nie przysługują byłym małżonkom, którzy utracili status małżonka obywatela Ukrainy wskutek rozwodu. Warto również podkreślić, że skorzystanie z uprawnień nie jest uzależnione od obecności małżonka posiadającego obywatelstwo ukraińskie. Oznacza to, że uprawnieni małżonkowie mogą przebywać na terytorium Rzeczypospolitej Polskiej samodzielnie i niezależnie od miejsca pobytu swojego partnera. Ustawa przyznaje im autonomiczne prawo do korzystania z przewidzianych w niej środków pomocowych na takich samych zasadach, jakie dotyczą obywateli Ukrainy. Przepis ten nie wiąże zatem skutków prawnych z sytuacją faktyczną bądź prawną małżonka, lecz wyłącznie z istnieniem formalnego związku małżeńskiego oraz okolicznością opuszczenia Ukrainy z powodu prowadzonych tam działań wojennych.

[12] W obowiązującym stanie prawnym nie istnieje już potrzeba dokumentowania faktu bezpośredniego przekroczenia granicy polsko-ukraińskiej. Decydujące znaczenie przypisuje się natomiast przyczynie opuszczenia terytorium Ukrainy, którą musi być ucieczka przed skutkami działań zbrojnych prowadzonych na obszarze tego państwa. Tym samym, prawo do korzystania z instrumentów wsparcia przewidzianych w ustawie przysługuje każdemu obywatelowi Ukrainy, niezależnie od tego, przez które państwo graniczne opuścił Ukrainę, kierując się do Polski.

Kluczowym warunkiem pozostaje fakt, że osoby te muszą przybyć na terytorium Polski z Ukrainy. Analogicznie jak w przypadku obywateli Ukrainy, nie wymaga się bezpośredniego przekroczenia granicy ukraińsko-polskiej – możliwy jest tranzyt przez inne państwa. Niemniej jednak wykluczone jest objęcie omawianymi regulacjami osób, które przybyły do Polski z innych krajów, w których uprzednio zamieszkiwały, takich jak Rosja czy Białoruś. Przepis ten znajduje zastosowanie wyłącznie wobec osób, które realnie przebywały na terytorium Ukrainy i uchodziły z niego wskutek konfliktu zbrojnego.

Przepis przewiduje dwa istotne ograniczenia w zakresie podmiotowym, które zostały wprowadzone na mocy kolejnych nowelizacji ustawy – odpowiednio z dnia 8 kwietnia 2022 r.[13] oraz 8 czerwca 2022 r.[14]. Na ich podstawie z zakresu osób uprawnionych do korzystania z pomocy przewidzianej w specustawie wyłączeni zostali obywatele Rzeczypospolitej Polskiej oraz obywatele innych państw członkowskich Unii Europejskiej. Zdaniem autorów wprowadzenie tych ograniczeń należy uznać za uzasadnione, gdyż osoby te posiadają już dostęp do rozbudowanego systemu wsparcia instytucjonalnego w Polsce. Obywatele polscy korzystają z pełni praw przysługujących im na podstawie przepisów krajowych, w tym prawa do świadczeń z systemu pomocy społecznej, opieki zdrowotnej, edukacji czy zatrudnienia. Z kolei obywatele państw członkowskich Unii Europejskiej, zgodnie z obowiązującym w Polsce prawem oraz regulacjami unijnymi, mają zapewnioną legalizację pobytu oraz dostęp do szeregu usług publicznych. W związku z tym objęcie ich zakresem regulacji specustawy byłoby niecelowe i prowadziłoby do niepotrzebnego dublowania uprawnień.

- Kolejną kategorią osób objętych zakresem podmiotowym specustawy są obywatele Ukrainy posiadający Kartę Polaka, którzy przybyli do Polski w związku z działaniami wojennymi prowadzonymi na terytorium Ukrainy. Ustawodawca ujął tę grupę jako odrębną kategorię beneficjentów, co

[13] Ustawa z 8 kwietnia 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz niektórych innych ustaw (Dz. U. z 2022 r. poz. 830).

[14] Ustawa z 8 czerwca 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz niektórych innych ustaw (Dz. U. z 2022 r. poz. 1383).

świadczy o intencjonalnym nadaniu jej szczególnego statusu oraz wprowadzeniu odmiennych warunków wjazdu i uzyskania wsparcia. Z formalnego punktu widzenia istotne znaczenie ma tu analiza literalnego brzmienia przepisów odnoszących się do tej grupy w porównaniu z regulacjami dotyczącymi pozostałych obywateli Ukrainy.

- W odniesieniu do osób posiadających Kartę Polaka ustawodawca posłużył się sformułowaniem, zgodnie z którym prawo do pomocy przysługuje im, jeżeli „z powodu działań wojennych przybyli na terytorium Rzeczypospolitej Polskiej". Warto zauważyć, że w tym przypadku pominięto wymóg przybycia „z terytorium Ukrainy", który występuje w przepisach dotyczących pozostałych obywateli Ukrainy. Oznacza to, że ustawodawca dopuszcza możliwość objęcia pomocą również te osoby, które – mimo iż posiadają obywatelstwo ukraińskie – nie przebywały w Ukrainie bezpośrednio przed przyjazdem do Polski, lecz mieszkały w innych państwach, np. w Białorusi, Rosji czy w innym państwie, skąd zmuszone były wyjechać w związku z konfliktem zbrojnym. Powyższe stanowisko znajduje uzasadnienie w specyfice sytuacji osób posiadających Kartę Polaka, które z założenia mają szczególne więzi z państwem polskim i są objęte polityką wsparcia repatriacyjnego lub integracyjnego.
- Kolejnym wyróżnikiem tej grupy jest możliwość objęcia ochroną również ich najbliższej rodziny[15], niezależnie od obywatelstwa jej członków. W praktyce oznacza to, że ze świadczeń przewidzianych w specustawie mogą korzystać również osoby, które nie posiadają obywatelstwa ukraińskiego, pod warunkiem, że są członkami rodziny obywatela Ukrainy posiadającego Kartę Polaka. W tym kontekście należy jednak podkreślić, że omawiane przepisy nie mają zastosowania wobec członków rodziny, którzy posiadają obywatelstwo ukraińskie, ponieważ przysługuje im ono z mocy ustawy jako osobom uprawnionym w sposób bezpośredni.

W kontekście regulacji ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa istotne znaczenie ma treść decyzji wykonawczej Rady (UE) 2022/382 z dnia 4 marca 2022 r.[16], która

[15] Polskie prawo nie zna kategorii najbliżej rodziny, posługuje się pojęciem osoby najbliższej. Szerzej zob. Ustawa z 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383), art. 115 § 11, Ustawa z 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2024 r. poz. 1237), art. 446 § 4.

[16] Decyzja wykonawcza Rady (UE) 2022/382 z dnia 4 marca 2022 r. stwierdzająca istnienie masowego napływu wysiedleńców z Ukrainy w rozumieniu art. 5 dyrektywy 2001/55/WE

– powołując się na art. 5 dyrektywy 2001/55/WE[17] – potwierdza istnienie masowego napływu osób przemieszczających się z terytorium Ukrainy w wyniku działań wojennych, wprowadzając tymczasową ochronę na terytorium Unii Europejskiej. Zgodnie z art. 2 ust. 4 decyzji wykonawczej 2022/382, za członków rodziny uznaje się: małżonka lub – w niektórych przypadkach – partnera pozostającego z osobą uciekającą w stałym, nieformalnym związku; małoletnie dzieci, pozostające na utrzymaniu osoby objętej ochroną, w tym także dzieci współmałżonka; a także innych bliskich krewnych, którzy zamieszkiwali wspólnie z osobą uciekającą w ramach jednego gospodarstwa domowego i byli w tamtym czasie w pełni lub częściowo na jej utrzymaniu[18]. Tak szeroka definicja ma na celu objęcie ochroną faktycznych wspólnot rodzinnych, niezależnie od stopnia pokrewieństwa formalnego, w sytuacjach, gdy relacje te miały istotne znaczenie ekonomiczne i społeczne dla funkcjonowania danej osoby.

Niezwykle istotnym aspektem determinującym uprawnienie do korzystania z regulacji zawartych w specustawie jest przyczyna opuszczenia Ukrainy przez daną osobę. Zgodnie z treścią ustawy, uprawnienie to przysługuje wyłącznie osobom, które przybyły do Polski „w związku z działaniami wojennymi prowadzonymi na terytorium Ukrainy". W pierwszej kolejności należy zaliczyć do tej grupy osoby bezpośrednio uciekające przed zagrożeniem militarnym – m.in. przed działaniami wojsk rosyjskich, w tym z terytoriów okupowanych lub objętych intensywnymi działaniami bojowymi. Jednak ograniczenie katalogu uprawnionych wyłącznie do osób uchodzących bezpośrednio z obszarów objętych walkami, byłoby sprzeczne z brzmieniem przepisu, ale również niewspółmierne wobec rzeczywistej skali skutków wojny.

W związku z tym należy przyjąć szerszą interpretację, zgodnie z którą prawo do korzystania ze wsparcia przysługuje również tym osobom, które – choć nie były narażone bezpośrednio na działania militarne – uciekły z powodu skutków wojny o charakterze ekonomicznym, społecznym lub rodzinnym. Oznacza to objęcie ochroną m.in. osób, które utraciły źródła utrzymania, zostały

i skutkująca wprowadzeniem tymczasowej ochrony, Dz. Urz. UE L 71/1 z 4.03.2022.

[17] Dyrektywa Rady 2001/55/WE z dnia 20 lipca 2001 r. w sprawie minimalnych standardów przyznawania tymczasowej ochrony na wypadek masowego napływu wysiedleńców oraz środków wspierających równowagę wysiłków między Państwami Członkowskimi związanych z przyjęciem takich osób wraz z jego następstwami, Dz. Urz. UE L 212/12 z 7.08.2001.

[18] Decyzja wykonawcza Rady (UE) 2022/382 z dnia 4 marca 2022 r. stwierdzająca istnienie…, op. cit.

zmuszone do opuszczenia miejsca zamieszkania z powodów bezpieczeństwa lub których sytuacja rodzinna uległa destabilizacji w wyniku wojny np. śmierć lub mobilizacja członka rodziny, zniszczenie infrastruktury cywilnej, zamknięcie instytucji publicznych itp.

Autorzy rozdziału podkreślają, że zakres zastosowania specustawy wykracza poza osoby, które przekroczyły granicę Polski po 24 lutego 2022 r., czyli po rozpoczęciu przez Federację Rosyjską pełnoskalowych działań wojennych na terytorium Ukrainy. W ustawie zawarto bowiem również przepisy odnoszące się do obywateli Ukrainy, którzy przebywali w Polsce już wcześniej, tj. przed wybuchem wojny. Przepisy te przewidują szereg uprawnień mających na celu stabilizację ich sytuacji prawnej i ekonomicznej w warunkach kryzysu humanitarnego. Zgodnie z art. 22 specustawy, osoby te uzyskały prawo do podejmowania zatrudnienia bez konieczności uzyskiwania zezwolenia na pracę, co znacząco uprościło ich sytuację na rynku pracy. Ponadto, art. 23 umożliwia im prowadzenie działalności gospodarczej na terytorium Polski, zrównując ich w tym zakresie z obywatelami RP. Wreszcie, art. 42 przewiduje mechanizmy automatycznego przedłużenia ważności dokumentów pobytowych, takich jak wizy czy karty pobytu, w sytuacji, gdy przedłużenie na dotychczasowych zasadach nie jest możliwe – np. z uwagi na brak możliwości powrotu do Ukrainy lub ograniczenia funkcjonowania tamtejszych instytucji administracyjnych[19].

Specustawa zakłada udzielanie pomocy i wsparcia wyłącznie osobom z obywatelstwem ukraińskim. Nie obejmuje obywateli innych państw, którzy uciekli z Ukrainy przed działaniami wojennymi, choćby mieszkali tam przez długi czas. Tymczasem imigranci i imigrantki stanowili w Ukrainie wysoki odsetek ogółu ludności, przekraczający 10% populacji tego kraju i sięgający 4,8 mln osób[20]. W tej grupie było prawie 80 tys. studentów i studentek zagranicznych z ponad 150 krajów – w większości odległych, takich jak Indie, Maroko czy Nigeria[21]. Dla osób pochodzących z państw oddalonych geograficznie od Polski przewidziany okres piętnastu dni na podstawie zezwolenia udzielonego przez komendanta placówki Straży Granicznej wydanego

[19] Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku…, art. 22, art. 23, art. 42.

[20] Ukraine Immigration Statistics 1990-2025, https://www.macrotrends.net/countries/UKR/ukraine/i mmigration-statistics, [dostęp: 12.03.2025].

[21] *International students in Ukraine*, Ministry of Education and Science of Ukraine, https://studyinukraine.gov.ua/statistic/, [dostęp: 10.04.2025].

w trybie art. 32 ust. 1 ustawy z 12.12.2013 r. o cudzoziemcach[22].Bardzo często okres 15 dni okazywał się niewystarczający do podjęcia skutecznych działań organizacyjnych umożliwiających powrót do państwa pochodzenia, często w związku z trudnościami wizowymi oraz kosztami transportu. Dodatkowo, wśród tej grupy znajdowały się osoby, które nie posiadały realnej możliwości powrotu do kraju pochodzenia, ponieważ Ukraina była ich miejscem długotrwałego, a często także stałego pobytu.

Komplementarność rozwiązań specustawy i dyrektywy 2001/55/WE w kontekście kryzysu uchodźczego

Rosyjska inwazja na Ukrainę w lutym 2022 r. wywołała zdecydowaną reakcję społeczności międzynarodowej, czego przejawem było uruchomienie mechanizmów zawartych w dyrektywie Rady 2001/55/WE z dnia 20 lipca 2001 r., ustanawiającej minimalne standardy przyznawania tymczasowej ochrony w przypadku masowego napływu wysiedleńców oraz zasady solidarności i podziału odpowiedzialności pomiędzy państwami członkowskimi Unii Europejskiej[23]. Było to pierwsze w historii zastosowanie tego aktu prawnego, który od ponad dwóch dekad stanowił potencjalne narzędzie reagowania na kryzysy humanitarne w skali kontynentalnej. Zgodnie z założeniami dyrektywy 2001/55/WE, tymczasowa ochrona ma charakter zbiorowy i uproszczony – przysługuje ona wszystkim osobom spełniającym kryteria wynikające z decyzji Rady, bez konieczności prowadzenia indywidualnych postępowań administracyjnych weryfikujących przesłanki przyznania ochrony, jak ma to miejsce w przypadku procedury azylowej. Ochrona ta jest z założenia czasowa, z możliwością obowiązywania do maksymalnie dwóch lat, w zależności od dalszego rozwoju sytuacji geopolitycznej oraz decyzji instytucji unijnych.

Dyrektywa nakłada na państwa członkowskie UE szereg obowiązków względem osób objętych tymczasową ochroną, w szczególności w zakresie zapewnienia: zakwaterowania oraz odpowiednich warunków bytowych, dostępu do systemów opieki zdrowotnej i pomocy społecznej, prawa do podejmowania pracy lub prowadzenia działalności gospodarczej, czy prawa

[22] Ustawa z 12 grudnia 2013 r. o cudzoziemcach (Dz. U. z 2021 r. poz. 2354 ze zm.).

[23] Dyrektywa Rady 2001/55/WE z dnia 20 lipca 2001 r. w sprawie minimalnych standardów przyznawania tymczasowej ochrony na wypadek masowego napływu wysiedleńców… op. cit.

do nauki dla dzieci i młodzieży[24]. Implementacja tych zobowiązań przez państwa członkowskie, w tym Polskę, stanowiła kluczowy element efektywnej odpowiedzi na kryzys uchodźczy, wywołany działaniami wojennymi w Ukrainie. W praktyce przyczyniło się to do znacznego odciążenia krajowych systemów azylowych, umożliwiając szybkie objęcie ochroną dużej liczby osób w potrzebie.

W efekcie okazało się, że w Polsce funkcjonują równolegle trzy różne systemy prawne, z których osoba uciekająca z Ukrainy może skorzystać:

- złożenie w placówce Straży Granicznej wniosku o nadanie statusu uchodźcy i wejście w regularną procedurę wynikającą z przepisów ustawy o udzielaniu cudzoziemcom ochrony na terytorium RP;
- złożenie do Szefa Urzędu ds. Cudzoziemców wniosku o wydanie zaświadczenia o korzystaniu z ochrony czasowej[25] zgodnej z dyrektywą 2001/55/WE oraz decyzją wykonawczą 2022/382;
- skorzystanie z przepisów specustawy i przewidzianych w niej uprawnień.

Zgodnie z danymi opublikowanymi przez Szefa Urzędu do Spraw Cudzoziemców, w 2022 roku o udzielenie ochrony międzynarodowej na terytorium Rzeczypospolitej Polskiej ubiegało się łącznie 9,9 tys. cudzoziemców. Najliczniejszą grupę wnioskodawców stanowili obywatele Białorusi – 3,1 tys. osób. Kolejne miejsca zajmowali: obywatele Federacji Rosyjskiej (2,2 tys. osób), Ukrainy (1,8 tys. osób), Iraku (0,6 tys. osób) oraz Afganistanu (0,4 tys. osób)[26].

Do form ochrony międzynarodowej zaliczamy status uchodźcy oraz ochronę uzupełniającą, natomiast wśród form ochrony krajowej wyróżniamy azyl oraz ochronę czasową.

[24] Ibidem, art. 12-14.

[25] Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 389), art. 110 ust 5.

[26] *Ochrona międzynarodowa w 2022 r.,* Urząd do Spraw Cudzoziemców, https://www.gov.pl/web/udsc/ochrona-miedzynarodowa-w-2022-r, [dostęp: 08.03.2025].

Tabela 1. Główne formy ochrony cudzoziemców w Polsce

Formy ochrony międzynarodowej		
Forma ochrony	**Kryteria przyznawania**	**Organ przyznający**
Status uchodźcy w RP	Nadawany jest na wniosek cudzoziemca, jeżeli na skutek uzasadnionej obawy przed prześladowaniem w kraju pochodzenia z powodu rasy, religii, narodowości, przekonań politycznych lub przynależności do określonej grupy społecznej nie może lub nie chce korzystać z ochrony tego kraju.	Szef Urzędu do Spraw Cudzoziemców
Ochrona uzupełniająca	Przyznawana jest cudzoziemcowi, który nie spełnia warunków do nadania statusu uchodźcy, a powrót do kraju pochodzenia może narazić go na rzeczywiste ryzyko doznania poważnej krzywdy przez orzeczenie kary śmierci lub wykonanie egzekucji, tortury, nieludzkie lub poniżające traktowanie albo karanie, a także poważne i zindywidualizowane zagrożenie dla życia lub zdrowia wynikające z powszechnego stosowania przemocy wobec ludności cywilnej w sytuacji międzynarodowego lub wewnętrznego konfliktu zbrojnego.	Szef Urzędu do Spraw Cudzoziemców
Formy ochrony krajowej		
Forma ochrony	**Kryteria przyznawania**	**Organ przyznający**
Azyl	Może być udzielony na wniosek cudzoziemca, gdy jest to niezbędne do zapewnienia mu ochrony oraz gdy przemawia za tym ważny interes RP.	Szef Urzędu do Spraw Cudzoziemców po uzyskaniu zgody ministra właściwego do spraw zagranicznych
Ochrona czasowa	Przyznawana jest cudzoziemcom masowo przybywającym do RP, którzy opuścili swój kraj pochodzenia lub określony obszar geograficzny, z powodu obcej inwazji, wojny, wojny domowej, konfliktów etnicznych lub rażących naruszeń praw człowieka, bez względu na to, czy ich przybycie miało charakter spontaniczny, czy też było wynikiem pomocy udzielonej im przez RP lub społeczność międzynarodową.	Szef Urzędu do Spraw Cudzoziemców

Źródło: opracowanie własne.

Osoba, która chce złożyć wniosek do Szefa Urzędu do Spraw Cudzoziemców o udzielenie ochrony międzynarodowej w trakcie wjazdu na terytorium Polski podczas kontroli granicznej musi poinformować funkcjonariusza Straży Granicznej o chęci wystąpienia z wnioskiem uchodźczym, a także

zgłosić się do oddziału lub placówki Straży Granicznej. Podczas składania wniosku osoba ubiegająca się o udzielenie ochrony międzynarodowej musi okazać wszystkie posiadane dokumenty (w tym dokumenty tożsamości i podróży) oraz wszystkie posiadane dowody, które mogą potwierdzać sytuację danej osoby. Zasada ta dotyczy zarówno wnioskodawcy, jak też wszystkich osób, których dotyczyć ma wniosek. Wniosek o nadanie statusu uchodźcy jest wypełniany w języku polskim na specjalnym formularzu w oparciu o informacje uzyskane podczas rozmowy cudzoziemca z funkcjonariuszem SG. W tej rozmowie uczestniczy tłumacz języka, w którym porozumiewa się dana osoba. W stosunku do osób ubiegających się o udzielenie ochrony międzynarodowej podczas składania wniosku towarzyszą procedury obowiązkowego fotografowania, a dla osób powyżej 14. roku życia obligatoryjne jest pobieranie odcisków palców. Poza tym przeprowadzane zostają badania lekarskie i zabiegi sanitarne, zaś w przypadkach uzasadnionych względami bezpieczeństwa i porządku dokonuje się szczegółowego sprawdzenia osoby. Przeprowadzana zostaje też indywidualna rozmowa na temat okoliczności wskazujących, które państwo będzie odpowiedzialne za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej[27].

Podstawy uznania legalności pobytu obywateli Ukrainy i członków ich rodzin na terytorium Rzeczypospolitej Polskiej w świetle przepisów prawa

Przedmiotowa regulacja określa przesłanki, których spełnienie skutkuje uznaniem legalności pobytu na terytorium Rzeczypospolitej Polskiej określonych kategorii obywateli Ukrainy, w tym osób posiadających Kartę Polaka[28], a także członków ich najbliższej rodziny. Nabycie prawa do legalnego pobytu ma charakter ex lege, nie wymaga wydania decyzji administracyjnej potwierdzającej ten status. Zakres podmiotowy regulacji obejmuje:

- obywateli Ukrainy, którzy po 24 lutego 2022 r. przybyli z terytorium Ukrainy na terytorium Polski w związku z działaniami wojennymi, a także ich małżonków nieposiadających obywatelstwa ukraińskiego,

[27] *Załatwiaj sprawy urzędowe przez Internet, bezpiecznie i wygodnie!*, Portal gov.pl, https://www.gov.pl/web/udsc/w-jaki-sposob-zlozyc-wniosek-o-udzielenie-ochrony-miedzynarodowej, [dostęp: 04.01.2025].

[28] Ustawa z ustawy z dnia 7 września 2007 r. o Karcie Polaka (Dz.U. z 2019 r. poz. 1598 ze zm.).

pod warunkiem, że również przybyli z terytorium Ukrainy w związku z konfliktem zbrojnym i nie są obywatelami Rzeczypospolitej Polskiej;

- dzieci urodzone w Polsce, jeżeli ich matki – obywatelki Ukrainy – przybyły do Polski po 24 lutego 2022 r. z terytorium Ukrainy w związku z działaniami wojennymi;
  – obywateli Ukrainy posiadających Kartę Polaka, którzy opuścili Ukrainę po 24 lutego 2022 r. z powodu toczącej się wojny i przybyli do Polski, a także ich najbliższych członków rodziny.

Aby pobyt osób z wymienionych kategorii został uznany za legalny z mocy prawa, konieczne jest łączne spełnienie następujących warunków:

- Przyjazd do Polski od dnia 24 lutego 2022 r. (włącznie) do momentu, który zostanie określony w rozporządzeniu Rady Ministrów[29].
- Związek przybycia z działaniami wojennymi prowadzonymi na terytorium Ukrainy. Z przepisu wyłączone są zatem osoby, które – choć przybyły do Polski po 24 lutego 2022 r. – nie opuściły Ukrainy w związku z konfliktem zbrojnym, na przykład dlatego, że wcześniej zamieszkiwały w innym państwie i z niego wjechały do Polski.
- Legalność wjazdu na terytorium Polski, która może być rozumiana dwojako:– jako spełnienie warunków m.in. posiadanie ważnego dokumentu podróży, wizy, ubezpieczenia zdrowotnego, środków finansowych na utrzymanie i uzasadnienie celu pobytu[30], – albo jako przyjazd na podstawie indywidualnej zgody wydanej przez komendanta placówki Straży Granicznej z uwagi na względy humanitarne, interes państwa lub zobowiązania międzynarodowe – mimo niespełnienia ogólnych warunków wjazdu[31]. Za nielegalny uznaje się natomiast wjazd z naruszeniem przepisów dotyczących przekraczania granicy zewnętrznej strefy Schengen (art. 5 kodeksu granicznego Schengen).
- Zadeklarowanie zamiaru pozostania w Polsce. Najbardziej jednoznacznym sposobem potwierdzenia zamiaru pozostania jest złożenie wniosku o nadanie numeru PESEL, co skutkuje wpisem do rejestru obywateli Ukrainy, którzy przybyli do Polski z terytorium Ukrainy w związku

[29] Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku…, art. 2 ust. 4.
[30] Ustawa z 12 grudnia 2013 r. o cudzoziemcach…, art. 23,25.
[31] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad…, art. 6 ust. 5 lit. c.

z wojną[32]. Brak takiego wpisu nie wyklucza prawa do legalnego pobytu, jeżeli pozostałe przesłanki zostały spełnione.

Spełnienie powyższych warunków skutkuje automatycznym uznaniem pobytu za legalny na okres 18 miesięcy, liczonych od dnia 24 lutego 2022 r. Zgodnie z zasadami obliczania terminów, określonymi w art. 57 § 3 Kodeksu postępowania administracyjnego, oznacza to, że legalność pobytu obowiązuje do dnia 24 sierpnia 2023 r.

Z zakresu regulacji wyłączone zostały osoby posiadające zezwolenie na pobyt czasowy na pobyt stały, zgodę na pobyt ze względów humanitarnych, zgodę na pobyt tolerowany[33], zezwolenie na pobyt rezydenta długoterminowego Unii Europejskiej, zezwolenie, status uchodźcy, ochronę uzupełniającą[34]oraz które złożyły wnioski lub zadeklarowały zamiar złożenia wniosków o udzielenie ochrony międzynarodowej na terytorium Rzeczypospolitej Polskiej bądź w imieniu których takie wnioski zostały złożone lub zamiar złożenia wniosku zadeklarowany[35], chyba że wniosek lub deklaracja zostaną wycofane. Uznanie pobytu za legalny następuje z momentem wycofania wniosku lub deklaracji, a zatem przed formalnym zakończeniem postępowania w drodze decyzji o umorzeniu postępowania[36].

Diia.pl – elektroniczny dokument dla uchodźców wojennych z Ukrainy

W związku z napływem uchodźców wojennych z Ukrainy, będącym skutkiem agresji Federacji Rosyjskiej na to państwo, Polska wdrożyła szereg rozwiązań legislacyjnych i administracyjnych mających na celu zapewnienie efektywnej ochrony i integracji osób objętych działaniami specustawy. Jednym z kluczowych instrumentów potwierdzających legalność pobytu obywateli Ukrainy na terytorium Rzeczypospolitej Polskiej oraz umożliwiających im korzystanie z prawa przemieszczania się w ramach Unii Europejskiej jest elektroniczny dokument Diia.pl.

[32] Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku…, op. cit., art. 4 ust. 1.

[33] Ustawa z 12 grudnia 2013 r. o cudzoziemcach…, art. 98, art. 195, art. 211, art. 348, art. 351.

[34] Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony…, op. cit., art. 13, art. 15.

[35] Ibidem, art. 13, art. 15, art. 28 ust. 1, art. 61 ust. 1

[36] Ibidem, art. 40.

W dniu 12 lipca 2022 r. Ministerstwo Spraw Wewnętrznych i Administracji dokonało oficjalnej notyfikacji dokumentu Diia.pl Komisji Europejskiej, zgłaszając jego tymczasowe wykorzystanie jako elektronicznego potwierdzenia legalnego pobytu osób objętych przepisami ustawy z 12 marca 2022 r. o pomocy obywatelom Ukrainy. Zgłoszenie to miało na celu uregulowanie kwestii związanych z przekraczaniem granic zewnętrznych Unii Europejskiej oraz przemieszczaniem się w obrębie strefy Schengen przez osoby korzystające z ochrony czasowej na terytorium Polski[37]. Równolegle informacje o dokumencie zostały przekazane do wszystkich państw członkowskich UE oraz państw stowarzyszonych strefy Schengen.

Diia.pl stanowi instrument dokumentujący legalność pobytu, a po spełnieniu warunku posiadania ważnego dokumentu podróży, umożliwia również przekraczanie granicy zewnętrznej UE. Dodatkowo dokument ten daje jego posiadaczowi prawo do przemieszczania się w obrębie strefy Schengen przez okres 90 dni w każdym 180-dniowym okresie[38].

Diia.pl dostępna jest za pośrednictwem aplikacji mobilnej mObywatel, kompatybilnej z systemami Android oraz iOS, co stanowi przykład nowoczesnego podejścia do cyfryzacji usług publicznych i ułatwienia kontaktu obywateli z administracją publiczną. Rozwiązanie to jest istotnym elementem budowania zintegrowanego systemu zarządzania kryzysowego, opartego na narzędziach cyfrowych[39]. Dzięki aplikacji mObywatel obywatel Ukrainy, którego pobyt w Polsce jest uznawany za legalny, po uwierzytelnieniu może: pobrać, przechowywać i przedstawić dokument elektroniczny zawierający dane pobrane z rejestru obywateli Ukrainy, którym nadano numer PESEL, a także zweryfikować integralność i pochodzenie dokumentu elektronicznego[40]. Analogiczne zasady mają zastosowanie w przypadku danych dzieci pozostających pod

[37] A. Szachoń-Pszenny, *Wojna w Ukrainie jako czynnik zmiany zasad przekraczania granicy zewnętrznej UE*, Wschodni Rocznik Humanistyczny, Tom XX (2023), No 4, s. 139.

[38] M. Łysienia, *Following the EU Response to the Russian Invasion of Ukraine? The Implementation of the Temporary Protection Directive in Poland*, Central and Eastern European Migration Review Received, Vol. 12, No. 1, 2023, s.189.

[39] *Diia.pl – elektroniczny dokument dla uchodźców wojennych z Ukrainy*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/diiapl--elektroniczny-dokument-dla-uchodzcow-wojennych-z-ukrainy, [dostęp: 18.04.2025].

[40] J. Matusiak, A. Narożniak, *Diia.pl: Navigating legal, technological and human rights dimensions of an electronic document for Ukrainian citizens in Poland*, Smart Cities and Regional Development Journal, V9. I2. 2025, s.22.

władzą rodzicielską. Obywatel Ukrainy ma prawo uzyskać elektroniczną wersję dokumentu dziecka, jeżeli jego numer PESEL został powiązany z numerem PESEL dziecka w rejestrze. W przypadku braku takiego powiązania, właściwy urząd miejski może – po przedstawieniu stosownej dokumentacji potwierdzającej status rodzicielski – dokonać odpowiedniego uzupełnienia danych. Warunkiem pobrania dokumentu elektronicznego dziecka jest wówczas złożenie przez obywatela Ukrainy oświadczenia pod rygorem odpowiedzialności karnej, że dziecko znajduje się pod jego opieką rodzicielską[41].

Równolegle, w celu ujednolicenia praktyk w zakresie przemieszczania się osób korzystających z ochrony czasowej, ale nieposiadających obywatelstwa ukraińskiego, Ministerstwo Spraw Wewnętrznych i Administracji zgłosiło do Komisji Europejskiej także zaświadczenie o korzystaniu z ochrony czasowej, które wydawane jest przez Szefa Urzędu do Spraw Cudzoziemców. Dokument ten, analogicznie jak Diia.pl, pełni funkcję dokumentu pobytowego umożliwiającego przekraczanie granic i przemieszczanie się w ramach Unii Europejskiej.

Powyższe działania wpisują się w szerszy kontekst harmonizacji środków ochrony stosowanych przez państwa członkowskie Unii Europejskiej wobec osób uciekających przed skutkami konfliktu zbrojnego, wskazując jednocześnie na rolę innowacji technologicznych w zwiększaniu dostępności i efektywności usług publicznych w warunkach kryzysu migracyjnego[42].

Podsumowanie

Według autorów rozdziału, przedstawione powyżej informacje odzwierciedlają kształt regulacji zawartych w komentowanej ustawie, która była opracowywana równolegle z dynamicznie rozwijającą się sytuacją migracyjną. Ustawodawcy dążyli do bieżącego reagowania na wyzwania wynikające z masowego napływu ludności, co wymagało rozwiązań dotyczących przekraczania granicy, procesów rejestracji oraz legalizacji pobytu uchodźców. Konieczne było również wsparcie zarówno osób prywatnych udzielających schronienia, jak i jednostek samorządu terytorialnego, które musiały sprostać

[41] Ibidem, s. 22.

[42] *Diia.pl – elektroniczny dokument dla uchodźców wojennych z Ukrainy,* Ministerstwo Spraw Wewnętrznych i Administracji, Portal gov.pl, https://www.gov.pl/web/mswia/diiapl--elektroniczny-dokument-dla-uchodzcow-wojennych-z-ukrainy, [dostęp: 18.04.2025].

niespodziewanemu wzrostowi liczby mieszkańców, zapewniając im miejsca w systemie oświaty oraz dostęp do usług publicznych. Należy ponadto zauważyć, że potrzeby i oczekiwania osób przybywających do Polski ulegały zmianom w czasie, co wymagało od twórców przepisów stałego dostosowywania rozwiązań prawnych.

Rozdział stanowi kompleksową analizę rozwiązań prawnych wdrożonych w Polsce po 24 lutego 2022 r. w odpowiedzi na masowy napływ obywateli Ukrainy uciekających przed skutkami agresji zbrojnej Rosji. Autorzy skupiają się na kluczowych aspektach tzw. specustawy z 12 marca 2022 r., która ustanowiła uproszczony i szybki tryb legalizacji pobytu uchodźców wojennych oraz przyznawania im uprawnień społecznych i administracyjnych. W rozdziale wyodrębniono poszczególne kategorie osób objętych ochroną, w tym: obywateli Ukrainy, ich małżonków, dzieci urodzone w Polsce, osoby posiadające Kartę Polaka oraz najbliższych członków ich rodzin. Warunkiem uzyskania legalnego pobytu na terytorium Polski z mocy prawa (ex lege) jest spełnienie kilku przesłanek, takich jak: przyjazd po 24 lutego 2022 r., związek przybycia z wojną, legalność wjazdu oraz deklaracja zamiaru pozostania w Polsce.

W rozdziale wskazano także, że specustawa funkcjonuje równolegle z unijnym mechanizmem ochrony czasowej na mocy dyrektywy 2001/55/WE, wdrożonej decyzją Rady UE 2022/382. Współistnienie tych mechanizmów wraz z klasyczną procedurą azylową pozwoliło na zbudowanie trójtorowego systemu ochrony cudzoziemców, co znacznie zwiększyło elastyczność reagowania państwa na kryzys uchodźczy.

Autorzy rozdziału dokonali analizy roli elektronicznego dokumentu Diia.pl, który jako pierwszy w pełni cyfrowy dokument pobytowy w UE, został notyfikowany Komisji Europejskiej i umożliwia obywatelom Ukrainy nie tylko potwierdzenie legalności pobytu, ale także swobodne przemieszczanie się po strefie Schengen.

Literatura

1. Decyzja wykonawcza Rady (UE) 2022/382 z dnia 4 marca 2022 r. stwierdzająca istnienie masowego napływu wysiedleńców z Ukrainy w rozumieniu art. 5 dyrektywy 2001/55/WE i skutkująca wprowadzeniem tymczasowej ochrony, Dz. Urz. UE L 71/1 z 4.3.2022.
2. *Diia.pl – elektroniczny dokument dla uchodźców wojennych z Ukrainy*, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.gov.pl/web/mswia/diiapl--elektroniczny-dokument-dla-uchodzcow-wojennych-z-ukrainy

3. Duszczyk M., Kaczmarczyk P., *Imigranci i uchodźcy wojenni a sytuacja demograficzna Polski,* [w:] *Gościnna Polska 2022+. Jak mądrze wesprzeć Polskę i Polaków w pomocy osobom uciekającym przed wojną w Ukrainie?*, Warszawa 2022.
4. *Dyrektywa Rady 2001/55/WE z dnia 20 lipca 2001 r. w sprawie minimalnych standardów przyznawania tymczasowej ochrony na wypadek masowego napływu wysiedleńców oraz środków wspierających równowagę wysiłków między Państwami Członkowskimi związanych z przyjęciem takich osób wraz z jego następstwami*, Dz. Urz. UE L 212/12 z 7.8.2001.
5. *International students in Ukraine*, Ministry of Education and Science of Ukraine, https://studyinukraine.gov.ua/statistic/.
6. Komunikat Komisji zawierający wytyczne operacyjne dotyczące zarządzania granicami zewnętrznymi w celu ułatwienia przekraczania granicy między UE a Ukrainą 2022/C 104 I/01, Dz. Urz. UE C 104 I z 4.3.2022.
7. Łysienia M., Following *the EU Response to the Russian Invasion of Ukraine? The Implementation of the Temporary Protection Directive in Poland*, Central and Eastern European Migration Review Received, Vol. 12, No. 1, 189, 2023.
8. Matusiak J., Narożniak A., *Diia.pl: Navigating legal, technological and human rights dimensions of an electronic document for Ukrainian citizens in Poland*, Smart Cities and Regional Development Journal, V9. I2. 2025.
9. *Ochrona międzynarodowa w 2022 r.,* Urząd do Spraw Cudzoziemców, https://www.gov.pl/web/udsc/ochrona-miedzynarodowa-w-2022-r.
10. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen), Dz. Urz. UE L 77/1
11. Sobestjańska A., Sopińska A., *Miejska gościnność: wielki wzrost, wyzwania i szanse. Raport o uchodźcach z Ukrainy w największych polskich miastach*, Unia Metropolii Polskich im. P. Abramowicza, Warszawa 2022.
12. Szachoń-Pszenny A., *Wojna w Ukrainie jako czynnik zmiany zasad przekraczania granicy zewnętrznej UE*, Wschodni Rocznik Humanistyczny, Tom XX, No 4, 2023.
13. Ukraine Refugee Situation, https://data.unhcr.org/en/situations/ukraine
14. *Ukraine Immigration Statistics 1990-2025,* https://www.macrotrends.net/countries/UKR/ukraine/imigration-statistics.
15. Ustawa z 12 grudnia 2013 r. o cudzoziemcach, Dz.U. z 2021 r. poz. 2354 ze zm.
16. Ustawa z 23 kwietnia 1964 r. Kodeks cywilny, Dz.U. z 2024 r. poz. 1237.
17. Ustawa z 23 marca 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, Dz. U. 2022 poz. 683.
18. Ustawa z 6 czerwca 1997 r. Kodeks karny, Dz.U. z 2025 r. poz. 383.
19. Ustawa z 8 czerwca 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz niektórych innych ustaw, Dz.U. poz. 1383.
20. Ustawa z 8 kwietnia 2022 r. o zmianie ustawy o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa oraz niektórych innych ustaw, Dz.U. poz. 830.

21. Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, Dz. U. z 2025 r. poz. 337.
22. Ustawa z dnia 13 czerwca 2003 r. o udzielaniu cudzoziemcom ochrony na terytorium Rzeczypospolitej Polskiej, Dz. U. z 2025 r., poz. 389.
23. Ustawa z dnia z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, Dz. U. z 2024 poz. 1897.
24. Ustawa z ustawy z dnia 7 września 2007 r. o Karcie Polaka, Dz.U. z 2019 r., poz. 1598 ze zm.

dr Dariusz Brążkiewicz
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-5372-1210

lic. Rafał Mazurek
Akademia Sztuki Wojennej w Warszawie

https://doi.org/10.29316/9788368103205_7

ROZBUDOWA ROSYJSKICH WOJSK POWIETRZNODESANTOWYCH I SKALA ICH UŻYCIA W WOJNIE ROSYJSKO-UKRAIŃSKIEJ OD 2022 R.

EXPANSION OF RUSSIAN AIRBORNE TROOPS AND THE SCALE OF THEIR USE IN THE RUSSIAN-UKRAINIAN WAR FROM 2022

Streszczenie

Bezpośrednia agresja Federacji Rosyjskiej na Ukrainę w 2022 r. pokazała skalę, w tym zaangażowanie poszczególnych rodzajów sił zbrojnych obu walczących państw. Po stronie rosyjskiej, szczególnie w pierwszych dniach wojny, ale nie tylko, duże znaczenie miały działania Wojsk Powietrznodesantowych. W związku z elitarnym, różnorodnym szkoleniem, wojska te po rozpadzie Związku Radzieckiego, nadal były traktowane jako priorytetowe siły we wszelkiego rodzaju działaniach w głębi obszaru przeciwnika oraz gwarancja sukcesu poprzez zaskoczenie i wyszkolenie. Przedmiotem badań

Summary

The direct aggression of the Russian Federation against Ukraine in 2022 showed its scale, including the involvement of individual types of armed forces of both warring countries. On the Russian side, especially in the first days of the war, but not only, the actions of the Airborne Troops were of great importance. Due to their elite, diverse training, these troops, after the collapse of the Soviet Union, were still treated as priority forces in all types of operations deep in the enemy's area and a guarantee of success through surprise and training. The subject of the research of this work is the importance of

niniejszego rozdziału jest znaczenie Wojsk Powietrznodesantowych w armii rosyjskiej i ich możliwości we współczesnych konfliktach zbrojnych. Celem rozdziału jest przedstawienie budowy rosyjskich Wojsk Powietrznodesantowych i ich wykorzystanie na wojnie rosyjsko-ukraińskiej. W związku z przedmiotem badań i celem badań, powstał główny problem badawczy, który został wyrażony w postaci następującego pytania: Jakie znaczenie mają Wojska Powietrznodesantowe Federacji Rosyjskiej na współczesnym polu walki i jakie są ich możliwości w prowadzonych działaniach bojowych? Poszukiwanie naukowych rozstrzygnięć, w odniesieniu do określonego głównego problemu badawczego, wymagało przyjęcia i rozwiązania szczegółowych problemów badawczych: 1) Jak realizowano transformację i użycie Wojsk Powietrznodesantowych w Federacji Rosyjskiej? 2) Jaka była skala reformy organizacyjno-strukturalnej rosyjskich Wojsk Powietrznodesantowych w pierwszych latach XXI wieku? 3) Jaka była skala zaangażowania rosyjskich Wojsk Powietrznodesantowych w wojnę rosyjsko-ukraińską? Przeprowadzone badania wstępne, określony cel badań i problemy badawcze, zdeterminowały przyjętą na potrzeby badań hipotezę główną: Znaczenie wojsk powietrznodesantowych dla współczesnego pola walki ma ważne znaczenie wynikające z elitarności przygotowania tego rodzaju jednostek do działania. Weryfikacji dostępnych materiałów dokonano poprzez analizę i krytykę dostępnej literatury przedmiotu oraz faktów z informacji prasowych.

Słowa kluczowe: Wojska Powietrznodesantowe Federacji Rosyjskiej, wojna rosyjsko-ukraińska

the Airborne Troops in the Russian Army and their capabilities in modern armed conflicts. The aim of the work is to present the structure of the Russian Airborne Troops and their use in the Russian-Ukrainian war. In connection with the subject of the research and the purpose of the research, the main research problem was formed, which was expressed in the form of the following question: What is the significance of the Airborne Troops of the Russian Federation on the modern battlefield and what are their capabilities in combat operations? The search for scientific solutions, in relation to the specified main research problem, required the adoption and solution of detailed research problems: 1) How was the transformation and use of the Airborne Troops implemented in the Russian Federation? 2) What was the scale of the organizational and structural reform of the Russian Airborne Troops in the first years of the 21st century? 3) What was the scale of the involvement of the Russian Airborne Troops in the Russian-Ukrainian wars? The preliminary research, the specific research goal and research problems determined the main hypothesis adopted for the research: The importance of airborne troops on the modern battlefield is of great importance resulting from the elite preparation of such units for combat. The verification of available materials was carried out by analyzing and criticizing the available literature on the subject and facts from press releases.

Keywords: airborne troops of the Russian Federation, Russian-Ukrainian war

Wstęp

Jednym z ważnych elementów składowych każdych sił zbrojnych są wojska specjalne. Ich specjalistyczne przygotowanie, połączone z dobrą selekcją żołnierzy, pozwala otrzymać sprawne narzędzie walki w różnym środowisku, jak i z przeważającymi siłami. W przypadku Federacji Rosyjskiej, kraj ten stał się kontynuatorem Wojsk Powietrznodesantowych rozwijanych od lat 30. XX wieku w Związku Radzieckim. Na przestrzeni wielu lat i wielu konfliktów zbrojnych pokazano ich zwiększone możliwości w stosunku do zwykłych jednostek lądowych. Przygotowanie do szybkiego przerzutu drogą powietrzną pozwala na sprawne użycie tych wojsk, gwarantując możliwie szybką interwencję lub ingerencję.

Znaczenie Wojsk Powietrznodesantowych potwierdzają kolejne konflikty zbrojne, a dobitnym tego przykładem jest wojna rosyjsko-ukraińska. Pomijając skryte działania tych wojsk w 2014 r., to ich masowe użycie rozpoczęło się w 2022 r. po agresji na Ukrainę. Generalnie w różnych odstępach czasu większość jednostek rosyjskich Wojsk Powietrznodesantowych uczestniczyła w walkach na froncie. Ich możliwości nie zawsze były w stanie pokonać dobrze przygotowane wojska ukraińskie, co pokazuje, że ten rodzaj wojsk jest również narażony na ponoszenie wysokich strat, wynikających ze specyfiki wykonywanych zadań. W omawianym konflikcie zbrojnym, rosyjskie Wojska Powietrznodesantowe w ograniczony sposób realizowały swoje zadania drogą powietrzną, a wynikało to z wysokiego zagrożenia porażeniem ogniowym środków transportowych, czy to samolotów, czy śmigłowców.

Wojska powietrznodesantowe w powstającej Federacji Rosyjskiej

Federacja Rosyjska, po odziedziczeniu Sił Zbrojnych byłego Związku Radzieckiego w 1991 roku, borykała się z wieloma problemami, głównie finansowymi. To było przyczynkiem permanentnej redukcji, szczególnie w pierwszej połowie lat 90. Wynikało to również z faktu, że wiele jednostek wojskowych wyprowadzonych z tworzących się nowych państw byłego związku republik, miało niską wartość bojową, ze względu na niski procent ukompletowania w uzbrojenie i sprzęt wojskowy, co powodowało, że w pierwszej kolejności poddawano je likwidacji. Te i wiele innych czynników, wpływało na funkcjonowanie armii, a wśród najważniejszych należy wymienić:

- system mobilizacji żołnierzy przystosowany do wojny na pełną skalę (między innymi z Chinami oraz krajami Paktu Północnoatlantyckiego),
- brak w pełni ukompletowanego stanu osobowego, gdzie większość jednostek posiadała liczebność w okolicach 50%, a w przypadku oddziałów skadrowanych, wynosiło to w okolicach 15%,
- system dowodzenia przejęty ze Związku Radzieckiego, poprzez mnogość szczebli dowodzenia, komplikował działania (przygotowany był głównie na realizowanie planów mobilizacyjnych),
- różnorodność rodzajów uzbrojenia, co prowadziło do uznawania kilku ich rodzajów za np. czołg podstawowy,
- duża ilość broni składowana w magazynach (przeznaczona na mobilizację) wymagała oddelegowania do jej dozorowania w składach i jednostkach remontowych znaczącej część personelu[1].

Ponadto rozpad Związku Radzieckiego przysporzył również problemów natury lokalizacji sił rosyjskich. Nie we wszystkich byłych republikach proces przenoszenia jednostek wojskowych na teren powstałej Federacji Rosyjskiej odbywał się bezproblemowo. Dla przykładu, by rozwiązać problem rozlokowania byłych jednostek wojskowych między byłe republiki radzieckie w obszarze Azji Centralnej, doszło w 1992 r. do spotkania prezydentów Rosji, Kazachstanu, Kirgistanu i Uzbekistanu w Taszkiencie. Na mocy osiągniętych porozumień w latach 1992-1993 jednostki Federacji Rosyjskiej – w tym powietrznodesantowe – zostały przeniesione na terytorium Rosji[2].

Jeden z wyjątków stanowi Naddniestrze, które jest prorosyjskim, separatystycznym regionem Mołdawii wspieranym przez Federację Rosyjską, lecz nieuznawanym przez społeczność międzynarodową. Stacjonuje w tym regionie około 2 tysiące rosyjskich żołnierzy, pozbawionych ciężkiego sprzętu pod szyldem „kontyngentu pokojowego", wspólnie z niewielką lokalną armią, której siły posiadają również oddział powietrznodesantowy. Regionem rządzi nomenklatura wywodząca się ze służb specjalnych Związku Radzieckiego.

[1] M. Jastrzębski, *Zmiany struktur organizacyjnych i wzrost potencjału Wojsk Lądowych Federacji Rosyjskiej po reformach 2009 roku*, [w:] *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, red. R. Prusak, E. Kardas, Wydawnictwo Uniwersytetu Kazimierza Wielkiego, Bydgoszcz 2016, s. 250-251.

[2] J. Elfving, *An Assessment of the Russian Airborne Troops and Their Role on Tomorrow's Battlefield*, The Jamestown foundation, Waszyngton 2021, s. 6.

Federacja Rosyjska, tak samo jak w przypadku separatystycznych regionów Ukrainy i w tym przypadku, deklaruje szanowanie praw separatystów[3].

Wojska Powietrznodesantowe Federacji Rosyjskiej (WDW)[4], tak zwany Desant, stanowi elitarny element Sił Zbrojnych Federacji Rosyjskiej od 1992 r., będący kontynuacją sowieckich wojsk powietrznodesantowych, których początek stanowi umowna data 2 sierpnia 1930 r., kiedy to po raz pierwszy podczas ćwiczenia dokonano zrzutu spadochronowego niewielkiego oddziału dywersyjnego, którego zadaniem było operowanie na tyłach przeciwnika. Rozwój wojsk powietrznodesantowych przebiegał równolegle z rozwojem aktualnego Specnazu, co wskazuje na wykonywanie zbliżonych zadań podczas tworzenia obydwu formacji. Dodatkowo, kwestią wartą zaznaczenia, jest przechodzenie Specnazu spod kontroli wywiadu wojskowego, pod kontrolę wojsk powietrznodesantowych[5]. Od 1934 r. wojska Związku Radzieckiego zaczęły przeprowadzać zmasowane zrzuty ćwiczebne spadochroniarzy, zaczynając od desantu 900 osób. Rok później zrzucono blisko 1200 skoczków w tym samym czasie, następnie kolejne ponad 1750 żołnierzy wspartych lekkimi czołgami, artylerią oraz samochodami pancernymi. Ćwiczebne wykorzystanie tak dużej siły, świadczyło o testowaniu w praktyce wykorzystania WDW do działań zaczepnych, ofensywnych. Już w 1938 r. radzieckie wojska powietrznodesantowe liczyły 6 brygad, w tym około 18 tysięcy ludzi. Natomiast wkraczając w drugą wojnę światową, Związek Radziecki dysponował milionem wyszkolonych spadochroniarzy[6].

W ciągu swojego istnienia po powstaniu Federacji Rosyjskiej, Wojska Powietrznodesantowe brały udział we wszystkich konfliktach, w których zaangażowane było nowo powstałe państwo. Wraz ze Specnazem brały udział w I i II wojnie czeczeńskiej, wojnie rosyjsko-gruzińskiej z 2008 r., w Kirgizji w 2010 r., w Syrii od 2015 do 2024 r., w Kazachstanie w 2022 r., podczas aneksji Krymu w 2014 r. oraz w pełnoskalowej agresji Federacji Rosyjskiej na Ukrainę w 2022 r[7].

---

[3] *Naddniestrze. V kolumna Rosji na zapleczu frontu [Armie Świata odc. 59]*, Defence24, portal youtube.com, https://www.youtube.com/watch?v=rfcQ9f7d5Mo, [dostęp: 28.05.2025].

[4] Wozduszno-Diesantnyje Wojska (WDW), Воздушно-десантные войска (ВДВ).

[5] W. Suworow, *Specnaz. Historia sił specjalnych armii radzieckiej*, Rebis, Poznań 2011, s. 69.

[6] Ibidem, s. 70-71.

[7] T. W. Grabowski, *Rosyjska Siła…* op.cit., s. 153-154.

Sztab WDW znajduje się w Moskwie, a podlega bezpośrednio pod Naczelnego Dowódcę Sił Zbrojnych FR, co zapewnia możliwość szybkiego przerzutu i desantu w miejscu określonym przez ww. dowódcę[8].

Obecnie WDW przeznaczone jest do ataku z powietrza i prowadzenia działań bojowych na operacyjnych i strategicznych tyłach nieprzyjaciela. Wśród jej literalnych zadań należy wymienić:

- przejmowanie centrów administracyjno-politycznych, węzłów komunikacyjnych, obiektów przemysłowych, lotnisk oraz baz morskich,
- zajęcie ważnych dróg komunikacyjnych (ważnych z punktu widzenia prowadzonej operacji),
- niszczenie najważniejszych obiektów wojskowych, łączności i dezorganizację tyłów wroga oraz uniemożliwianie formowania i przerzutu rezerw ludzkich i materiałowych[9].

Jako jedne z niewielu w latach 90. ubiegłego stulecia rosyjskie Wojska Powietrznodesantowe zachowywały stan ciągłej gotowości bojowej i były wyposażone w jeden z najlepszych możliwych sprzętów.

Charakterystycznym elementem ubioru żołnierzy rosyjskiego desantu jest niebieski beret, szarfy Św. Jerzego (zapoczątkowane w czasach carskich pomarańczowo-czarne odznaczenia odnoszące się do Orderu Świętego Jerzego) oraz koszulka w paski „Tielniaszka" (charakterystyczna niebieska koszulka w białe paski noszona również przez Specnaz, piechotę morską i marynarzy)[10].

Wojska Powietrznodesantowe Federacji Rosyjskiej po 1991 r. zaznaczyły swoją obecność również w misjach pokojowych, stabilizacyjnych:

- IFOR (Implementation Force) Międzynarodowe Siły Implementacyjne w Bośni i Hercegowinie – misja trwała od 20 grudnia 1995 r. do 20 grudnia 1996 r. W przeciągu roku w działaniach uczestniczyło 60 tysięcy żołnierzy z 32 państw. Zadaniami misji było zapewnienie o przestrzeganiu zawieszenia broni, nadzór nad wycofaniem i rozmieszczeniem stron konfliktu zgodnie z poprzednio ustalonymi strefami, wsparcie w procesie

[8] Ibidem.

[9] T. W. Grabowski, *Rosyjska Siła. Siły Zbrojne i główne problemy polityki obronnej Federacji Rosyjskiej w latach 1991-2010*, Instytut Geopolityki, Częstochowa 2011, s. 152.

[10] M. Szopa, *Armie Świata: Wojska Powietrznodesantowe Rosji (WDW)*, portal defence24.pl, https://defence24.pl/sily-zbrojne/armie-swiata-wojska-powietrznodesantowe-rosji-wdw, [dostęp: 02.05.2025].

rozminowywania, ochrona ludności cywilnej oraz pomoc humanitarna[11]. Rosyjskie Wojska Powietrznodesantowe podczas misji współpracowały z amerykańską 1. Dywizją Pancerną[12].

- SFOR (Stabilization Force) – zostały rozlokowane na terenie Bośni i Hercegowiny 20 grudnia 1996 r., misja trwała do 2 grudnia 2004 r. (przekazano misję siłom UE, zmiana mandatu na EUFOR). Głównym celem misji było zapobieganie wznowieniu działań wojennych oraz nadzór nad wdrażaniem wojskowych aspektów zawartych w układzie pokojowym z Dayton. SFOR zastąpiło wcześniejszy IFOR. Podczas misji brało udział (w zależności od okresu) od 19-30 tysięcy żołnierzy[13]. Brygada rosyjskich sił pokojowych w misji SFOR stacjonowała w sektorze USA – Wielonarodowej Dywizji Północ. W początkowej fazie misji rosyjskie siły liczyły 1200 żołnierzy Wojsk Powietrznodesantowych, które były odpowiedzialne za obszar około 1800 kilometrów[14].
- KFOR (Kosovo Force) – to międzynarodowe siły stabilizacyjne NATO w Kosowie rozmieszczone w czerwcu 1999 r., stacjonujące do chwili obecnej. Głównym celem misji jest zapewnienie bezpieczeństwa, stabilizacja regionu oraz wspieranie procesu odbudowy i rozwoju demokratycznych struktur państwowych po zakończeniu konfliktu zbrojnego. Wśród uczestników misji należy wymienić państwa NATO oraz państwa partnerskie. W początkowej fazie misji siły liczyły około 50 tysięcy żołnierzy[15]. Podczas początkowej fazy misji KFOR rosyjskie Wojska Powietrznodesantowe współpracowały z 9. Batalionem Operacji Psychologicznych armii USA[16].

[11] *IFOR*, portal wojsko-polskie.pl, https://www.wojsko-polskie.pl/ifor-bih/, [dostęp: 28.05.2025].

[12] J. W. Kipp, *US-Russian Military Cooperation and the IFOR Experience: A Comparison of Survey Results*, portal bits.de, https://www.bits.de/NRANEU/docs/Kipp98.htm, [dostęp: 28.05.2025].

[13] *Siły Stabilizacyjne NATO SFOR*, portal wojsko-polskie.pl, https://www.wojsko-polskie.pl/sfor-bih/, [dostęp: 28.05.2025].

[14] *NATO and Russia: Partners in Peacekeeping*, portal nato.int, https://www.nato.int/docu/presskit/010219/brocheng.pdf, [dostęp: 28.05.2025].

[15] *Siły dla Kosowa, KFOR ONZ*, portal wojsko-polskie.pl, https://www.wojsko-polskie.pl/kfor-kosowo/, [dostęp: 28.05.2025].

[16] *American and Russian soldiers pass out flyers to the citizens of Kamenica, Kosovo*., portal defense.gov, https://www.defense.gov/Multimedia/Photos/igphoto/2002018201/, [dostęp: 28.05.2025].

Zasadniczą reformę WDW zapoczątkowano w 2008 r., choć działania reorganizacyjne i modernizacyjne z lat 2009-2016 przypisuje się działaniom rozpoczętym w 2005 r. Nowa koncepcja (wykorzystania Wojsk Powietrznodesantowych jako sił szybkiego reagowania) wpłynęła na strukturę organizacyjną jednostek oraz ich wyposażenie. W 2010 r. przyjęta została Koncepcja rozwoju Wojsk Powietrznodesantowych do 2025 r., zakładająca profesjonalizację większości pododdziałów, oddziałów i związków taktycznych. Doprowadzono również do specjalizacji jednostek i podziału na spadochronowo-desantowe i desantowo-szturmowe[17].

Podczas wojny rosyjsko-gruzińskiej, w sierpniu 2008 r. wykorzystano Wojska Powietrznodesantowe, lecz zrezygnowano z desantowania spadochronowego. Pomimo pominięcia standardowego sposobu dyslokacji żołnierzy, WDW odegrało kluczową rolę, gdyż było jednym z nielicznych narzędzi do działania w obszarze przeciwnika zdolnym do prowadzenia działań rajdowych. Czas konfliktu uniemożliwiał rozwinięcie pełnych sił Wojsk Powietrznodesantowych (nie przerzucono całego pułku lub dywizji, wykorzystywano taktyczne bataliony i kompanijne grupy bojowe)[18].

Podczas operacji przejmowania Półwyspu Krymskiego w 2014 r., brało udział około 6 tysięcy żołnierzy Wojsk Powietrznodesantowych, których skryty transport na półwysep odbywał się drogą morską lub powietrzną (również zrezygnowano z desantu spadochronowego). Do przeprowadzenia operacji sformowanych zostało około 11 taktycznych batalionowych grup bojowych, była to blisko połowa sił zaangażowanych w działalność na półwyspie. Po osiągnięciu celu strategicznego, wycofano z półwyspu Wojska Powietrznodesantowe i rozlokowano je na wschodniej linii granicznej z Ukrainą, skąd wiosną 2014 r. pełniły zadania wspierające separatystów w Donieckiej oraz Ługańskiej Republice Ludowej[19].

[17] R. Ciechanowski, *Wojska Powietrznodesantowe – modernizacja techniczna w latach 2008-2017*, Nowa Technika Wojskowa Numer Specjalny nr 14, 2018.

[18] M. Depczyński, *Zmiany w rosyjskich Wojskach Powietrznodesantowych*, Nowa Technika Wojskowa nr 3, 2021.

[19] Ibidem.

Reformy organizacyjno-strukturalne jednostek powietrznodesantowych w XXI wieku

W 2010 r., zgrupowania wchodzące w skład Wojsk Powietrznodesantowych Federacji Rosyjskiej liczyły około 33 tysięcy żołnierzy, a struktura przedstawiała się następująco:

- 98. Dywizja Powietrznodesantowa,
- 106. Dywizja Powietrznodesantowa,
- 7. Dywizja Desantowo-Szturmowa,
- 76. Dywizja Desantowo-Szturmowa,
- 31. Samodzielna Brygada Desantowo-Szturmowa,
- 45. Samodzielny Pułk Wywiadowczy Specjalnego Przeznaczenia,
- 38. Samodzielny Pułk Łączności[20].

Od 2013 r. kompanie rozpoznawcze w dywizjach powietrznodesantowych i powietrzno-szturmowych zostały przeorganizowane w bataliony wywiadowcze. Podczas trwania tego procesu, równocześnie od 2016 r., dodano więcej nowych jednostek: kompanie czołgów, bezzałogowych statków powietrznych (BSP) i walki radioelektronicznej. Za wprowadzenie do wojsk powietrznodesantowych jednostek BSP i przeciwdziałania radioelektronicznego, uważa się implikowanie wniosków Rosji z wojny z Gruzją w 2008 r., operacji w Ukrainie od 2014 r. i operacji syryjskiej. Już z początkiem 2019 r. WDW dysponowało sześcioma kompaniami BSP i dwoma plutonami BSP[21].

Federacja Rosyjska, niejednokrotnie wykorzystywała taktykę demonstracji siły poprzez prowadzenie manewrów wojskowych z państwami Organizacji Układu o Bezpieczeństwie Zbiorowym przy granicach Unii Europejskiej. Niejednokrotnie, dokonując naruszania przestrzeni powietrznej czy morskiej (za naruszenia odpowiadała flota Bałtycka i Czarnomorska) krajów zachodnich, prowadzono testy gotowości obronnej oraz szukano luk w zabezpieczeniach systemów NATO i UE. Na początku 2014 r., dokładnie w marcu, przeprowadzono wspólne ćwiczenia wojsk obrony powietrznej Zachodniego Okręgu Wojskowego wraz z Wojskami Powietrznodesantowymi. Ćwiczenie obejmowało desant 350 spadochroniarzy na Wyspach Nowosyberyjskich, przy bardzo niebezpiecznych warunkach pogodowych – podczas silnego wiatru, gdy temperatura wynosiła minus 15 stopni Celsjusza. Miesiąc później

[20] T. W. Grabowski, *Rosyjska Siła…,* op. cit., s. 152.

[21] J. Elfving, *An Assessment of...,* op. cit., s. 12.

przeprowadzono ćwiczenia z udziałem piechoty morskiej i desantu w Dagestanie, gdzie głównym naciskiem ćwiczenia była walka z nieregularnymi formacjami zbrojnymi przeciwnika[22]. W 2015 r. wykorzystano blisko 2000 żołnierzy Wojsk Powietrznodesantowych do manewrów przy granicy z Estonią, jednocześnie twierdząc, że działania miały charakter wyłącznie obronny[23].

Rok później, w 2016 r. przeprowadzono ćwiczenia, które wcześniej nigdy się nie odbyły. Żołnierze Wojsk Powietrznodesantowych przeprowadzili desant na dryfującą krę w okolicach bieguna północnego. Na miejscu nie dostarczono żołnierzom żadnego dodatkowego sprzętu, wszystko, z czym przyszło im ćwiczyć, musieli zabrać ze sobą. Wcześniej zostali wyposażeni w specjalistyczny sprzęt (mundury odpowiednie na warunki arktyczne, plecaki ekspedycyjne, specjalne racje żywnościowe (zawierające więcej kalorii, by żołnierz operujący w trudnych warunkach mógł zaspokoić wzmożone zapotrzebowanie energetyczne, wynikające z wymagających warunków atmosferycznych i wydatku energetycznego przy działaniach standardowych), zaprojektowano również specjalistyczne dwu-trzy stopniowe podgrzewacze do jedzenia, które spełniały założone cele, nawet przy minus 50 stopniach Celsjusza[24].

Od 2009 r. Wojska Powietrznodesantowe Federacji Rosyjskiej prowadzą co roku ćwiczenia z białoruskimi Siłami Operacji Specjalnych i naziemnymi pododdziałami obrony powietrznej Sił Zbrojnych Republiki Białoruskiej. Działania odbywają się zarówno na poligonach Federacji Rosyjskiej oraz Białorusi. Współpraca odbywa się na szczeblu taktycznym, co w niedalekiej przeszłości było sporadycznym działaniem, obecnie stało się normą. Podczas ćwiczeń dochodzi do integracji obydwu wojsk, wymiany pomiędzy jednostkami, gdzie trenuje się działanie mniejszych pododdziałów białoruskich w ramach jednostki rosyjskiej i odwrotnie, a także charakter bardziej mieszany świadczący o ścisłej kooperacji i badaniu potencjalnego przyszłego wykorzystania Sił Zbrojnych Republiki Białorusi jako integralnej części Sił Zbrojnych Federacji Rosyjskiej (zmiana nazewnictwa brygad mobilnych Republiki Białorusi na brygady desantowo-szturmowe również świadczy o procesie unifikacji).

[22] A. M. Dyner, *Rosyjskie ćwiczenia wojskowe - przesłanie dla przeciwników i sojuszników*, Biuletyn PISM, nr 90(1202), 2014, s. 1-2.

[23] I. Topolski, *Manewry wojskowe jako forma demonstracji siły militarnej Federacji Rosyjskiej w Europie*, Wschód Europy. Studia humanistyczno-społeczne, 5(1), 2019, s. 195.

[24] A. Oszczęda, *Perspektywy rozwoju i modernizacja SM FR w aspekcie „arktycznego" wyścigu zbrojeń*, Rocznik Bezpieczeństwa Morskiego nr 11, 2017, s. 92.

Ćwiczenia mieszanych pododdziałów rozpoczęły się w kwietniu 2012 r. i miały miejsce dwa razy do roku, od 2017 r. nastąpiła intensyfikacja szkolenia i odbywają się już trzy razy w ciągu roku[25].

Ważną kwestią w kontekście współpracy Wojsk Powietrznodesantowych z innymi armiami są ćwiczenia „Słowiańskie Braterstwo", kiedy to w latach 2016-2019 siły zbrojne Federacji Rosyjskiej i Białorusi trenowały wspólnie z formacjami powietrznodesantowymi Serbii[26].

Warto zaznaczyć również kwestię wykorzystywania do szkolenia białoruskiego desantu sprzętu, który na co dzień nie jest powszechnie dostępny, mianowicie nowoczesnego sprzętu produkowanego przez Federację Rosyjską, na przykład bojowych wozów piechoty BMD-4M[27].

Wśród wyposażenia rosyjskich Wojsk Powietrznodesantowych występują następujące grupy uzbrojenia i sprzętu:

- Wybrane pojazdy:
  - Tigr – wielozadaniowy samochód opancerzony w układzie 4x4, produkowany od 2005 r. W 2010 r. został zmodernizowany do wersji Tigr-M. Przewozi do 9 żołnierzy, ma silnik o mocy 215 KM, może być uzbrojony w karabin maszynowy 12,7mm lub granatnik ASG-30 (30mm)[28],
  - Ryś – rosyjska wersja włoskiego opancerzonego samochodu IVECO LMV, Rysie obok Tigrów są wykorzystywane do akcji rozpoznawczo-patrolowych z racji swojej mobilność[29],
  - BMD-2 – bojowy wóz piechoty radzieckiej produkcji przeznaczony dla desantu. Jest pływającym wozem gąsienicowym przystosowanym do transportu drogą lotniczą i desantu na spadochronie. Produkowany od 1985 r. Wyposażony w 30 mm automatyczne działko, karabin

[25] A. Wilk, *Rosyjska armia białoruska. Praktyczne aspekty integracji wojskowej Białorusi i Rosji.* Raport OSW, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2021, s. 33-36.

[26] Ibidem.

[27] Ibidem.

[28] A. Świerkowski, *Armia 2023: Pancerny Tigr rodem z Mad Maxa*, portal defence23.pl, https://defence24.pl/przemysl/armia-2023-pancerny-tigr-rodem-z-mad-maxa, [dostęp: 27.05.2025].

[29] A. Charuk, *Rosyjska egzotyka – rzadkie pojazdy opancerzone na wojnie z Ukrainą*, Nowa Technika Wojskowa nr 5, 2023.

maszynowy PKT oraz wyrzutnię przeciwpancernych pocisków kierowanych[30],

- BMD-4M – pływający bojowy wóz piechoty desantu, wyposażony w armatę kalibru 100 mm, działko automatyczne 30 mm i karabin maszynowy. Armatę stu milimetrową można wykorzystywać do rażenia celów pociskami kierowanymi. Sprawdza się w walce z dronami[31],
- BTR-D – gąsienicowy transporter opancerzony mogący przetransportować do 10 żołnierzy desantu. Pojazd pływający przystosowany do transportu lotniczego i zrzutu spadochronowego. Wyposażony w karabin maszynowy 7,62 mm. Jest solidną podstawą, na której powstało wiele specjalistycznych wersji między innymi wozy dowodzenia, techniczne, niszczyciele czołgów.[32].
- BTR-82AM (130 sztuk) – kołowy transporter opancerzony 8x8. Wyposażony w automatyczną armatę kal. 30 mm oraz karabin maszynowy 7,62 mm. Wielowarstwowa podłoga chroni przed minami i IED. Maksymalna prędkość 80km/h i zasięg do 600 km. Transporter jest pływający, zawierający nowoczesne systemy łączności i nawigacji satelitarnej[33],
- T-72B3 (łącznie 160 sztuk) – modernizacja czołgu T-72B. Zastosowano pancerz reaktywny Kontakt-5, zwiększono moc silnika do 840 KM, zainstalowano nowy system kierowania ogniem oraz dzięki zastosowaniu armaty 2A46M istnieje możliwość użycia nowoczesnej amunicji i pocisków kierowanych[34].

- Wybrane śmigłowce i samoloty:
  - Ka-52 – dwumiejscowy śmigłowiec bojowy produkowany od 2005 r. (seryjna produkcja rozpoczęta w 2010 r.). Charakterystycznym elementem konstrukcyjnym jest unikalny układ wirników. Wyposażony

[30] *BMD-2*, portal opisybroni.pl, https://opisybroni.pl/bmd-2/, [dostęp: 27.05.2025].

[31] Ł. Michalik, *Rosyjski sposób na drony. Chcą użyć 100-mm armat z pojazdów BMD-4*, 15.04.2025, portal tech.wp.pl, https://tech.wp.pl/rosyjski-sposob-na-drony-chca-uzyc-100-mm-armat-z-pojazdow-bmd-4,7146831019465248a, [dostęp: 27.05.2025].

[32] *BTR-D*, portal opisybroni.pl, https://opisybroni.pl/btr-d/, [dostęp: 27.05.2025].

[33] *BTR-82A BTR-82AM*, portal armyrecognition.com, https://armyrecognition.com/military-products/army/armoured-personnel-carriers/wheeled-vehicles/btr-82a-russia-uk, [dostęp: 27.05.2025].

[34] P. Przeździecki, *Czołg podstawowy T-72B3*, Wojsko i Technika, nr 8, 2017.

w nowoczesne systemy kontroli pola walki. Przeznaczony do zadań wsparcia, rozpoznania i zwalczania celów opancerzonych[35],

- Mi-28N – śmigłowiec szturmowy (odpowiednik AH-64 Apache). Produkowany od końca lat 90. XX wieku, a przyjęty na uzbrojenie rosyjskich sił zbrojnych w 2009 r. Przetestowany w działaniach bojowych w Syrii, Iraku i Algierii. Konstrukcja klasyczna – pięciopłatowy wirnik górny i krzyżowy ogonowy. Dwóch pilotów siedzi w układzie tandem. Nazwę Nocnego Łowcy zawdzięcza systemom umożliwiającym operacje nocne oraz w ciężkich warunkach[36],
- Ił-76 – czterosilnikowy samolot transportowy. W wojskach powietrznodesantowych odpowiada za przerzut wojsk i sprzętu. Ma możliwość przewożenia ładunków do 33 ton oraz możliwość przewiezienia od 167 do 245 żołnierzy. Na bazie Ił-76 powstało wiele wersji specjalistycznych, m.in. samoloty-szpitale, pasażerskie oraz przeciwpożarowe[37].

- Przykładowe wyposażenie Kompanii WRE:
  - RB-531 Infauna – kołowy system walki radioelektronicznej na podwoziu BTR-80. Służy do ochrony wojsk i pojazdów przed zdalnie odpalanymi ładunkami, zagłusza środki łączności przeciwnika i prowadzi rozpoznanie elektroniczne. Załogę stanowi od 3 do 5 osób, a konstrukcja umożliwia przemieszczanie się w wodzie (właściwości amfibijne)[38],
  - Leer-2 – mobilny system walki radioelektronicznej na pojeździe Tigr-M. Przeznaczony do wykrywania, zakłócania i tłumienia środków łączności przeciwnika, wliczając w to sieci telefonii komórkowej. System może działać w ruchu i w pozycji statycznej. Załogę stanowi 2 żołnierzy oraz 4 operatorów[39],

[35] P. Butowski, *Kamow Ka-52 Aligator*, Lotnictwo Aviation International nr 12, 2019.

[36] P. Butowski, *Śmigłowiec szturmowy Mil Mi-28N Nocny Myśliwy*, Lotnictwo Aviation International nr 11, 2019.

[37] P. Butowski, *Iljuszyn Ił-76*, Lotnictwo Aviation International nr 3, ZBiAM, Warszawa 2021.

[38] *Infauna (RB-531B) Russian 8x8 Amphibious Electronic Warfare System*, portal odin.tradoc.army.mil, https://odin.tradoc.army.mil/WEG/Asset/Infauna_(RB-531B)_Russian_8x8_Amphibious_Electronic_Warfare_System, [dostęp: 27.05.2025].

[39] *Leer-2 85Ya6*, portal armyrecognition.com, https://armyrecognition.com/military-products/army/electronic-warfare/tigr-m-mktk-rei-pp-leer-2-russia-uk, [dostęp: 27.05.2025].

- RP-377LA Lorandit – to system walki radioelektronicznej montowany na pojazdach opancerzonych, między innymi na BTR-80 lub MT-LB. Głównym zadaniem systemu jest zakłócanie sygnałów radiowych. Podczas wojny rosyjsko-ukraińskiej rozpoczętej w 2022 r. przez Federację Rosyjską, system ten stanowi jedno z głównych utrudnień dla Sił Zbrojnych Ukrainy [40].

Kompanie bezzałogowych statków powietrznych (BSP) Wojsk Powietrznodesantowych Federacji Rosyjskiej korzystają z różnych typów dronów rozpoznawczych i wsparcia radioelektronicznego, takich jak Orłan-10, Eleron-3, Tahin oraz Iskatiel. Orłan-10 to wielozadaniowy dron rozpoznawczy, zdolny do prowadzenia obserwacji w paśmie widzialnym i podczerwieni, a także do walki elektronicznej, w tym zakłócania łączności GSM i GPS oraz wspierania artylerii przez wskazywanie celów[41].

Przed wojną rosyjsko-ukraińską rozpoczętą przez Federację Rosyjską w 2022 r., rosyjskie Wojska Powietrznodesantowe posiadały łącznie około 1300 pływających bojowych wozów piechoty, w skład których wchodziły takie konstrukcje jak BMD-2, oraz BMD-4M (około 300 sztuk)[42].

Na początku 2022 r. struktura Sił Zbrojnych Federacji Rosyjskiej składała się hierarchicznie z Ministerstwa Obrony, poprzez Sztab Generalny, aż do poszczególnych rodzajów sił zbrojnych i samodzielnych rodzajów wojsk. Zasadniczo Siły Zbrojne Federacji Rosyjskiej składały się z trzech rodzajów sił zbrojnych: Wojsk Lądowych, Sił Powietrzno-Kosmicznych i Marynarki Wojennej, oraz dwóch samodzielnych rodzajów wojsk: Wojsk Rakietowych Strategicznego Przeznaczenia i Wojsk Powietrznodesantowych. W czasie pokoju wojsko rosyjskie zorganizowane było w pięć Okręgów Wojskowych, które odpowiedzialne są za szkolenie i rozwój. Ponadto Wojska Powietrznodesantowe, Strategiczne Siły Rakietowe, GRU oraz Specnaz. Okręgi przeznaczone były do operacji w Połączonych Dowództwach Strategicznych[43].

---

[40] M. Jabłoński, *Ten niepozorny wóz był utrapieniem Ukraińców. Rozerwali go jednym pociskiem*, portal geekweek.interia.pl, https://geekweek.interia.pl/militaria/news-ten-niepozorny-woz-byl-utrapieniem-ukraincow-rozerwali-go-je,nId,6840681, [dostęp: 27.05.2025].

[41] A. M. Maciejewski, *Bezzałogowiec Moskit, czyli Orłan-10 do walki radioelektronicznej [wideo]*, portal zbiam.pl, https://zbiam.pl/bezzalogowiec-moskit-czyli-orlan-10-do-walki-radioelektronicznej-wideo/, [dostęp: 27.05.2025].

[42] M. Szopa, *Armie Świata: Wojska Powietrznodesantowe…,* op. cit.

[43] M. Clark, K. Hird, *Russian regular ground forces order of battle*, ISW, Waszyngton 2023, s. 13.

Zaangażowanie i reorganizacja w działaniach zbrojnych przeciwko Ukrainie od 2022 r.

Przed pełnoskalową agresją Federacji Rosyjskiej na Ukrainę w 2022 r., w skład rosyjskich Wojsk Powietrznodesantowych wchodziły następujące jednostki i centra szkoleniowe:

- 98. Dywizja Powietrznodesantowa,
- 106. Dywizja Powietrznodesantowa,
- 7. Dywizja Desantowo-Szturmowa (górska),
- 76. Dywizja Desantowo-Szturmowa,
- 11. Samodzielna Brygada Desantowo-Szturmowa,
- 31. Samodzielna Brygada Desantowo-Szturmowa,
- 83. Samodzielna Brygada Desantowo-Szturmowa,
- 45. Samodzielna Brygada Specjalnego Przeznaczenia,
- 38.Samodzielna Brygada Dowodzenia,
- Szkoła WDW – Ujanów,
- Wyższa Szkoła Dowodzenia WDW – Riazań,
- 242. Centrum Szkolne WDW,
- 309. Centrum Szkolenia Spadochronowego WDW[44].

Wyposażenie Wojsk Powietrznodesantowych przed wojną wyglądało następująco:

- 3 bataliony czołgów (ok. 90 sztuk),
- blisko 1400 bojowych wozów desantowych,
- około 300 transporterów opancerzonych,
- około 360 haubic i moździerzy samobieżnych oraz holowanych[45].

Ponadto przed 24 lutego 2022 r. istniały plany rozbudowy Wojsk Powietrznodesantowych. Zakładano rozbudowę 31. Brygady Desantowo-Szturmowej w (piątą) 104. Dywizję Desantowo-Szturmową. Jej skład miał być analogiczny do już istniejących dywizji (zawierające po 3 pułki desantowo-szturmowe, mieszany desantowo-szturmowy i powietrznodesantowy komponent szczebla taktycznego). Kolejnym rozwiązaniem braku perspektyw

[44] T. Kwasek, *Rosyjskiej Wojska Powietrznodesantowe*, Nowa Technika Wojskowa, Numer Specjalny 15, Wojna rosyjsko-ukraińska (1), Warszawa 2023, s. 23-31.

[45] J. Ciślak, *Rosyjskie WDW bardziej szturmowe niż powietrznodesantowe [ANALIZA]*, portal defence24.pl, https://defence24.pl/sily-zbrojne/rosyjskie-wdw-bardziej-szturmowe-niz-powietrznodesantowe-analiza, [dostęp: 28.05.2025].

zwiększenia przepustowości lotnictwa transportowego miało być sformowanie brygady śmigłowców, zawierającej maszyny bojowe oraz transportowo-bojowe[46]. Przed rozpoczęciem wojny nie doszło do jej sformowania, zrealizowano ten plan latem 2023 r[47].

Pierwsze dwa dni wojny rosyjsko-ukraińskiej pokazały błędy Federacji Rosyjskiej, które przyniosły starty w maszynach, którymi również posługiwał się desant. Zestrzelono dwa samoloty transportowe Ił-76, którego ładunkiem mogli być żołnierze Wojsk Powietrznodesantowych lub zaopatrzenie[48].

Rosyjskie Wojska Powietrznodesantowe miały być kluczowym elementem w operacji desantu na lotnisko w Hostomelu w dniu 24 lutego 2022 r. Federacja Rosyjska określiła to lotnisko jako kluczowy element do szybkiego zdobycia stolicy Ukrainy – Kijowa. Zadanie zostało przydzielone siłom specjalnym z elitarnych Wojsk Powietrznodesantowych – 45. Samodzielnej Brygadzie Specjalnego Przeznaczenia. Desant miał liczyć około 200 żołnierzy wspieranych śmigłowcami szturmowymi Ka-52 oraz Mi-24/Mi-35M. Początkowo opanowano pas startowy i część lotniska, lecz silny i zorganizowany opór jednostek ukraińskich uniemożliwił pełne przejęcie terenu. Kontroli nad pasem nie utrzymano, ukraińska artyleria uszkodziła pas, co uniemożliwiło lądowanie samolotów. Ostatecznie walki w rejonie lotniska i pobliskiego miasta Hostomel trwały do początkowych dni kwietnia 2022 r. i zakończyły się wyparciem sił rosyjskich. Rosjanie, na podstawie nieudanej operacji przejęcia strategicznego lotniska, starali się stworzyć legendę „200 Spartan" broniących lotniska przed przeważającymi siłami wroga i zachodnimi najemnikami[49].

Do ataków na froncie kijowskim użyto elementów następujących zgrupowań Wojsk Powietrznodesantowych:

- 45. Samodzielnej Brygady Specjalnego Przeznaczenia,
- 31. Samodzielnej Brygady Desantowo-Szturmowej,
- 98. Dywizji Powietrznodesantowej (217. i 331. pułk),

---

[46] Ibidem.

[47] M. Boulègue, J. Bronk, K. Hird, J. Kerr, R. Lee, M. B. Petersen, *Assessing Russian plans for military regeneration. Modernization and reconstitution challenges for Moscow's war machine*, Chatham house, Londyn 2024, s. 9.

[48] B. Kucharski, *Rosyjskie straty na Ukrainie wg źródeł ukraińskich*, portal zbiam.pl, https://zbiam.pl/rosyjskie-straty-na-ukrainie-wg-zrodel-ukrainskich/, [dostęp: 23.05.2025].

[49] M. Gawęda, *Desant na Hostomel. Anatomia porażki Rosji [ANALIZA]*, portal defence24.pl, https://defence24.pl/sily-zbrojne/desant-na-hostomel-anatomia-porazki-rosji-analiza, [dostęp: 28.05.2025].

- 76. Dywizji Desantowo-Szturmowej (104. i 234. pułk),
- 106. Dywizji Powietrznodesantowej (137. pułk)[50].

Początkowe wykorzystywanie WDW niezgodnie z ich naturą – jako zwykłej piechoty – do szybkich rajdów oraz walk pozycyjnych w mieście, spowodowało szybkie wykrwawienie elitarnych jednostek rosyjskich. Niewątpliwie było to posunięcie błędne z taktycznego i strategicznego punktu widzenia. Ich lekki sprzęt, w tym wozy bojowe desantu i pojazdy opancerzone, okazały się nie być odporne na ukraiński ostrzał artyleryjski i broń przeciwpancerną. Dodatkowy brak ciężkiej artylerii jako wsparcia, ograniczał możliwości operacyjne tego rodzaju wojsk[51].

21 czerwca 2022 r. Ukraiński Sztab Generalny poinformował o problemach kadrowych rosyjskich jednostek powietrznodesantowych, które zmuszone były do rekrutacji oficerów rezerwy na trzymiesięczne kontrakty, z powodu znacznych strat wśród oficerów. BBC dodatkowo poinformowało, że Ministerstwo Obrony Federacji Rosyjskiej oferuje spłaty pożyczek i długów ochotników zaciągających się do armii[52].

W 321 dniu wojny (11 stycznia 2023 r.) Rosjanie za pomocą żołnierzy Wojsk Powietrznodesantowych i najemników Grupy Wagnera, opanowali Sołedar oraz wyszli na północ od Bachmutu. Działania te przecięły szlak komunikacyjny między Bachmutem a Siewierskiem oraz zagroziły odcięciem autostrady ze Słowiańskiem[53].

2 sierpnia 2023 r. generał pułkownik Michaił Teplinski potwierdził przekształcenie 31. Samodzielnej Brygady Desantowo-Szturmowej w 104. Dywizję Desantowo-Szturmową, która osiągnęła zamierzoną strukturę 26 września tego samego roku. Generał pułkownik zapowiedział również utworzenie dwóch nowych pułków – 299. i 119., mających podlegać pod odpowiednio 98. i 106. Dywizję Powietrznodesantową, zwiększając te dywizje do trzech pułków. Zakładano również pod koniec 2023 r. utworzenie 44. Dywizji

[50] Ibidem.

[51] M. Gawęda, *Rosyjski desant w wojnie z Ukrainą [ANALIZA]*, 16.04.2022, portal defence24.pl, https://defence24.pl/sily-zbrojne/rosyjski-desant-w-wojnie-z-ukraina-analiza, [dostęp: 28.05.2025].

[52] M. Clark, K. Stepanenko, G. Barros, G. Mappes, *Russian Offensive Campaign Assessment*, ISW, Waszyngton 2022, s. 2-3.

[53] A. Wilk, P. Żochowski (red.), *Rok wojny w analizach Ośrodka Studiów Wschodnich*, OSW, Warszawa 2023, s. 577.

Powietrznodesantowej, w którą miały wchodzić pułki strzeleckie, co czyniłoby tę dywizję Powietrznodesantową jedynie z nazwy[54].

15 lutego 2024 r. doszło do wycofania się pod rosyjskim ostrzałem sił ukraińskich z umocnionych pozycji na obrzeżach Awdijiwki. Dwa dni później padł oficjalny rozkaz opuszczenia miasta przez SZU. Rosjanie do 19 lutego 2024 r. opanowali całe miasto wraz z okolicami, wkroczyli również do Łastoczkyne, gdzie doszło do kolejnej wymiany ognia z wycofującymi się oddziałami ukraińskimi. Utrata z rąk ukraińskich miasta Awdijiwka stanowiła dużą stratę w obronie linii frontu, który był jednym z najlepiej ufortyfikowanych regionów. Upadek miasta naznaczony był zaciętymi walkami, w końcowej fazie natarcia rosyjskie środki powietrzne wraz z artylerią kierowały nawet 80 bomb dziennie. Zdobycie takiego kluczowego miejsca otwierało drogę Rosjanom do dalszych ofensyw na kierunku zachodnim[55]. W działaniach ofensywnych po stronie rosyjskiej brała udział 76. Dywizja Powietrznodesantowa[56].

Wiosna i lato 2024 r. to czas, kiedy WDW odegrało istotną rolę w skutecznych walkach o Casiw Jar. Jest to miejsce położone na wyżynie (lokalizacja pozwala na prowadzenie dalekiego rozpoznania) oraz punkt „kontrolny" do dalszego rosyjskiego natarcia na kierunkach Konstantynówka i aglomeracja Kramatorsk-Słowiańska. Główną siłą natarcia była 98. Dywizja Powietrznodesantowa, siłą trzech pułków (dodatkowo sformowany podczas wojny 299. pułk), wspierana między innymi piechotą morską (również elitarny rodzaj wojsk Federacji Rosyjskiej) oraz elementami 200. Brygady Zmechanizowanej i Ochotniczego Korpusu Ekspedycyjnego. Działania WDW charakteryzowały się użyciem małych grup szturmowych wspieranych przez artylerię (wnioski ze strat z początku agresji), drony oraz lotnictwo. Casiw Jar atakowano z trzech kierunków: północy, centralnie, południa[57].

---

[54] K. Hird, *Restructuring and Expansion of the Russian Ground Forces Hindered by Ukraine War Requirements*, ISW, Waszyngton 2023, s. 3-4.

[55] A. Wilk, P. Żochowski, J. Ber, *Drugi rok wojny w analizach Ośrodka Studiów Wschodnich*, OSW, Warszawa 2024, s. 572-574.

[56] P. Lewandowski, *Złe wiadomości z pól bitew w Ukrainie. Rosjanie wciąż w ofensywie [SYTUACJA NA FRONCIE]*, 20.02.2024, portal oko.press.pl, https://oko.press/rosjanie-wciaz-w-ofensywie-sytuacja-na-froncie, [dostęp: 28.05.2025].

[57] M. Gawęda, *W cieniu Charkowa. Rosyjski desant naciera na Czasiw Jar*, 18.05.2025, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/w-cieniu-charkowa-rosyjski-desant-naciera-na-czasiw-jar, [dostęp: 28.05.2025].

Mimo ciągłej ofensywy w 2025 r., przełamywanej na niektórych odcinakach frontu walką pozycyjną, wojska Federacji Rosyjskiej nadal są zdolne do dalszego prowadzenia działań. Charakter dowodzenia, który nie skupia się na oszczędzaniu podwładnych, tylko na osiąganiu konkretnych celów i stałym uzupełnianiu braków kadrowych, czyni armię groźnym przeciwnikiem. Postępujące wykluczenia gospodarcze ze strony państw zachodnich, mimo zamykania kluczowych kanałów finansowania rosyjskiej agresji, dają szeroką możliwość prowadzenia działań hybrydowych, wymierzonych w jedność Unii Europejskiej oraz NATO[58].

Od końca maja 2025 r. Federacja Rosyjska gromadzi swoje siły w rejonie Charkowa. Eksperci, analitycy wojskowi zaznaczają obecność Wojsk Powietrznodesantowych. Może to świadczyć o wykorzystaniu najbardziej doświadczonych jednostek Sił Zbrojnych FR do kolejnych działań ofensywnych, a nawet do próby zdobycia miasta, które jest kluczowym punktem obrony – niejako „twierdzą" Ukrainy. Warto zaznaczyć również ogólną sytuację na froncie ukraińskim, gdzie Federacja Rosyjska „zmęczona" trzyletnią wojną, którą rozpoczęła – nie dysponuje już takim dużym zapleczem, by przeprowadzić dużą operację ofensywną. Eksperci wskazują na większe prawdopodobieństwo stopniowego wzrostu przeprowadzanych ataków, niż manewrowania dużymi jednostkami[59].

Podsumowanie

Kilkudziesięcioletnie tradycje Wojsk Powietrznodesantowych Federacji Rosyjskiej, które za kilka lat będą miały sto lat tradycji, pokazują znaczenie tego rodzaju wojsk na polu walki, mimo zmieniających się uwarunkowań prowadzonych działań zbrojnych. Należy tu wskazać, że ten rodzaj sił zbrojnych jest jednym z bardziej skomplikowanych w utrzymaniu, a szczególnie w wyszkoleniu żołnierzy i posiadaniu dużej ilości środków ich transportu. To warunkuje, że nie wszystkie armie świata są w stanie posiadać i utrzymywać dużą ilość jednostek powietrznodesantowych. Federacja Rosyjska

[58] J. Starosta, *Co czeka Rosję w 2025 roku?*, 02.02.2025, portal ine.org.pl, https://ine.org.pl/co-czeka-rosje-w-2025-roku/, [dostęp: 23.05.2025].

[59] R. Strzelec, *Rosja gromadzi siły. Eksperci mówią, co to oznacza*, portal o2.pl, https://www.o2.pl/informacje/rosja-gromadzi-sily-eksperci-mowia-co-to-oznacza-7160863787645920a, [dostęp: 27.05.2025].

w ograniczony sposób dokonała redukcji oddziedziczonych jednostek wojskowych, komasując jej najlepszy personel w zachowanych strukturach.

Mimo wyposażenia w sprzęt zmechanizowany, jednostki Wojsk Powietrznodesantowych są pododdziałami mającymi ograniczone możliwości użycia ciężkiego uzbrojenia i sprzętu, co wskazuje na ich specyficzne działanie, zakładające użycie tych wojsk do szybkich rajdów bojowych w ograniczonym czasie. W przypadku działań połączonych Wojsk Powietrznodesantowych z Wojskami Lądowymi, sukces jest możliwy, a w wypadku braku takiej koordynacji należy liczyć się z wysokimi stratami wśród żołnierzy desantu. Przykładem tego jest porażka desantu śmigłowcowego Wojsk Powietrznodesantowych na początku wojny rosyjsko-ukraińskiej, na lotnisku w Hostomelu. Żołnierze Wojsk Powietrznodesantowych są w grupie elitarnych wojsk tego rodzaju, wykorzystywanych w walkach, co pokazuje, jak groźny jest to komponent Sił Zbrojnych Federacji Rosyjskiej.

Literatura

1. Boulègue M., Bronk J., Hird K., Kerr J., Lee R., Petersen M. B., *Assessing Russian plans for military regeneration. Modernization and reconstitution challenges for Moscow's war machine*, Chatham house, Londyn 2024.
2. Butowski P., *Iljuszyn Il-76*, Lotnictwo Aviation International nr 3, ZBiAM, Warszawa 2021.
3. Butowski P., *Kamow Ka-52 Aligator*, Lotnictwo Aviation International nr 12, ZBiAM, Warszawa 2019.
4. Butowski P., *Śmigłowiec szturmowy Mil Mi-28N Nocny Myśliwy*, Lotnictwo Aviation International nr 11, ZBiAM, Warszawa 2019.
5. Charuk A., *Rosyjska egzotyka - rzadkie pojazdy opancerzone na wojnie z Ukrainą*, Nowa Technika Wojskowa nr 5, Magnum-X, Warszawa 2023.
6. Ciechanowski R., *Wojska Powietrznodesantowe – modernizacja techniczna w latach 2008-2017*, Nowa Technika Wojskowa, Numer Specjalny nr 14, Magnum-X, Warszawa 2018.
7. Clark M., Hird K., *Russian regular ground forces order of battle*, ISW, Waszyngton 2023.
8. Clark M., Stepanenko K., Barros G., Mappes G., *Russian Offensive Campaign Assessment*, ISW, Waszyngton 2022.
9. Depczyński M., *Zmiany w rosyjskich Wojskach Powietrznodesantowych*, Nowa Technika Wojskowa nr 3, Magnum-X, Warszawa 2021.
10. Dyner A. M., *Rosyjskie ćwiczenia wojskowe - przesłanie dla przeciwników i sojuszników*, Biuletyn PISM, nr 90 (1202), 1-2, Warszawa 2014.
11. Elfving J., *An Assessment of the Russian Airborne Troops and Their Role on Tomorrow's Battlefield*, The Jamestown foundation, Waszyngton 2021.

12. Grabowski T. W., *Rosyjska Siła. Siły Zbrojne i główne problemy polityki obronnej Federacji Rosyjskiej w latach 1991-2010*, Instytut Geopolityki, Częstochowa 2011.
13. Hird K., *Restructuring and Expansion of the Russian Ground Forces Hindered by Ukraine War Requirements*, ISW, Waszyngton 2023.
14. Jastrzębski M., *Zmiany struktur organizacyjnych i wzrost potencjału Wojsk Lądowych Federacji Rosyjskiej po reformach 2009 roku*, [w:] Prusak R., Kardas E. (red.), *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, Wydawnictwo Uniwersytetu Kazimierza Wielkiego, Bydgoszcz 2016.
15. Kwasek T., *Rosyjskiej Wojska Powietrznodesantowe*, Nowa Technika Wojskowa Numer Specjalny 15, Wojna rosyjsko-ukraińska (1), Magnum-X, Warszawa 2023.
16. Oszczęda A., *Perspektywy rozwoju i modernizacja SM FR w aspekcie „arktycznego" wyścigu zbrojeń*, Rocznik bezpieczeństwa morskiego nr 11, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, Gdynia 2017.
17. Przeździecki P., *Czołg podstawowy T-72B3*, Wojsko i Technika nr 8, ZBiAM, Warszawa 2017.
18. Suworow W., *Specnaz. Historia sił specjalnych armii radzieckiej*, Rebis, Poznań 2011.
19. Topolski I., *Manewry wojskowe jako forma demonstracji siły militarnej Federacji Rosyjskiej w Europie*, Wschód Europy. Studia humanistyczno-społeczne 5, nr 1 (2019), Wydawnictwo UMCS, Lublin 2019.
20. Wilk A., *Rosyjska armia białoruska. Praktyczne aspekty integracji wojskowej Białorusi i Rosji. Raport OSW*, Ośrodek Studiów Wschodnich im. Marka Karpia, Warszawa 2021.
21. Wilk A., Żochowski P. (red.), *Rok wojny w analizach Ośrodka Studiów Wschodnich*, OSW, Warszawa 2023.
22. Wilk A., Żochowski P., Ber J., *Drugi rok wojny w analizach Ośrodka Studiów Wschodnich*, OSW, Warszawa 2024.

Netografia

1. *American and Russian soldiers pass out flyers to the citizens of Kamenica, Kosovo*., portal defense.gov, https://www.defense.gov/Multimedia/Photos/igphoto/2002018201/.
2. *BMD-2*, portal opisybroni.pl, https://opisybroni.pl/bmd-2/.
3. *BTR-82A BTR-82AM*, 02.01.2025, portal armyrecognition.com, https://armyrecognition.com/military-products/army/armoured-personnel-carriers/wheeled-vehicles/btr-82a-russia-uk.
4. *BTR-D*, portal opisybroni.pl, https://opisybroni.pl/btr-d/.
5. Ciślak J., *Rosyjskie WDW bardziej szturmowe niż powietrznodesantowe [ANALIZA]*, 21.10.2023, portal defence24.pl, https://defence24.pl/sily-zbrojne/rosyjskie-wdw-bardziej-szturmowe-niz-powietrznodesantowe-analiza.
6. Gawęda M., *Desant na Hostomel. Anatomia porażki Rosji [ANALIZA]*, 15.08.2022, portal defence24.pl, https://defence24.pl/sily-zbrojne/desant-na-hostomel-anatomia-porazki-rosji-analiza.

7. Gawęda M., *Rosyjski desant w wojnie z Ukrainą [ANALIZA]*, 16.04.2022, portal defence24.pl, https://defence24.pl/sily-zbrojne/rosyjski-desant-w-wojnie-z-ukraina-analiza.
8. Gawęda M., *W cieniu Charkowa. Rosyjski desant naciera na Czasiw Jar*, 18.05.2025, portal defence24.pl, https://defence24.pl/wojna-na-ukrainie-raport-specjalny-defence24/w-cieniu-charkowa-rosyjski-desant-naciera-na-czasiw-jar.
9. *IFOR*, portal wojsko-polskie.pl, https://www.wojsko-polskie.pl/ifor-bih/.
10. *Infauna (RB-531B) Russian 8x8 Amphibious Electronic Warfare System*, 12.05.2025, portal odin.tradoc.army.mil, https://odin.tradoc.army.mil/WEG/Asset/Infauna_(RB-531B)_Russian_8x8_Amphibious_Electronic_Warfare_System.
11. Jabłoński M., *Ten niepozorny wóz był utrapieniem Ukraińców. Rozerwali go jednym pociskiem*, 14.06.2023, portal geekweek.interia.pl, https://geekweek.interia.pl/militaria/news-ten-niepozorny-woz-byl-utrapieniem-ukraincow-rozerwali-go-je,nId,6840681.
12. Kipp J. W., *US-Russian Military Cooperation and the IFOR Experience: A Comparison of Survey Results*, portal bits.de, https://www.bits.de/NRANEU/docs/Kipp98.htm.
13. Kucharski B., *Rosyjskie straty na Ukrainie wg źródeł ukraińskich*, 26.02.2022, portal zbiam.pl, https://zbiam.pl/rosyjskie-straty-na-ukrainie-wg-zrodel-ukrainskich/.
14. *Leer-2 85Ya6*, 18.07.2024, portal armyrecognition.com, https://armyrecognition.com/military-products/army/electronic-warfare/tigr-m-mktk-rei-pp-leer-2-russia-uk.
15. Lewandowski P., *Złe wiadomości z pól bitew w Ukrainie. Rosjanie wciąż w ofensywie [SYTUACJA NA FRONCIE]*, 20.02.2024, portal OKO.press, https://oko.press/rosjanie-wciaz-w-ofensywie-sytuacja-na-froncie.
16. Maciejewski A. M., *Bezzałogowiec Moskit, czyli Orłan-10 do walki radioelektronicznej [wideo]*, 10.12.2022, portal zbiam.pl, https://zbiam.pl/bezzalogowiec-moskit-czyli-orlan-10-do-walki-radioelektronicznej-wideo/.
17. *Naddniestrze. V kolumna Rosji na zapleczu frontu [Armie Świata odc. 59]*, Defence24, 11.01.2023, portal youtube.com, https://www.youtube.com/watch?v=rfcQ9f7d5Mo.
18. Michalik Ł., *Rosyjski sposób na drony. Chcą użyć 100-mm armat z pojazdów BMD-4*, 15.04.2025, portal tech.wp.pl, https://tech.wp.pl/rosyjski-sposob-na-drony-chca-uzyc-100-mm-armat-z-pojazdow-bmd-4,7146831019465248a.
19. *NATO and Russia: Partners in Peacekeeping*, portal nato.int, https://www.nato.int/docu/presskit/010219/brocheng.pdf.
20. *Siły dla Kosowa, KFOR ONZ*, portal wojsko-polskie.pl, https://www.wojsko-polskie.pl/kfor-kosowo/.
21. *Siły Stabilizacyjne NATO SFOR*, portal wojsko-polskie.pl, https://www.wojsko-polskie.pl/sfor-bih/.
22. Starosta J., *Co czeka Rosję w 2025 roku?*, 02.02.2025, portal ine.org.pl, https://ine.org.pl/co-czeka-rosje-w-2025-roku/.
23. Strzelec R., *Rosja gromadzi siły. Eksperci mówią, co to oznacza*, 26.05.2025, portal o2.pl, https://www.o2.pl/informacje/rosja-gromadzi-sily-eksperci-mowia-co-to-oznacza-7160863787645920a.

24. Szopa M., *Armie Świata: Wojska Powietrznodesantowe Rosji (WDW)*, 01.04.2022, portal defence24.pl, https://defence24.pl/sily-zbrojne/armie-swiata-wojska-powietrznodesantowe-rosji-wdw.
25. Świerkowski A., *Armia 2023: Pancerny Tigr rodem z Mad Maxa*, 22.08.2023, portal defence23.pl, https://defence24.pl/przemysl/armia-2023-pancerny-tigr-rodem-z-mad-maxa.

dr Marek Ciekanowski
Społeczna Akademia Nauk w Warszawie
ORCID: 0009-0009-1271-0652

dr inż. Marta Chodyka
Akademia Bialska im. Jana Pawła II
ORCID: 0000-0002-8819-2451

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

mgr Weronika Parczewska
Wojskowa Akademia Techniczna w Warszawie
ORCID: 0000-0001-8991-4068

https://doi.org/10.29316/9788368103205_8

BEZPIECZEŃSTWO TELEINFORMATYCZNE W ZARZĄDZANIU KRYZYSOWYM

ICT SECURITY IN CRISIS MANAGEMENT

Streszczenie

Celem rozdziału jest analiza znaczenia bezpieczeństwa systemów teleinformatycznych w zarządzaniu kryzysowym oraz identyfikacja głównych zagrożeń i skutecznych strategii ochrony. W pierwszej części rozdziału opisano rolę systemów teleinformatycznych w zarządzaniu kryzysowym, podkreślając ich znaczenie dla komunikacji, analizy danych i podejmowania decyzji. Druga część przedstawia główne zagrożenia i wyzwania,

Summary

The aim of the chapter is to analyze the importance of ICT systems security in crisis management and to identify the main threats and effective protection strategies. The first part of the chapter describes the role of ICT systems in crisis management, emphasizing their importance for communication, data analysis and decision-making. The second part presents the main threats and challenges, such as cyberattacks, technical failures and

takie jak cyberataki, awarie techniczne i dezinformacja. Trzecia część koncentruje się na najlepszych praktykach i strategiach zabezpieczeń, wskazując na znaczenie szyfrowania danych, systemów wykrywania zagrożeń, redundancji infrastruktury oraz szkoleń personelu. Problem badawczy sformułowano: Jakie są kluczowe zagrożenia dla systemów teleinformatycznych w zarządzaniu kryzysowym i jakie środki mogą zwiększyć ich odporność? W badaniu wykorzystano metody teoretyczne, takie jak analiza literatury naukowej, przegląd norm i regulacji dotyczących cyberbezpieczeństwa oraz studia przypadków dotyczące incydentów naruszenia bezpieczeństwa systemów teleinformatycznych w zarządzaniu kryzysowym.

Słowa kluczowe: zarządzanie kryzysowe, bezpieczeństwo teleinformatyczne, cyberzagrożenia, strategie ochrony

disinformation. The third part focuses on security best practices and strategies, highlighting the importance of data encryption, threat detection systems, infrastructure redundancy, and staff training. The research problem was formulated: What are the key threats to ICT systems in crisis management and what measures can increase their resilience? The study used theoretical methods such as an analysis of the scientific literature, a review of cybersecurity standards and regulations, and case studies on ICT security incidents in crisis management.

Keywords: crisis management, ICT security, cyber threats, protection strategies

Wstęp

Współczesne zarządzanie kryzysowe w dużym stopniu opiera się na wykorzystaniu nowoczesnych systemów teleinformatycznych, które umożliwiają sprawną komunikację, gromadzenie i analizę danych oraz podejmowanie szybkich decyzji w sytuacjach zagrożenia. Od niezawodności i bezpieczeństwa tych systemów zależy skuteczność działań podejmowanych przez służby ratunkowe, administrację publiczną oraz inne podmioty odpowiedzialne za minimalizowanie skutków katastrof i kryzysów.

Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym obejmuje szeroki zakres zagadnień, w tym ochronę przed cyberatakami, odporność na awarie techniczne, zapewnienie ciągłości działania oraz zabezpieczenie integralności i poufności informacji. W dobie rosnących zagrożeń cybernetycznych oraz coraz większej zależności od technologii cyfrowych, kluczowe staje się opracowanie skutecznych strategii i narzędzi zapewniających bezpieczeństwo infrastruktur krytycznych oraz systemów wspomagających podejmowanie decyzji.

Celem niniejszego rozdziału jest analiza kluczowych aspektów związanych z bezpieczeństwem systemów teleinformatycznych w kontekście zarządzania kryzysowego. Przedstawione zostaną zagrożenia, wyzwania oraz najlepsze praktyki w zakresie ochrony tych systemów, ze szczególnym uwzględnieniem technologii wykorzystywanych w instytucjach odpowiedzialnych za reagowanie na sytuacje kryzysowe.

Zagrożenia i wyzwania dla bezpieczeństwa systemów teleinformatycznych

Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym wiąże się z wieloma zagrożeniami, które mogą znacząco wpłynąć na ich funkcjonowanie i skuteczność podejmowanych działań. Jednym z kluczowych zagrożeń są cyberataki, obejmujące m.in. ataki typu DDoS (Distributed Denial of Service), próby przejęcia kontroli nad systemami, złośliwe oprogramowanie oraz phishing skierowany do pracowników instytucji zarządzających kryzysowo. Ataki te mogą prowadzić do zakłócenia działania systemów, wycieku poufnych informacji, a nawet przejęcia infrastruktury przez podmioty nieuprawnione[1]. Ataki DDoS wykorzystują słabość architektury TCP/IP oraz serwerów DNS umożliwiającą przeciążenie zasobów systemowych sztucznie wygenerowanym ruchem sieciowym[2]. Przeprowadzenie tego typu ataku wymaga zaangażowania znacznych zasobów sprzętowych. Jako że mało kto dysponuje własnym rozbudowanym centrum obsługi danych, osoby przeprowadzające ataki DDoS wykorzystują w tym celu systemy komputerowe, nad którymi przejmują kontrolę za pomocą szkodliwego oprogramowania[3].

Phishing również stanowi jedno z najpoważniejszych zagrożeń dla systemów teleinformatycznych[4], a jego wpływ na zarządzanie kryzysowe może być katastrofalny. Ataki phishingowe, polegające na podszywaniu się pod

[1] E. Niewiadomska-Szynkiewicz, R. Litka, *Ataki na urządzenia mobilne i metody ich wykrywania*, Cybersecurity and Law, nr 1(9), 2023, s. 91.

[2] Ł. Apiecionek, *Fuzzy Observation of DDoS Attack,* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor* , W. Kosiński, P. Prokopowicz, J. Czerniak, D. Mikołajewski, Ł. Apiecionek, D. Slezak, Bydgoszcz 2017, s. 240.

[3] I. Protasowicki, *Wpływ zagrożenia atakami DOS/DDOS na bezpieczeństwo teleinformatycznej infrastruktury krytycznej*, Modern Management Review, vol. XXIII, 25 (1/2018), 2018, s. 134.

[4] S. Grzebielec, *Analiza podatności użytkowników systemów informatycznych na atak phishingowy*, Journal of Computer Sciences Institute, vol. 15, 2020, s. 164.

zaufane instytucje lub osoby w celu wyłudzenia danych uwierzytelniających, mogą prowadzić do przejęcia kontroli nad systemami, wycieku poufnych informacji oraz zakłócenia koordynacji działań w sytuacjach kryzysowych. Ataki phishingowe często prowadzą do przejęcia danych logowania do systemów zarządzania kryzysowego. Cyberprzestępcy mogą w ten sposób uzyskać dostęp do baz danych, narzędzi monitorujących czy systemów komunikacyjnych wykorzystywanych przez służby ratunkowe. W efekcie może dojść do paraliżu operacyjnego, opóźnień w reakcji na zagrożenia oraz dezinformacji, co zwiększa ryzyko strat ludzkich i materialnych. Phishing może być wykorzystywany do rozpowszechniania fałszywych informacji w celu wywołania paniki lub skierowania działań kryzysowych w niewłaściwym kierunku. Atakujący, przejmując dostęp do oficjalnych kanałów komunikacyjnych, mogą rozsyłać fałszywe ostrzeżenia, podawać błędne instrukcje lub publikować zmanipulowane dane, co prowadzi do chaosu i dezinformacji wśród ludności oraz służb ratunkowych.

Systemy teleinformatyczne w zarządzaniu kryzysowym przechowują wrażliwe informacje, takie jak plany ewakuacyjne, dane osobowe ofiar, szczegóły dotyczące zagrożeń czy taktyki działań ratowniczych. Phishing umożliwia cyberprzestępcom uzyskanie dostępu do tych informacji i ich nieautoryzowane wykorzystanie, co może skutkować szantażem, sprzedażą danych lub wykorzystaniem ich do dalszych ataków na infrastrukturę krytyczną.

Ataki phishingowe mogą również wpływać na łańcuchy dostaw i logistykę w zarządzaniu kryzysowym. Oszuści mogą podszywać się pod dostawców sprzętu medycznego, organizacje humanitarne czy instytucje rządowe, wprowadzając fałszywe zamówienia, przekierowując zasoby w niewłaściwe miejsca lub manipulując procesami zaopatrzenia. Takie działania prowadzą do opóźnień w dostarczaniu niezbędnej pomocy i osłabiają skuteczność operacji kryzysowych.

Kolejnym wyzwaniem są awarie techniczne[5], które mogą wynikać zarówno z błędów w oprogramowaniu, jak i problemów sprzętowych. Wysoka niezawodność systemów teleinformatycznych jest kluczowa, zwłaszcza w sytuacjach kryzysowych, gdzie każda przerwa w dostępie do informacji może prowadzić do opóźnień w reagowaniu i zwiększenia strat. W szczegól-

[5] M. Elszkowski, *Działalność Policji w sytuacjach kryzysowych. Podejście formalne*, Zeszyty Naukowe SGSP, Nr 61(2), 2017, s. 95.

ności zagrożeniem są awarie sieci telekomunikacyjnych, utrata zasilania oraz uszkodzenia infrastruktury IT na skutek klęsk żywiołowych, aktów sabotażu lub błędów ludzkich[6].

Dodatkowym ryzykiem jest manipulacja danymi oraz dezinformacja, które mogą prowadzić do podejmowania błędnych decyzji w sytuacjach kryzysowych[7]. Ataki na integralność danych, np. fałszowanie informacji dotyczących zagrożeń, mogą skutkować nieprawidłowym rozmieszczeniem zasobów i opóźnieniem działań ratunkowych.

Dezinformacja stanowi jedno z najpoważniejszych wyzwań w zarządzaniu kryzysowym, wpływając na procesy decyzyjne, reakcję społeczeństwa oraz skuteczność działań instytucji odpowiedzialnych za bezpieczeństwo i porządek publiczny. W dobie powszechnego dostępu do informacji i mediów społecznościowych dezinformacja może szybko eskalować, prowadząc do chaosu, paniki oraz podważania zaufania do organów państwowych. Dezinformacja w zarządzaniu kryzysowym może pochodzić z różnych źródeł, w tym:

- aktorów państwowych prowadzących działania hybrydowe,
- grup ekstremistycznych i terrorystycznych,
- osób prywatnych, które nieświadomie rozpowszechniają fałszywe informacje,
- mediów społecznościowych, które ułatwiają szybkie rozprzestrzenianie się fake newsów.

Dezinformacja stanowi istotne zagrożenie w zarządzaniu kryzysowym, mogąc prowadzić do chaosu i utraty zaufania do instytucji publicznych. Kluczowe znaczenie mają skuteczne strategie komunikacyjne, monitorowanie źródeł dezinformacji oraz edukacja społeczeństwa, które mogą ograniczyć negatywne skutki manipulacji informacyjnej w sytuacjach kryzysowych. Dezinformacja może znacząco utrudnić skuteczne zarządzanie kryzysowe, prowadząc do:

- opóźnień w podejmowaniu decyzji,
- spadku zaufania do instytucji publicznych,
- rozprzestrzeniania się paniki i chaosu społecznego,
- błędnych alokacji zasobów, gdy służby reagują na fałszywe informacje.

[6] M. Witkowski, *Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym*, Zeszyty Naukowe WSOWL, nr 4(162), 2011, s. 83.

[7] J. Pyka, *Komunikacja w zarządzaniu kryzysowym – problemy i wyzwania*, Zeszyty Naukowe Akademii Górnośląskiej, Nr 7, 2023, s. 127.

Klasyczne reakcje systemów zabezpieczeń w produkcyjnych systemach teleinformatycznych zmierzają do jak najszybszego zablokowania możliwości oddziaływania zdalnego napastnika na atakowane zasoby[8]. Rosnąca liczba zagrożeń cybernetycznych oraz rosnąca zależność od technologii cyfrowych sprawiają, że kluczowe staje się wdrażanie skutecznych środków ochrony. Niezbędne są zaawansowane systemy monitorowania, wykrywania zagrożeń, mechanizmy redundancji infrastruktury oraz procedury zapewniające ciągłość działania. Odpowiednia polityka bezpieczeństwa i szkolenie personelu to kolejne istotne elementy minimalizowania ryzyka w zarządzaniu kryzysowym.

Rola systemów teleinformatycznych w zarządzaniu kryzysowym

Współczesne zarządzanie kryzysowe w dużym stopniu opiera się na zaawansowanych systemach teleinformatycznych, które odgrywają kluczową rolę w zapewnieniu sprawnej komunikacji, gromadzenia i analizy danych oraz podejmowania szybkich i trafnych decyzji w sytuacjach nadzwyczajnych. Systemy te umożliwiają integrację informacji z różnych źródeł, co pozwala na kompleksową ocenę zagrożeń i skuteczniejsze zarządzanie zasobami.

Jednym z podstawowych zadań systemów teleinformatycznych jest zapewnienie niezawodnej komunikacji między służbami ratunkowymi, administracją publiczną oraz innymi podmiotami zaangażowanymi w działania kryzysowe. Dzięki nowoczesnym technologiom, takim jak sieci radiowe, systemy łączności satelitarnej czy platformy wymiany danych w czasie rzeczywistym, możliwe jest szybkie przekazywanie kluczowych informacji oraz koordynacja działań w terenie. Na rysunku poniżej przedstawiono sieci i systemy teleinformatyczne wykorzystywane na potrzeby systemu kierowania bezpieczeństwem państwa.

[8] A. Patkowski, *„Cicha reakcja" na zdalne ataki teleinformatyczne*, Przegląd Teleinformatyczny, T. 5, nr 3(44), 2017, s. 38.

Rysunek 1. Sieci i systemy teleinformatyczne wykorzystywane na potrzeby systemu kierowania bezpieczeństwem państwa

Źródło: G. Michalewski, M. Witkowski, R*ola sieci i systemów teleinformatycznych w procesie podejmowania decyzji w sytuacjach kryzysowych*, Rocznik Kolegium Analiz Ekonomicznych, nr 49, 2018, s. 325.

Ponadto systemy teleinformatyczne wspomagają proces decyzyjny poprzez analizę dużych zbiorów danych, prognozowanie zagrożeń oraz modelowanie scenariuszy kryzysowych. Narzędzia oparte na sztucznej inteligencji i analizie Big Data pozwalają na skuteczniejsze przewidywanie sytuacji kryzysowych, co umożliwia odpowiednie przygotowanie i minimalizację strat. Właściwie zaprojektowany i funkcjonujący system obiegu informacji w procesie podejmowania decyzji w sytuacjach kryzysowych powinien pozwalać na:

- monitorowanie sytuacji bezpieczeństwa;
- ostrzeganie (system alarmowania i ostrzegania) – prognozowanie zagrożeń i rozwoju sytuacji,
- podejmowanie decyzji,
- opracowanie niezbędnych dokumentów (plany działania, rozkazu, dyrektywy),
- reagowanie na sytuacje kryzysowe (wypadki, siły szybkiego reagowania (QRF) itp.),
- podejmowanie działań (ratowniczych itp.),
- wprowadzanie korekt w działaniu (decyzjach),
- aktualizację i modyfikację planów,
- modyfikację procedur (system „Lessons Learned”14),

- bieżące zaspokajanie potrzeb materiałowych i zasobowych (logistyka), w celu utrzymywania żywotności i gotowości elementów wykonawczych systemu bezpieczeństwa do działania[9].

Współczesne zarządzanie kryzysowe opiera się na skutecznej koordynacji działań wielu podmiotów, takich jak administracja publiczna, służby ratownicze oraz siły zbrojne. Kluczową rolę w tym procesie odgrywają zaawansowane systemy teleinformatyczne, które umożliwiają sprawną wymianę informacji, monitorowanie sytuacji w czasie rzeczywistym oraz podejmowanie szybkich i trafnych decyzji.

Jednym z przykładów systemów wspierających zarządzanie kryzysowe jest system Jaśmin, który znajduje zastosowanie zarówno w działaniach wojskowych, jak i cywilnych.

Systemy teleinformatyczne pozwalają na szybkie przekazywanie informacji pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo, co umożliwia skuteczne reagowanie na sytuacje kryzysowe. Dzięki zdolności do przetwarzania ogromnych ilości danych w czasie rzeczywistym, wspierają one analizę zagrożeń oraz przewidywanie ich potencjalnych skutków. Narzędzia te pozwalają na monitorowanie kluczowych zasobów, takich jak pojazdy ratownicze, sprzęt czy infrastruktura krytyczna, co znacząco usprawnia zarządzanie operacyjne w trakcie sytuacji nadzwyczajnych.

System Jaśmin został opracowany jako kompleksowe rozwiązanie teleinformatyczne, które integruje dane z różnych źródeł i umożliwia ich wizualizację na interaktywnych mapach. Jego zastosowanie obejmuje zarówno działania wojskowe, jak i cywilne operacje ratunkowe, w tym zarządzanie klęskami żywiołowymi czy zagrożeniami terrorystycznymi. Wykorzystanie systemu pozwala na lepsze planowanie i realizację operacji dzięki zaawansowanym narzędziom do analizy danych i zarządzania logistyką[10]. Na poniższym rysunku przedstawiono struktury zarządzania kryzysowego w systemie Jaśmin.

[9] G. Michalewski, M. Witkowski, *Rola sieci i systemów teleinformatycznych w procesie podejmowania decyzji w sytuacjach kryzysowych*, Rocznik Kolegium Analiz Ekonomicznych, nr 49, 2018, s. 323.

[10] SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego – TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html, [dostęp: 26.03.2025].

Rysunek 2. SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego

Źródło: SZK JAŚMIN – Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego – TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html, [dostęp: 26.03.2025].

Podczas katastrof naturalnych system Jaśmin wspierał działania służb ratowniczych, umożliwiając efektywne monitorowanie rozwoju sytuacji i koordynację pracy zespołów w terenie. W przypadku zagrożeń terrorystycznych pozwalał na szybką identyfikację ryzyka oraz organizację działań prewencyjnych[11]. Jego zastosowanie w operacjach wojskowych potwierdziło skuteczność w zakresie dowodzenia i zarządzania zasobami, co czyni go istotnym narzędziem także w ramach współpracy międzynarodowej, na przykład w strukturach NATO[12].

Systemy teleinformatyczne, takie jak Jaśmin, znacząco zwiększają efektywność zarządzania kryzysowego, pozwalając na skuteczniejsze reagowanie na sytuacje nadzwyczajne. Dzięki zdolności do integracji danych, monitorowania sytuacji w czasie rzeczywistym oraz wspomagania podejmowania decyzji, ich rola w zapewnianiu bezpieczeństwa publicznego jest nie do przecenienia. Dynamiczny rozwój technologii teleinformatycznych wskazuje na to, że w przyszłości ich zastosowanie w zarządzaniu kryzysowym będzie

[11] System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych, https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i--wsparciu-akcji-antykryzysowych, [dostęp: 26.03.2025].

[12] NATO CWIX 2023 – kolejny sukces systemu JAŚMIN, https://zbiam.pl/nato-cwix-2023-kolejny-sukces-systemu-jasmin/, [dostęp: 26.03.2025].

jeszcze szersze, co wpłynie na dalszą poprawę skuteczności działań ratowniczych i operacyjnych.

Niezawodność i efektywność systemów teleinformatycznych mają zatem kluczowe znaczenie dla skutecznego zarządzania kryzysowego. Ich rozwój i doskonalenie stanowią istotny element polityki bezpieczeństwa, ponieważ w sytuacjach zagrożenia każda sekunda ma znaczenie, a sprawny przepływ informacji może decydować o powodzeniu działań ratunkowych i ochronie ludności.

Najlepsze praktyki i strategie zabezpieczeń

W celu zwiększenia odporności systemów teleinformatycznych na zagrożenia kluczowe jest wdrażanie nowoczesnych metod ochrony, które minimalizują ryzyko cyberataków, awarii oraz utraty integralności danych. Jednym z podstawowych środków zabezpieczeń jest szyfrowanie danych, które zapewnia poufność informacji i chroni je przed nieautoryzowanym dostępem. Stosowanie silnych algorytmów kryptograficznych w komunikacji i przechowywaniu danych znacząco utrudnia przechwycenie lub manipulację informacjami.

Kolejnym istotnym elementem ochrony są systemy wykrywania i zapobiegania zagrożeniom (IDS/IPS – Intrusion Detection/Prevention Systems), które monitorują ruch sieciowy i automatycznie reagują na podejrzane aktywności[13]. W połączeniu z analizą behawioralną i sztuczną inteligencją systemy te pozwalają na wczesne wykrywanie ataków oraz podejmowanie działań zapobiegawczych.

Strategie zabezpieczeń w kontekście sztucznej inteligencji (AI) w zarządzaniu kryzysowym odgrywają kluczową rolę w zapewnieniu bezpieczeństwa zarówno samych systemów teleinformatycznych, jak i danych, które są zbierane i przetwarzane w czasie rzeczywistym. W przypadku kryzysów, szczególnie takich o charakterze międzynarodowym, terrorystycznym czy związanym z katastrofami naturalnymi, informacje przekazywane między służbami ratunkowymi, administracją publiczną i obywatelami muszą być nie tylko dokładne, ale również chronione przed nieautoryzowanym dostępem, manipulacjami czy atakami cybernetycznymi.

[13] M. Wrzesień, Ł. Olejnik, P. Ryszawa, *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, Studia i Materiały Informatyki Stosowanej, nr 7, 2012, s. 166.

Pierwszym aspektem strategii zabezpieczeń jest zapewnienie integralności danych. W sytuacjach kryzysowych, gdzie dane pochodzą z różnych źródeł – takich jak drony, czujniki, media społecznościowe, czy systemy monitoringu – istotne jest, aby były one wiarygodne i nie zostały zmienione. AI odgrywa tutaj rolę w szyfrowaniu przesyłanych informacji, stosowaniu metod detekcji anomalii w danych oraz weryfikacji ich autentyczności[14]. Zabezpieczenie tych informacji przed złośliwymi atakami czy manipulacjami jest podstawą do podejmowania właściwych decyzji, które mogą mieć krytyczne znaczenie dla życia i zdrowia ludzi.

W kontekście prywatności danych, szczególnie gdy wykorzystuje się AI do analizy danych osobowych, takich jak lokalizacje użytkowników czy informacje o zdrowiu, niezbędne jest stosowanie odpowiednich regulacji i technologii ochrony prywatności. W tym przypadku chodzi o zastosowanie zaawansowanych metod szyfrowania danych, anonimizacji, a także zapewnienia, że dostęp do wrażliwych informacji będzie możliwy tylko dla uprawnionych osób, zgodnie z obowiązującymi przepisami prawa, takimi jak RODO w Unii Europejskiej.

Wyzwanie stanowi również ochrona przed cyberatakami, które mogą mieć na celu zakłócenie działania systemów zarządzania kryzysowego. W tym kontekście, systemy AI muszą być wyposażone w mechanizmy wykrywania prób nieautoryzowanego dostępu, takich jak ataki DDoS (rozproszona odmowa usługi) czy złośliwe oprogramowanie, które mogłyby sparaliżować funkcjonowanie całych sieci zarządzania kryzysowego. Odpowiednia detekcja takich zagrożeń w czasie rzeczywistym, a także szybka reakcja na nie, są kluczowe dla utrzymania stabilności i bezpieczeństwa systemów teleinformatycznych.

Kolejnym aspektem zabezpieczeń jest właściwe zarządzanie dostępem do systemów AI. W sytuacjach kryzysowych, dostęp do systemów zarządzania kryzysowego i platform AI powinien być ściśle kontrolowany i ograniczony do osób posiadających odpowiednie uprawnienia. Zastosowanie rozwiązań, takich jak autentykacja dwuskładnikowa (2FA) czy biometria, które zapewniają dodatkową warstwę ochrony, jest niezbędne, by zapobiec nieuprawnionemu dostępowi do wrażliwych informacji.

[14] K. Sienkiewicz-Małyjurek, *Możliwości i problemy zastosowania sztucznej inteligencji w zarządzaniu kryzysowym*, Bezpieczeństwo. Teoria i Praktyka, 1, 2024, s. 53.

Aby zapewnić ciągłość działania systemów, niezbędne jest także posiadanie rozwiązań awaryjnych i planów odzyskiwania danych w razie awarii systemów. Systemy AI wykorzystywane w zarządzaniu kryzysowym muszą być odporne na różne scenariusze awaryjne, takie jak przerwy w dostępie do sieci czy uszkodzenia infrastruktury[15]. Zapewne AI będzie też wspierać działania na rzecz sprawniejszego zarządzania infrastrukturą krytyczną i ogólnie usługami użyteczności publicznej, co obecnie jest skomplikowane i czasochłonne[16].

Zastosowanie redundancji systemów, zasilania awaryjnego oraz procedur na wypadek awarii pozwala na szybkie przywrócenie pełnej funkcjonalności systemu, co ma kluczowe znaczenie w sytuacjach kryzysowych.

Ostatecznie, strategia zabezpieczeń w kontekście AI w zarządzaniu kryzysowym wymaga nie tylko technologicznych rozwiązań, ale także odpowiednich regulacji i procedur w zakresie ochrony danych, zarządzania dostępem oraz reagowania na zagrożenia[17]. Skuteczna integracja sztucznej inteligencji z systemami kryzysowymi, przy jednoczesnym zapewnieniu najwyższych standardów bezpieczeństwa, pozwala na optymalne wykorzystanie potencjału AI w zarządzaniu kryzysowym, przy minimalizacji ryzyk związanych z cyberzagrożeniami. Ważnym aspektem jest również redundancja infrastruktury, czyli zastosowanie zapasowych systemów, serwerów i połączeń sieciowych. Rozwiązania, takie jak rozproszone centra danych, systemy automatycznego przełączania oraz backupy w chmurze, zapewniają ciągłość działania nawet w przypadku awarii lub ataku cybernetycznego.

Nieodzownym elementem skutecznej strategii bezpieczeństwa jest także rozwój procedur reagowania na incydenty. Opracowanie i regularne testowanie planów awaryjnych pozwalają na szybkie i skuteczne reagowanie na zagrożenia, minimalizując negatywne skutki ataków lub awarii technicznych[18]. Ich

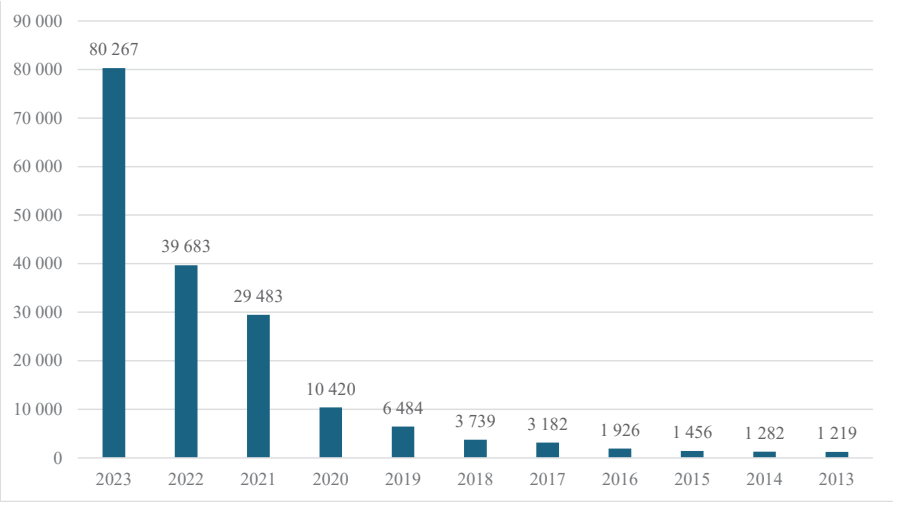
[15] W. Krasiński, *Sztuczna inteligencja w ochronie ludności w Polsce – możliwości i perspektywy wykorzystania*, DOCTRINA.Studia Społeczno-Polityczne, 21, 2024, s. 34.

[16] T. Michalak, *Sztuczna inteligencja i ochrona infrastruktury krytycznej*. „AI to broń obosieczna" (wywiad przeprowadzony przez M. Górskiego), https://cyberdefence24.pl/cybermagazyn/cybermagazyn-sztucznainteligencja-i-ochrona-infrastruktury-krytycznej-ai-to-bron-obosieczna, [dostęp: 26.03.2025].

[17] A. Manoj, A. Shweta, *A systematic review on artificial intelligence/deep learning applications and challenges to battle against covid-19 pandemic*, Disaster Advances 2021, vol. 14, nr 8, s. 90.

[18] P. Gibuła, *Działania na rzecz bezpieczeństwa teleinformatycznego Polski. Niebezpieczna cyberprzestrzeń*, Kontrola Państwowa, 4(369), 2016, s. 630.

liczba z roku na rok drastycznie wzrasta. Ilość incydentów obsłużonych przez CISIRT NAKS w latach 2013-2023 przestawiono na poniższym rysunku.



Rysunek 3. Zestawienie liczby obsłużonych incydentów przez CERT Polska w latach 2013-2023

Źródło: Raport roczny z działalności CERT POLSKA 2023.

Oprócz technologicznych środków ochrony kluczowe znaczenie ma szkolenie personelu oraz wdrażanie odpowiednich polityk bezpieczeństwa. Ludzki błąd jest jednym z najczęstszych powodów naruszeń systemów teleinformatycznych, dlatego edukacja pracowników w zakresie rozpoznawania zagrożeń, stosowania zasad cyberhigieny oraz przestrzegania procedur bezpieczeństwa jest niezbędna. Rozwiązania edukacyjne oraz konsekwentnie wdrażane rozwiązania i aplikacje, metody i sposoby ochrony informacji, mogą poprawić istniejący stan bezpieczeństwa informacji, co sprzyja skutecznej ochronie informacji w cyberprzestrzeni[19] również w odniesieniu do zarządzania kryzysowego.

Dynamicznie zmieniające się środowisko zagrożeń wymaga ciągłego doskonalenia strategii zabezpieczeń oraz dostosowywania ich do nowych wyzwań. Systematyczne audyty, testy penetracyjne oraz aktualizacje oprogramowania stanowią kluczowe elementy długoterminowej polityki bezpieczeństwa, która zapewnia stabilność i niezawodność systemów teleinformatycznych wykorzystywanych w zarządzaniu kryzysowym.

[19] M. Kowalewski, *Problemy i potrzeby kształcenia w zakresie bezpieczeństwa informacji i systemów teleinformatycznych*, Obronność. Zeszyty Naukowe, 4(28), 2018, s. 119.

Podsumowanie

Bezpieczeństwo systemów teleinformatycznych odgrywa kluczową rolę w skutecznym zarządzaniu kryzysowym. Współczesne technologie umożliwiają szybkie gromadzenie i analizę danych, efektywną komunikację oraz podejmowanie trafnych decyzji w sytuacjach nadzwyczajnych. Jednak ich rosnąca zależność od technologii cyfrowych niesie ze sobą również poważne zagrożenia, takie jak cyberataki, awarie techniczne czy dezinformacja. W szczególności phishing stanowi jedno z najpoważniejszych wyzwań, mogąc prowadzić do utraty dostępu do kluczowych systemów, naruszenia poufności danych oraz dezorganizacji działań kryzysowych.

Analiza zagrożeń i najlepszych praktyk w zakresie ochrony systemów teleinformatycznych wskazuje na konieczność wdrażania wielopoziomowych mechanizmów bezpieczeństwa, takich jak szyfrowanie danych, systemy wykrywania zagrożeń, redundancja infrastruktury oraz procedury reagowania na incydenty. Niezwykle istotne jest również regularne szkolenie personelu, ponieważ czynniki ludzkie nadal pozostają jednym z najsłabszych ogniw w systemach zabezpieczeń.

Wnioski płynące z niniejszej analizy podkreślają, że zapewnienie bezpieczeństwa systemów teleinformatycznych wymaga podejścia kompleksowego i dynamicznego. Zagrożenia cybernetyczne ewoluują w szybkim tempie, co oznacza, że również strategie obronne muszą być stale aktualizowane i dostosowywane do nowych wyzwań. Kluczowe znaczenie ma tu współpraca między instytucjami odpowiedzialnymi za zarządzanie kryzysowe, sektorem IT oraz ekspertami ds. cyberbezpieczeństwa.

Dalsze badania w tym obszarze powinny koncentrować się na opracowywaniu bardziej zaawansowanych metod wykrywania i neutralizacji zagrożeń cybernetycznych w czasie rzeczywistym. Szczególnie istotne jest rozwijanie technologii sztucznej inteligencji i uczenia maszynowego, które mogą automatycznie analizować anomalie w systemach teleinformatycznych i skutecznie identyfikować potencjalne ataki. Ponadto warto prowadzić badania nad odpornością systemów zarządzania kryzysowego na ataki socjotechniczne, a także doskonalić metody edukacji i szkolenia personelu w zakresie cyberhigieny i reagowania na incydenty.

Ostatecznie, bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym nie jest jednorazowym działaniem, lecz ciągłym procesem

wymagającym zaangażowania, innowacyjnych rozwiązań oraz współpracy między różnymi sektorami. Skuteczna ochrona tych systemów jest niezbędna do zapewnienia stabilności i bezpieczeństwa społeczeństwa w obliczu różnorodnych zagrożeń.

Literatura

1. Apiecionek Ł., *Fuzzy Observation of DDoS Attack,* [w:] *Theory and Applications of Ordered Fuzzy Numbers. A Tribute to Professor*, W. Kosiński, P. Prokopowicz, J. Czerniak, D. Mikołajewski, Ł. Apiecionek, D. Slezak, Bydgoszcz 2017.
2. Elszkowski M., *Działalność Policji w sytuacjach kryzysowych. Podejście formalne*, Zeszyty Naukowe SGSP, Nr 61 (tom 2)/1, 2017.
3. Gibuła P., *Działania na rzecz bezpieczeństwa teleinformatycznego Polski. Niebezpieczna cyberprzestrzeń*, Kontrola Państwowa, 4(369), 2016.
4. Grzebielec S., *Analiza podatności użytkowników systemów informatycznych na atak phishingowy*, Journal of Computer Sciences Institute, vol. 15, 2020.
5. Krasiński W., *Sztuczna inteligencja w ochronie ludności w Polsce – możliwości i perspektywy wykorzystania*, DOCTRINA.Studia Społeczno-Polityczne, 21, 2024.
6. Kowalewski M., *Problemy i potrzeby kształcenia w zakresie bezpieczeństwa informacji i systemów teleinformatycznych*, Obronność. Zeszyty Naukowe, 4(28), 2018.
7. Manoj A., Shweta A., *A systematic review on artificial intelligence/deep learning applications and challenges to battle against covid-19 pandemic*, Disaster Advances 2021, vol. 14, nr 8.
8. Michalak T., *Sztuczna inteligencja i ochrona infrastruktury krytycznej. „AI to broń obosieczna"* (wywiad przeprowadzony przez M. Górskiego), https://cyberdefence24.pl/cybermagazyn/cybermagazyn-sztuczna-inteligencja-i-ochrona-infrastruktury
9. NATO CWIX 2023 - kolejny sukces systemu JAŚMIN, https://zbiam.pl/nato-cwix-2023-kolejny-sukces-systemu-jasmin/
10. Niewiadomska-Szynkiewicz E., Litka R., *Ataki na urządzenia mobilne i metody ich wykrywania*, Cybersecurity and Law, nr 1(9), 2023.
11. Patkowski A., „*Cicha reakcja" na zdalne ataki teleinformatyczne*, Przegląd Teleinformatyczny, T. 5, nr 3(44), 2017.
12. Protasowicki I., *Wpływ zagrożenia atakami DOS/DDOS na bezpieczeństwo teleinformatycznej infrastruktury krytycznej*, Modern Management Review, vol. XXIII, 25(1), 2018.
13. Pyka J., *Komunikacja w zarządzaniu kryzysowym – problemy i wyzwania*, Zeszyty Naukowe Akademii Górnośląskiej, Nr 7/2023, s. 127.
14. SZK JAŚMIN - Wielośrodowiskowy Zautomatyzowany System Zarządzania Kryzysowego - TELDAT, https://www.teldat.com.pl/oferta/produkty/systemy/319-szk-jasmin.html

15. System JAŚMIN też w zarządzaniu kryzysowym i wsparciu akcji antykryzysowych, https://defence24.pl/polityka-obronna/system-jasmin-tez-w-zarzadzaniu-kryzysowym-i-wsparciu-akcji-antykryzysowych
16. Sienkiewicz-Małyjurek K., *Możliwości i problemy zastosowania sztucznej inteligencji w zarządzaniu kryzysowym*, Bezpieczeństwo. Teoria i Praktyka, 1, 2024.
17. Witkowski M., *Bezpieczeństwo systemów teleinformatycznych w zarządzaniu kryzysowym*, Zeszyty Naukowe WSOWL, nr 4(162), 2011.
18. Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, Studia i Materiały Informatyki Stosowanej, nr 7, 2012.

mgr Natalia Domasiak
Akademia Sztuki Wojennej w Warszawie
ORCID: 0009-0001-5162-6498

https://doi.org/10.29316/9788368103205_9

ROLA SŁUŻB SPECJALNYCH W ZAPEWNIANIU BEZPIECZEŃSTWA POLSKI W DOBIE ZAGROŻEŃ HYBRYDOWYCH

THE ROLE OF SPECIAL SERVICES IN ENSURING POLISH SECURITY IN THE ERA OF HYBRID THREATS

Streszczenie

Autorka analizuje istotę i charakter zagrożeń hybrydowych, podkreślając ich wielowymiarowość oraz trudność w wykryciu i przypisaniu odpowiedzialności za ich realizację. Przedstawiono definicje zagrożeń hybrydowych według NATO, Unii Europejskiej oraz polskich instytucji, wskazując na ich wspólne cechy: skoordynowanie działań państwowych i niepaństwowych, wykorzystanie zarówno środków militarnych, jak i niemilitarnych oraz prowadzenie operacji poniżej progu otwartej wojny. Autorka omawia również rolę polskich służb specjalnych – zarówno cywilnych (ABW, AW), jak i wojskowych (SKW, SWW) – w systemie bezpieczeństwa państwa. Służby te realizują zadania z zakresu rozpoznawania, zapobiegania

Summary

The author conducts an analysis of the essence and nature of hybrid threats, emphasising their multidimensionality and the complexity of detecting and attributing responsibility for their implementation. Definitions of hybrid threats are presented, drawn from the perspectives of NATO, the European Union, and Polish institutions. These definitions highlight common features, including coordination of actions between states and non-state actors, the utilisation of both military and non-military means, and the execution of operations that fall below the threshold of open warfare. The author also discusses the role of Polish special services – both civilian (ABW, AW) and military (SKW, SWW) – in the state security system. The aforementioned

i zwalczania zagrożeń hybrydowych, takich jak cyberataki, dezinformacja, sabotaż czy operacje wywiadowcze. Wskazano także na konkretne przykłady działań hybrydowych wymierzonych przeciwko Polsce, w tym kryzys migracyjny na granicy polsko-białoruskiej oraz operacje dywersyjne i propagandowe inspirowane przez rosyjskie służby specjalne. Podkreślono, że skuteczna ochrona przed zagrożeniami hybrydowymi wymaga ścisłej współpracy służb specjalnych, nowoczesnych technologii oraz ciągłego doskonalenia metod rozpoznania i przeciwdziałania tego typu zagrożeniom

Słowa kluczowe: służby specjalne, zagrożenia hybrydowe, bezpieczeństwo państwa

services are responsible for the identification, prevention and combating of hybrid threats, including, but not limited to, cyber-attacks, disinformation, sabotage, and intelligence operations. It was further noted that there were specific instances of hybrid actions against Poland, including the migration crisis on the Polish-Belarusian border and diversionary and propaganda operations inspired by Russian special services. It was emphasised that effective protection against hybrid threats requires close cooperation between special services, modern technologies, and continuous improvement in methods of identifying and countering such threats.

Keywords: special services, hybrid threats, state securit

Wstęp

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą złożonością i nieprzewidywalnością zagrożeń. Jednym z kluczowych wyzwań XXI wieku są zagrożenia hybrydowe, które wymykają się tradycyjnym klasyfikacjom konfliktów. Termin „zagrożenia hybrydowe" obejmuje szerokie spektrum działań prowadzonych poniżej progu otwartej wojny, łączących elementy konwencjonalne i niekonwencjonalne, militarne i niemilitarne, realizowanych przez aktorów państwowych i niepaństwowych w sposób skoordynowany i zsynchronizowany, a ich celem jest destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach. W obliczu tych wyzwań kluczową rolę odgrywają służby specjalne, które odpowiadają za identyfikację, analizę i przeciwdziałanie zagrożeniom hybrydowym, chroniąc bezpieczeństwo państwa zarówno w wymiarze wewnętrznym, jak i zewnętrznym. Do zadań służb należy zapewnienie odporności na nowe, nieliniowe formy agresji, które coraz częściej stają się narzędziem walki we współczesnym świecie.

Zagrożenia hybrydowe – istota i charakter

Współczesne środowisko bezpieczeństwa państwowego charakteryzuje się rosnącą złożonością i nieprzewidywalnością zagrożeń. Jednym z najbardziej dynamicznie rozwijających się wyzwań są zagrożenia hybrydowe, które wymykają się tradycyjnym klasyfikacjom konfliktów i działań zbrojnych. Termin ten odnosi się do szerokiego spektrum działań prowadzonych poniżej progu otwartej wojny, łączących metody konwencjonalne i niekonwencjonalne, militarne i niemilitarne, realizowanych przez aktorów państwowych i niepaństwowych w sposób skoordynowany i zsynchronizowany. Celem tych działań jest nie tylko zadanie bezpośrednich szkód, ale przede wszystkim destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach.

Według NATO są to działania militarne i niemilitarne oraz jawne i niejawne środki, obejmujące dezinformację, ataki cybernetyczne, presję ekonomiczną, użycie nieregularnych grup zbrojnych i wojsk regularnych. Mają na celu rozmywanie granicy między wojną i pokojem oraz dezorientowanie społeczeństw[1].

Z kolei Unia Europejska definiuje zagrożenia hybrydowe jako połączenie działań konwencjonalnych i niekonwencjonalnych (militarnych i niemilitarnych), stosowanych w skoordynowany sposób przez aktorów państwowych i niepaństwowych, ukierunkowanych na osiągnięcie celów politycznych”[2].

Słownik terminów z zakresu bezpieczeństwa definiuje zagrożenia hybrydowe jako „zagrożenia generowane przez działania hybrydowe – godzące w interesy podmiotu bezpieczeństwa”[3]. Przez działania hybrydowe rozumiane są „działania mające na celu osiągnięcie zamierzeń politycznych i strategicznych z możliwością utrzymywania dotychczasowych stosunków gospodarczych i/lub dyplomatycznych, prowadzone przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany, łączące różne środki wywierania nacisku oraz uzależniania od potencjalnego agresora”[4].

---

1 *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm, [dostęp: 23.04.2025].

2 *A Europe that Protects: Countering Hybrid Threats*, https://www.eeas.europa.eu/node/46393_en, [dostęp: 16.04.2025].

3 J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń 2020 r., s. 276.

4 Ibidem, s. 53.

Rządowe Centrum Bezpieczeństwa wskazuje, że „działania hybrydowe to działania zmierzające do osiągnięcia celów politycznych i strategicznych agresora. Prowadzone są w sposób wielowymiarowy, skryty, utrudniający identyfikację przeciwnika i przypisanie odpowiedzialności za nie sprawcy. Działania te prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany, często rozłożone w dłuższym czasie oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora. Mogą być prowadzone przy użyciu środków politycznych, ekonomicznych, prawnych, militarnych i społecznych, w tym z wykorzystaniem różnego rodzaju kanałów komunikacji społecznej. Mogą również być prowadzone pośrednio, z wykorzystaniem lokalnych podmiotów, organizacji i osób prywatnych, co utrudnia wykrycie i przeciwdziałanie im”[5]. Przykładami działań hybrydowych są „operacje informacyjne, psychologiczne, działania o charakterze terrorystycznym, kryminalnym, działania mające na celu zakłócenie funkcjonowania sieci i systemów informatycznych, systemu energetycznego, systemu dostarczania paliw, systemów funkcjonowania i usług telekomunikacyjnych, systemu gazowego, zdarzeń związanych ze skażeniem chemicznym na lądzie, w wodzie i powietrzu, skażeniem promieniotwórczym, zakłócenia porządku publicznego, dezinformacji. Trudność w wykryciu i zdefiniowaniu, czy dane zdarzenie wystąpiło w obszarze działań hybrydowych, spowodowana jest często charakterem tych działań, tzn. działania hybrydowe mają zwykle charakter „pełzający”. Sprzyja to trudności w ich początkowym rozpoznaniu i zdefiniowaniu. Działania te poddają się ocenie w perspektywie dłuższego przedziału czasowego”[6].

Strategia Bezpieczeństwa Narodowego z 2020 r. wskazuje, że działania o charakterze hybrydowym będą pozostawać istotnym środkiem polityki, służącym zarówno podmiotom państwowym, jak i pozapaństwowym do osiągania ich celów. Działania te, możliwe, że zostaną przeniesione do przestrzeni kosmicznej[7].

Rosyjska koncepcja prowadzenia działań hybrydowych „polega na używaniu całego spektrum instrumentów politycznych, ekonomicznych i społecznych w celu m.in. manipulowania poglądami ludności w państwach

[5] Krajowy Plan Zarządzania Kryzysowego, https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego, [dostęp: 15.04.2025].

[6] Ibidem.

[7] Strategia Bezpieczeństwa Narodowego z 2020 roku, s. 7.

uznawanych za wrogie. Do najważniejszych obszarów rosyjskiej aktywności należą wojna informacyjna, cyberataki oraz instrumentalizacja migracji”[8].

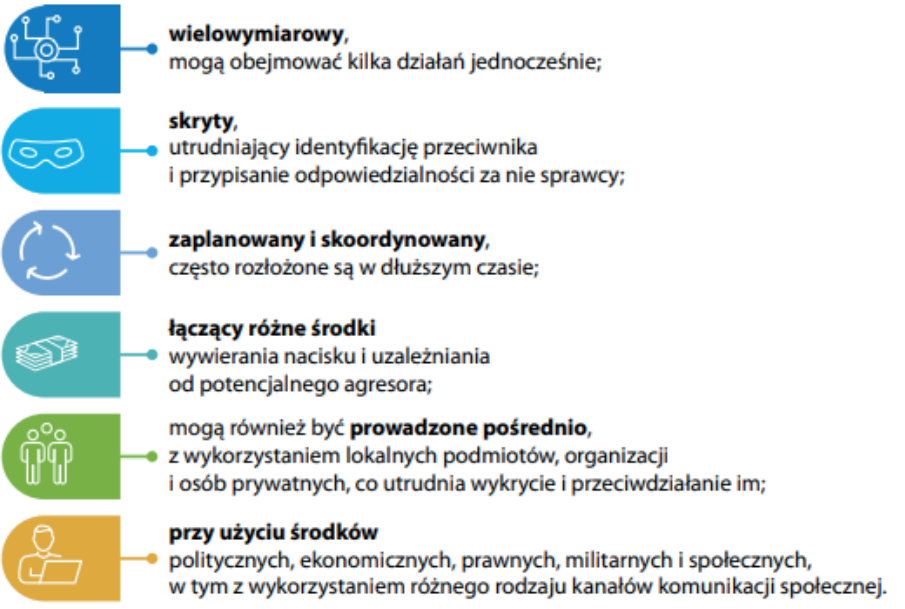
Termin zagrożenie hybrydowe odnosi się do działań podejmowanych przez podmioty państwowe lub niepaństwowe, których celem jest osłabienie lub zaszkodzenie celowi poprzez łączenie jawnych i tajnych środków militarnych i niemilitarnych[9]. Są one zaprojektowane tak, aby były trudne do wykrycia lub identyfikacji. Zagrożenia te są ukierunkowane na krytyczne słabe punkty i mają na celu wprowadzenie zamieszania, aby utrudnić szybkie i skuteczne podejmowanie decyzji. Zagrożenia hybrydowe mogą obejmować cyberataki na krytyczne systemy informatyczne, zakłócenia w świadczeniu kluczowych usług, takich jak dostawy energii czy usługi finansowe, podważanie zaufania publicznego do instytucji rządowych czy pogłębianie podziałów społecznych. Jako przykład zagrożeń hybrydowych możemy uznać operacje kinetyczne np. wykorzystanie nieoznakowanych żołnierzy do opanowania jakiegoś terytorium, cyberataki na infrastrukturę krytyczną, sabotaż, jak i niekinetyczne tj. dezinformacja, propaganda, presja ekonomiczna, operacje informacyjne, protesty itp.

Najwyższa Izba Kontroli do kontroli nt. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi przyjęła, że „działania hybrydowe (w czasie pokoju) to konwergencja różnych typów działań poniżej progu wojny, zagrażających lub mogących zagrażać bezpieczeństwu państwa i jego obywateli, prowadzonych z wykorzystaniem narzędzi klasycznych (np. dezinformacja), jak również nowoczesnych (np. cyberataki), mających na celu wywoływanie i podtrzymywanie sytuacji kryzysowych bez użycia regularnych środków militarnych. Spektrum środków wykorzystywanych w działaniach hybrydowych jest praktycznie nieograniczone i można zaliczyć do nich m.in. przestrzeń polityczną, dyplomatyczną, dezinformacyjno-propagandową, gospodarczą, kulturalną, terrorystyczną oraz humanitarną. Zagrożenia hybrydowe są różnorodne i ciągle się zmieniają, wykorzystując synergię tworzoną przez wiele podmiotów i działań. Działania hybrydowe mogą prowadzić zarówno agenci służb specjalnych obcego państwa i osoby z nimi współpracujące, jak również na przykład (świadomie bądź nie) organizacje,

[8] A. M. Dyner, *Działania hybrydowe Rosji przeciw państwom NATO i UE, Działania hybrydowe Rosji przeciw państwom NATO i UE*, https://pism.pl/publikacje/dzialania-hybrydowe--rosji-przeciw-panstwom-nato-i-ue, [dostęp: 15.04.2025].

[9] *Hybrid threats*, https://www.hybridcoe.fi/hybrid-threats/, [dostęp: 15.04.2025].

stowarzyszenia, instytucje, partie polityczne, firmy, korporacje i celebryci/osoby ogólnie znane. Należy przy tym podkreślić, że trudność w wykryciu i zdefiniowaniu, czy dane zdarzenie wystąpiło w obszarze działań hybrydowych, spowodowana jest często charakterem tych działań, tzn. działania hybrydowe mają zwykle charakter „pełzający”[10]. Poniżej na rysunku przedstawiono sposoby prowadzenia działań hybrydowych.



Rysunek 1. Sposoby prowadzenia działań hybrydowych

Źródło: wyniki kontroli NIK. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi. KPB.430.002.2023 Nr ewid. 16/2023/P/22/029/KPB.

Wojna hybrydowa, prowadzona poniżej progu działań zbrojnych lub bez bezpośredniej, jawnej agresji, przynosi liczne korzyści. Jest ona znacznie łatwiejsza, tańsza i mniej ryzykowna niż operacje kinetyczne. Taka forma walki wpisuje się również w starożytną filozofię wojny, według której najwyższą sztuką jest pokonanie przeciwnika bez konieczności walki – jak sugerował Sun Zi, jeden z największych strategów wojskowych. Drugą charakterystyczną cechą wojny hybrydowej jest jej niejednoznaczność i trudność w przypisaniu

[10] Wyniki kontroli NIK. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi. KPB.430.002.2023 Nr ewid. 16/2023/P/22/029/KPB.

odpowiedzialności, czyli tzw. atrybucji. Ataki hybrydowe zwykle cechuje wysoki poziom niejasności. Ta niepewność jest celowo kreowana i pogłębiania przez podmioty prowadzące takie działania, aby utrudnić wykrycie ataku i ustalenie jego sprawcy. Wykorzystując progi wykrywalności i poziomy atrybucji, agresorzy hybrydowi skutecznie utrudniają państwu obronę i opracowanie odpowiednich strategii[11].

Służby specjalne w systemie bezpieczeństwa państwa

W dobie tak specyficznych i unikalnych zagrożeń hybrydowych zapewnianie szeroko pojętego bezpieczeństwa jest naczelnym zadaniem polityki państwa, a także konstytucyjnym zadaniem jego organów. Funkcjonowanie państwa oparte na systemie bezpieczeństwa narodowego jest nierozerwalnie związane z działalnością służb specjalnych. Są to instytucje, które poprzez działalność operacyjno-rozpoznawczą (głównie o charakterze niejawnym) pozyskują i chronią kluczowe dla bezpieczeństwa państwa informacje. Ich cechą charakterystyczną jest tajność działania, a fundamentalnym zadaniem służb specjalnych ochrona bezpieczeństwa zewnętrznego i wewnętrznego wraz z ochroną jego porządku konstytucyjnego.

Rozważając problematykę służb specjalnych w systemie bezpieczeństwa państwa warto odpowiedzieć na pytanie: czym są służby specjalne? Sławomir Zalewski definiuje je jako „zorganizowane zazwyczaj przez państwo struktury, ukierunkowane na niejawne pozyskiwanie informacji, istotnych z punktu widzenia bezpieczeństwa organizatora tej działalności (państwa) bądź przeciwdziałania ich zdobywaniu przez podobne struktury, identyfikowane jako obce”[12]. Jednocześnie wskazuje, że pojęcie nie jest jednoznaczne, mimo że tym mianem powszechnie określany jest wywiad i kontrwywiad. W polskim systemie prawnym nie występuje definicja służb specjalnych, która wskazywałaby na charakter ich działalności. A zatem Zalewski wskazuje, że termin – służby specjalne – nie odnosi się do wszystkich służb prowadzących niejawną działalność, polegającą na podejmowaniu na podstawie przepisów

[11] A. Bilal, *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie” jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html, [dostęp: 15.04.2025].

[12] S. Zalewski, *Służby specjalne w państwie demokratycznym*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002, s. 13.

prawa działań operacyjno-rozpoznawczych, a tylko do tych, które „tradycyjnie" wykonują zadania wywiadowcze i kontrwywiadowcze"[13]. Bogusław Pacek z kolei wskazuje, że wszystkie instytucje państwowe, które prowadzą działania operacyjno-rozpoznawcze o niejawnym charakterze to służby specjalne[14]. *Słownik terminów z zakresu bezpieczeństwa* wskazuje, że służby specjalne to „instytucje pozyskujące i chroniące informacje kluczowe dla bezpieczeństwa państwa poprzez działalność operacyjno-rozpoznawczą, głównie o charakterze niejawnym". Przeważnie są to służby wywiadowcze i kontrwywiadowcze[15]. Na tej podstawie przyjmuje się, że w Polsce instytucje zajmujące się wywiadem i kontrwywiadem noszą miano służb specjalnych. Przyjmuje się także, że służby wywiadowcze koncentrują się na zdobywaniu i opracowywaniu informacji ważnych dla bezpieczeństwa państwa[16], a kontrwywiadowcze na udaremnianiu wysiłków obcych wywiadów w penetrowaniu lub dekonspirowaniu własnych służb wywiadowczych i ich operacji[17].

W polskim systemie bezpieczeństwa państwa funkcjonują cztery służby specjalne zajmujące się wywiadem i kontrwywiadem – dwie cywilne i dwie wojskowe. Do cywilnych służb specjalnych zalicza się Agencję Bezpieczeństwa Wewnętrznego odpowiedzialną za ochronę bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego oraz Agencję Wywiadu odpowiedzialną za ochronę bezpieczeństwa zewnętrznego państwa. Do wojskowych służb specjalnych należy Służba Kontrwywiadu Wojskowego właściwa w sprawach z zakresu ochrony przed zagrożeniami wewnętrznymi dla obronności kraju, zdolności bojowej i bezpieczeństwa Sił Zbrojnych RP oraz Służba Wywiadu Wojskowego odpowiedzialna za ochronę przed zagrożeniami zewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej SZ RP.

Z uwagi na szeroki zakres zadań, wiodącą rolę w systemie bezpieczeństwa państwa odgrywa w Polsce ABW. Głównym zadaniem ABW jest ochrona bezpieczeństwa wewnętrznego państwa oraz porządku konstytucyjnego. ABW

---

[13] D. Laskowski, *Prawne podstawy funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa*, Obronność. Zeszyty Naukowe, 2(10), 2014. s. 60-61.

[14] B. Pacek, *Osobowościowe uwarunkowania efektywności oficerów kontrwywiadu*, wyd. Akademia Obrony Narodowej Warszawa 2013, s. 10.

[15] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń 2020 r., s. 206-207.

[16] S. Hoc, *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Akademia Spraw Wewnętrznych, Warszawa 1985, s. 36.

[17] R. Kessler, *CIA od środka*, Wydawnictwo Ryton, Warszawa 1994, s. 295

zajmuje się rozpoznawaniem, zapobieganiem i zwalczaniem zagrożeń, takich jak terroryzm, szpiegostwo, naruszenia informacji niejawnych, przestępstwa godzące w podstawy ekonomiczne państwa czy korupcja na najwyższych szczeblach władzy. Do jej obowiązków należy również ochrona systemów teleinformatycznych i infrastruktury krytycznej państwa. Obszary w jakich ABW działa to: informacyjny, ścigania karnego oraz profilaktyczno-kontrolny. Zadania z zakresu zwalczania szpiegostwa, terroryzmu, ujawnienia bądź wykorzystania informacji niejawnych obejmują m.in. „monitorowanie instytucjonalnej i cudzoziemskiej aktywności na terenie Rzeczpospolitej Polskiej pod kątem realizacji zadań na rzecz obcych służb specjalnych, ofensywne rozpracowanie obcych służb specjalnych, rozpoznanie osób oraz innych podmiotów współpracujących z obcymi służbami specjalnymi”[18]. Z punktu widzenia zagrożeń hybrydowych istotnym zadaniem wykonywanym przez ABW jest prowadzenie szkoleń prewencyjnych dla urzędników państwowych na temat niebezpieczeństw z jakimi mogą się zetknąć w trakcie wykonywanych obowiązków.

Natomiast Służba Kontrwywiadu Wojskowego (SKW) ma za zadanie ochronę 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. Do podstawowych zadań SKW należy zwalczanie przestępstw tj. szpiegostwa przeciwko RP, zamachu lub sabotażu wobec SZ RP, nielegalnego obrotu z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa czy terroryzmu, ochrona informacji niejawnych, ochrona (kontrwywiadowcza) wojska poza granicami kraju, kontrwywiad radioelektroniczny oraz kryptografia i kryptoanaliza, kontrola umów międzynarodowych dotyczących rozbrojenia i ochrona badań naukowych. SKW zajmuje się również działaniami z zakresu cyberbezpieczeństwa np. dostarcza informacji o zagrożeniach związanych z wyborem oraz korzystaniem z technologii sprzętowych, informatycznych i szuka odpowiednich środków zaradczych”[19]. Jednocześnie prowadzi działania z zakresu „cyberkontrwywiadu w kontekście systemów teleinformatycznych i neutralizowania zagrożeń wewnętrznych o charakterze szpiegostwa, działania mające

[18] B. Opaliński, M. Rogalski, P. Szustakiewicz, Usta*wa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2017, s 21-22.

[19] *Służba Kontrwywiadu Wojskowego*, https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m--suzbakontrwywiadu-wojskowego/, [dostęp: 17.04.2025].

na celu wykrywanie przestępstw w kontekście systemów teleinformatycznych określonych w Rozdziale XXXIII Kodeksu karnego (przestępstwa przeciwko ochronie informacji)"[20]. Istotnym zadaniem jest także prowadzenie działań operacyjno-rozpoznawczych w cyberprzestrzeni, których celem jest badanie i neutralizowanie zagrożeń. W wyniku prowadzonych badań SKW gromadzi informacje nt. modus operandi oraz technik, taktyk i procedur grup hakerskich lub adwersarzy w cyberprzestrzeni celem umożliwienia realizacji działań wyprzedzających potencjalny atak cybernetyczny na systemy teleinformatyczne resortu.

Z kolei Agencja Wywiadu odpowiada za „uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego". Do jej zadań należy „rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej". W kontekście zagrożeń hybrydowych AW chroni zagraniczne przedstawicielstwa Polski oraz ich pracowników przed działaniami obcych służb specjalnych, a także zapewnia ochronę kryptograficzną łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej. Do zakresu zainteresowań AW należą także rejony napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo Polski. W tym zakresie funkcjonariusze AW rozpoznają i analizują zagrożenia tam występujące celem podjęcia działań mających je wyeliminować. Współczesne zagrożenia hybrydowe obejmują szerokie spektrum działań, takich jak operacje w cyberprzestrzeni, dezinformacja, ataki na infrastrukturę krytyczną, działania wywiadowcze, a także terroryzm i przestępczość zorganizowaną. W tym kontekście szczególnego znaczenia nabiera realizowany przez Agencję wywiad elektroniczny.

Służba Wywiadu Wojskowego otrzymała natomiast zadania z zakresu uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa potencjału obronnego Rzeczypospolitej Polskiej, bezpieczeństwa i zdolności bojowej SZ RP oraz warunków realizacji, przez SZ RP, zadań poza granicami państwa. Służba zajmuje się rozpoznawaniem i przeciwdziałaniem

[20] Ibidem.

militarnym zagrożeniom zewnętrznym godzącym w obronność Rzeczypospolitej Polskiej oraz zagrożeniom międzynarodowym terroryzmem. Analogicznie do AW funkcjonariusze SWW prowadzą rozpoznanie i analizę zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na obronność państwa oraz zdolność bojową SZ RP. SWW zostało również zobowiązane do eliminacji tych zagrożeń. SWW wykorzystuje zaawansowane technologie do zabezpieczania działań SZ RP (kryptografia) oraz łamania szyfrów stosowanych przez przeciwnika (kryptoanaliza), co ma szczególne znaczenie w walce z zagrożeniami hybrydowymi, gdzie granica między działaniami militarnymi, cybernetycznymi i informacyjnymi jest coraz bardziej płynna.

Służby specjalne wobec wybranych zagrożeń hybrydowych

Współczesny świat staje w obliczu coraz bardziej złożonych i różnorodnych zagrożeń, szczególnie tych o charakterze hybrydowym, które, choć znane od wieków, dopiero od lat 90. XX wieku są systematycznie badane i analizowane przez środowiska naukowe i wojskowe. Ich rosnące znaczenie wynika między innymi z działań Rosji wobec Ukrainy, które nasiliły się po Arabskiej Wiośnie, aneksji Krymu w 2014 r. i eskalacji konfliktu w 2022 r. W takich warunkach skuteczne zapewnienie bezpieczeństwa państwa wymaga sprawnie działających służb specjalnych, które odgrywają kluczową rolę w identyfikacji, analizie i przeciwdziałaniu współczesnym zagrożeniom hybrydowym.

Analizując rolę służb specjalnych w warunkach wojny hybrydowej, należy precyzyjnie powiązać ich działania z kluczowymi komponentami tego typu konfliktu. Wojna hybrydowa obejmuje bowiem równoległe operacje w przestrzeni dyplomatycznej, politycznej, ekonomicznej, informacyjnej oraz – choć w ograniczonym zakresie – militarnej. Celem tych działań jest destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach. „Profesor Khalid Mohamed Alqahtani, w publikacji „Modern Counter-IntelligenceSocial", podkreśla kluczowe znaczenie kontrwywiadu dla zapewnienia bezpieczeństwa, stabilności psychicznej społeczeństwa oraz wczesnego wykrywania wrogich zamiarów, zanim zostaną one zrealizowane"[21].

[21] A. Jawor, *Zadania kontrwywiadu w dobie współczesnych zagrożeń*, https://infosecurity24.pl/za-granica/zadania-kontrwywiadu-w-dobie-wspolczesnych-zagrozen, [dostęp: 18.04.2025].

Kontrwywiad tradycyjnie koncentrował się na zwalczaniu szpiegostwa, sabotażu i dywersji prowadzonej przez inne państwa. Po zakończeniu zimnej wojny i atakach z 11 września 2001 r., służby kontrwywiadowcze państw zachodnich ukierunkowały swoje zadania na walkę z terroryzmem i ekstremizmem oraz aktorami niepaństwowymi. Operacje antyterrorystyczne i antyrebelianckie sprawiły, że „kontrwywiad zaczął pełnić funkcję służebną wobec strategii ukierunkowanych na zwalczanie zagrożeń asymetrycznych". Wraz ze wzrostem znaczenia nowych technologii, aneksją Krymu w 2014 r., eskalacją konfliktu w Ukrainie i wojną informacyjną Rosji wobec Zachodu, zagrożenia hybrydowe przybierają na sile. W związku z tym, jak twierdzi Philip H. J. Davies, współczesny kontrwywiad skupia się nie tylko na przeciwdziałaniu infiltracji struktur państwowych poprzez wykrywanie obcych agentów, ale również na neutralizowaniu kanałów przenikania wpływów i aktywności informacyjno-psychologicznej, a także na przeciwdziałaniu zaawansowanym technikom rozpoznania przeciwnika[22]. W dobie cyberataków i dezinformacji kontrwywiad odpowiada za ochronę systemu politycznego, militarnego i gospodarczego państwa.

Z kolei wywiad w działaniach hybrydowych staje się niezbędny w realizacji złożonych operacji informacyjnych, przygotowaniu społeczeństw wg wcześniej opracowanych schematów oraz w prowadzeniu defensywnych i ofensywnych operacji. Służby wywiadowcze prowadzą działania w sferze politycznej, ekonomicznej, informacyjnej, dyplomatycznej i militarnej (w ograniczonym zakresie). W sferze politycznej wywiad monitoruje działania i zamiary zarówno państw, jak i aktorów niepaństwowych, analizując procesy decyzyjne, nastroje społeczne oraz potencjalne punkty zapalne. Pozwala to na wczesne wykrywanie prób destabilizacji, ingerencji w procesy wyborcze czy inspirowania protestów społecznych. Działania te są szczególnie istotne w kontekście zagrożeń hybrydowych, gdzie granica między polityką wewnętrzną a zewnętrzną często się zaciera, a operacje wpływu mogą być prowadzone zdalnie, przy użyciu nowoczesnych technologii komunikacyjnych. W wymiarze ekonomicznym wywiad skupia się na identyfikacji zagrożeń dla gospodarki państwa, takich jak próby przejęcia strategicznych przedsiębiorstw przez podmioty powiązane z obcymi wywiadami, manipulacje rynkami finansowymi, czy działania mające na celu wywołanie kryzysów energetycznych.

[22] Ibidem.

Służby wywiadowcze analizują również przepływy kapitału, inwestycje zagraniczne oraz transakcje handlowe, które mogą stanowić narzędzie wywierania nacisku lub infiltracji gospodarczej. W obszarze informacyjnym wywiad odgrywa kluczową rolę w rozpoznawaniu i przeciwdziałaniu kampaniom dezinformacyjnym, które mają na celu wprowadzenie chaosu, podważenie zaufania do instytucji państwowych, czy polaryzację społeczeństwa. Służby te monitorują media tradycyjne i społecznościowe, identyfikując źródła i kanały rozpowszechniania fałszywych informacji, a także analizują ich wpływ na opinię publiczną.

W razie potrzeby prowadzą działania kontrpropagandowe, mające na celu neutralizację szkodliwych narracji. Na płaszczyźnie dyplomatycznej wywiad wspiera działania rządu poprzez dostarczanie informacji o zamierzeniach i strategiach innych państw, przewidywanie reakcji na inicjatywy polityczne oraz identyfikowanie potencjalnych sojuszników i przeciwników na arenie międzynarodowej. Pozwala to na podejmowanie bardziej świadomych i skutecznych decyzji w zakresie polityki zagranicznej oraz budowanie koalicji przeciwdziałających zagrożeniom hybrydowym. W ograniczonym zakresie, wywiad angażuje się również w działania militarne, wspierając planowanie i realizację operacji wojskowych poprzez dostarczanie informacji o rozmieszczeniu sił przeciwnika, jego zdolnościach bojowych czy planowanych ruchach. Współczesne konflikty hybrydowe często wymagają ścisłej współpracy wywiadu z siłami zbrojnymi, zwłaszcza w zakresie rozpoznania elektronicznego, cyberoperacji oraz działań specjalnych[23].

Przykładem działań hybrydowych skierowanych przeciwko Polsce jest kryzys migracyjny na granicy polsko-białoruskiej toczący się od 2022 r. Operacja prowadzona przez Rosję i Białoruś z wykorzystaniem szlaku nielegalnej migracji ma na celu destabilizację krajów wschodniej flanki NATO. Przebieg operacji obejmuje zarówno działania fizyczne na granicy – forsowanie ogrodzeń, niszczenie zapór, prowokacje wobec polskich służb – jak i szeroko zakrojoną kampanię dezinformacyjną, mającą na celu oczernianie

[23] K. Surdyk, *Rola służb wywiadowczych w wojnie hybrydowej*, Ante Portas – Studia nad Bezpieczeństwem, Nr 2(11), 2018, s. 70-71.

Polski, polaryzację społeczeństw państw Zachodu i osłabianie ich solidarności, a także testowanie zdolności reagowania kryzysowego[24, 25].

Polskie służby specjalne w 2024 r. odnotowały intensyfikację działań o charakterze dywersyjnym wymierzonych przeciwko Rzeczypospolitej Polskiej oraz państwom członkowskim Unii Europejskiej i NATO. Są one inicjowane i koordynowane przez rosyjskie służby specjalne. Celem stały się przede wszystkim obiekty cywilne, w tym magazyny i sklepy wielkopowierzchniowe, a metodą – podpalenia. Działania te przybierają coraz częściej formę działań terrorystycznych. Charakter tych operacji wskazuje, że celem Rosji jest przede wszystkim zastraszenie obywateli Polski i państw Zachodu oraz zniechęcenie ich do udzielania dalszego wsparcia Ukrainie. Jednocześnie stanowią one narzędzie służące Moskwie do testowania odporności RP i naszych sojuszników na zagrożenia hybrydowe[26].

Działania hybrydowe obejmują szeroki wachlarz środków, w tym propagandę, dezinformację, operacje psychologiczne oraz próby rekrutacji do formacji zbrojnych, które służą destabilizacji państwa i społeczeństwa. Przykładem takiej aktywności była operacja zatrzymania przez Agencję Bezpieczeństwa Wewnętrznego w sierpniu 2023 r. dwóch obywateli Rosji, którzy rozklejali w Krakowie i Warszawie materiały propagandowe zachęcające do zaciągu do Grupy Wagnera – nielegalnej formacji najemniczej powiązanej z rosyjskimi służbami specjalnymi. Jak ustaliły polskie organy ścigania, zatrzymani prowadzili działania na rzecz rosyjskiego wywiadu, realizując elementy wojny hybrydowej, w tym operacje propagandowe i rekrutacyjne, mające na celu destabilizację sytuacji politycznej w Polsce i Europie oraz budowanie zaplecza do dalszych działań wywiadowczych i terrorystycznych[27].

---

[24] R. Gönczi, *Dezinformacja jako oręż wojny hybrydowej na granicy z Białorusią*, https://warsawinstitute.org/pl/dezionformacja-jako-orez-wojny-hybrydowej-na-granicy-z-bialorusia/, [dostęp: 15.04.2025].

[25] F. Bryjka, A. Legucka, *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, https://pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego, [dostęp: 15.04.2025].

[26] *Komunikat dotyczący działalności dywersyjnej FR*, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html, [dostęp: 15.04.2025].

[27] *ABW zatrzymała 2 obywateli Rosji*, https://www.abw.gov.pl/pl/informacje/2368,ABW-zatrzymala-2-obywateli-Rosji.html, [dostęp: 15.04.2025].

Podsumowanie

Zagrożenia hybrydowe, będące jednym z najpoważniejszych wyzwań dla współczesnych państw, charakteryzują się wielowymiarowością, tajnością oraz trudnością w jednoznacznym przypisaniu odpowiedzialności za ich realizację. Działania te łączą metody militarne i niemilitarne, konwencjonalne i niekonwencjonalne, a ich celem jest destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach. Przykłady takich działań obejmują cyberataki na infrastrukturę krytyczną, kampanie dezinformacyjne, presję ekonomiczną, sabotaż, działania terrorystyczne oraz instrumentalizację migracji – jak miało to miejsce na granicy polsko-białoruskiej w ostatnich latach.

Kluczową rolę w przeciwdziałaniu zagrożeniom hybrydowym odgrywają służby specjalne, zarówno cywilne, jak i wojskowe. W polskim systemie bezpieczeństwa są to m.in. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego. Instytucje te realizują zadania z zakresu rozpoznawania, zapobiegania i neutralizowania zagrożeń hybrydowych, prowadząc działania operacyjno-rozpoznawcze, monitorując aktywność obcych służb specjalnych, chroniąc infrastrukturę krytyczną oraz przeciwdziałając szpiegostwu, sabotażowi i dezinformacji. Szczególne znaczenie mają działania w cyberprzestrzeni, gdzie ataki na systemy informatyczne i telekomunikacyjne stanowią coraz większe zagrożenie dla funkcjonowania państwa.

Do współczesnych zagrożeń hybrydowych zalicza się działania Rosji wobec Ukrainy, operacje dywersyjne wymierzone w Polskę i jej sojuszników. Działania te pokazują, że zagrożenia są realne i dynamicznie się rozwijają. Rosyjskie służby specjalne prowadzą szeroko zakrojone operacje informacyjne, cybernetyczne i propagandowe, mające na celu destabilizację państw Zachodu, testowanie ich odporności oraz zniechęcanie do wspierania Ukrainy. Przykładem takich działań są podpalenia obiektów cywilnych, kampanie dezinformacyjne oraz próby rekrutacji do formacji zbrojnych, jak Grupa Wagnera.

Literatura

1. Hoc S., *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Warszawa 1985.
2. Kessler R., *CIA od środka*, Warszawa 1994.

3. Laskowski D., *Prawne podstawy funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa*, Obronność. Zeszyty Naukowe 2(10), 2014.
4. Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017.
5. Pacek B., *Osobowościowe uwarunkowania efektywności oficerów kontrwywiadu*, Warszawa 2013.
6. Pawłowski J., Zdrodowski B., Kuliczkowski M., *Słownik terminów z zakresu bezpieczeństwa*, Toruń 2020.
7. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Netografia

1. *A Europe that Protects: Countering Hybrid Threats*, https://www.eeas.europa.eu/node/46393_en.
2. *ABW zatrzymała 2 obywateli Rosji*, https://www.abw.gov.pl/pl/informacje/2368,ABW-zatrzymala-2-obywateli-Rosji.html.
3. Bilal A., *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie" jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html.
4. Bryjka F., Legucka A., *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, https://pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego.
5. *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm.
6. Dyner A. M., *Działania hybrydowe Rosji przeciw państwom NATO i UE, Działania hybrydowe Rosji przeciw państwom NATO i UE*, https://pism.pl/publikacje/dzialania-hybrydowe-rosji-przeciw-panstwom-nato-i-ue.
7. Gönczi R., *Dezinformacja jako oręż wojny hybrydowej na granicy z Białorusią*, https://warsawinstitute.org/pl/dezionformacja-jako-orez-wojny-hybrydowej-na-granicy-z-bialorusia/.
8. *Hybrid threats*, https://www.hybridcoe.fi/hybrid-threats/.
9. Jawor A., *Zadania kontrwywiadu w dobie współczesnych zagrożeń*, https://infosecurity24.pl/za-granica/zadania-kontrwywiadu-w-dobie-wspolczesnych-zagrozen.
10. *Komunikat dotyczący działalności dywersyjnej FR*, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html.
11. Krajowy Plan Zarządzania Kryzysowego, https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego.
12. Służba Kontrwywiadu Wojskowego, https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m-suzbakontrwywiadu-wojskowego/.

dr inż. Wojciech Szulc
Akademia Nauk Stosowanych im. ks. Jerzego Popiełuszki w Grudziądzu
ORCID: 0000-0002-4904-2020

https://doi.org/10.29316/9788368103205_10

OBRONA CYWILNA I POWSZECHNA SAMOOBRONA W POLSCE

CIVIL DEFENSE AND GENERAL SELF-DEFENSE IN POLAND

Streszczenie

Zapewnienie przetrwania ludności cywilnej w czasie wojny lub konfliktu zbrojnego jest ważnym obowiązkiem państwa. Niemniej nie zwalnia to osób przebywających na terenie Rzeczypospolitej Polskiej z odpowiedzialności za własne bezpieczeństwo. Należy brać pod uwagę, że w czasie wojny na obszarach o wysokiej intensywności prowadzenia działań zbrojnych organizacje obrony cywilnej nie będą w stanie terminowo udzielać pomocy wszystkim potrzebującym. W tym przypadku powszechna samoobrona będzie niezbędna dla zwiększenia szans ludności na przetrwanie.

Współczesny stan obrony cywilnej od 1989 roku kształtowany był przez ramy strategiczne polskiego bezpieczeństwa. Niemniej obecny stan przygotowań organów, podmiotów i zasobów ochrony ludności oraz obrony cywilnej do funkcjonowania w czasie wojny jest co najmniej niezadowalający. Można wręcz powiedzieć, że obrona cywilna dopiero

Summary

Ensuring the survival of civilians in times of war or armed conflict is an important duty of the state. However, this does not release anyone from responsibility for ensuring their own safety. It should be taken into account that in areas with high intensity of military operations civil defense organizations will not be able to provide timely assistance to all those in need. In this case, general self-defense will be necessary to increase the population's chances of survival.

The contemporary state of civil defence since 1989 has been shaped by the strategic framework of Polish security. Nevertheless, the current state of preparation of civil defence entities and resources is unsatisfactory. It can be said that civil defense is being created anew.

The aim of the study is to indicate how to improve the functioning of civil defence and general self-defence in Poland.

tworzy się na nowo. Celem opracowania jest wskazanie możliwości poprawy funkcjonowania obrony cywilnej i powszechnej samoobrony w Polsce.

Słowa kluczowe: obrona cywilna, powszechna samoobrona, bezpieczeństwo, ochrona ludności

Keywords: civil defense, self-defense, security, population protection

Wstęp

Zapewnienie przetrwania ludności cywilnej w czasie wojny jest kluczowym obowiązkiem państwa. Tylko przetrwanie ludności może zapewnić przetrwanie państwa. Rzeczypospolita Polska jest dobrem wspólnym wszystkich obywateli[1], które bez ludności nie będzie w stanie trwać. Niemniej musimy zdawać sobie sprawę z faktu, że ludność też jest odpowiedzialna za zapewnienie samym sobie warunków do przetrwania. Jest to nie tylko prawny obowiązek wynikający z postanowień ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), ale przede wszystkim logiczna konieczność wynikająca z występowania zagrożeń dla człowieka. Jednocześnie czas pokojowego funkcjonowania przyzwyczaił ludzi do powierzania własnego bezpieczeństwa wyłącznie służbom i instytucjom utrzymywanym z budżetu państwa. Czas wojny będzie zmuszał ludzi do własnej aktywności przejawiającej się w postaci powszechnej samoobrony. Należy przy tym pamiętać, że w czasie wojny priorytetem państwa będzie zabezpieczenie potrzeb systemu obronnego[2].

Niniejszy rozdział poświęcony został problematyce funkcjonowania obrony cywilnej i powszechnej samoobrony w Polsce. Obejmuje on wprowadzenie, część główną oraz podsumowanie. Część główna składa się z pięciu zatytułowanych rozdziałów. W pierwszym dokonano analizy wpływu ram strategicznych polskiego bezpieczeństwa po roku 1989 na kształtowanie się ochrony ludności i obrony cywilnej w Polsce. W drugim przedstawiono zadania obrony cywilnej. W trzecim rozdziale opisano problematykę funkcjonowania

[1] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r., nr 78, poz. 483 z późn. zm.), art. 1.

[2] W. Kitler, *Funkcjonowanie ludności w warunkach zewnętrznego zagrożenia państwa oraz w czasie wojny. Rozważania prawne i organizacyjne*, [w:] *Funkcjonowanie państwa w warunkach zewnętrznego zagrożenia państwa i w czasie wojny*, W. Kitler, P. Hac (red.), Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2022, s. 272.

systemu wykrywania, powiadamiania, ostrzegania i alarmowania o zagrożeniach. W czwartym dokonano analizy organizacji obrony cywilnej w Polsce. W piątym dokonano analizy roli powszechnej samoobrony w czasie wojny oraz zdarzeń kryzysowych. Problem badawczy niniejszego opracowania sformułowany został w postaci pytania: Jaki jest stan przygotowań obrony cywilnej i powszechnej samoobrony do funkcjonowania w czasie wojny? Celem rozdziału jest wskazanie możliwości poprawy funkcjonowania obrony cywilnej i powszechnej samoobrony w Polsce.

Złożoność problematyki niniejszego rozdziału determinuje wykorzystanie takich metod, jak: metoda uogólniania, metoda analizy, studium przypadków, metoda obserwacji oraz metoda wnioskowania.

Wpływ ram strategicznych polskiego bezpieczeństwa po roku 1989 na kształtowanie się ochrony ludności i obrony cywilnej w Polsce

Uzasadnionym jest twierdzić, że w ciągu ostatnich dekad w centrum uwagi pozostawał rozwój ratownictwa, spychając obronę cywilną na dalszy plan. Wynikało to ze skupienia się na bieżących sprawach czasu pokoju. Skupiliśmy się na zaspokojeniu potrzeb ochrony ludności wynikających z pokojowego funkcjonowania, co umożliwiło między innymi dynamiczny rozwój ratownictwa oraz służb współtworzących liczne systemy realizujące zadania ratownicze. To pozwoliło osiągnąć wysoki poziom ich skuteczności.

Od roku 1989 w odpowiedzi na nowo kształtujące się środowisko bezpieczeństwa Polski tworzono ramy strategiczne umacniania polskiego bezpieczeństwa. To na podstawie dokumentów wyznaczających owe ramy strategiczne bezpieczeństwa kształtowała się odpowiedź państwa na zagrożenia zarówno wewnętrzne, jaki i zewnętrzne w warunkach samodzielności strategicznej.

Po rozpadzie Związku Socjalistycznych Republik Radzieckich oraz Układu Warszawskiego podczas posiedzenia Komitetu Obrony Kraju 2 listopada 1992 r. przyjęto dwa dokumenty, jakimi były: założenia polskiej polityki bezpieczeństwa oraz Polityka bezpieczeństwa i strategia obronna Rzeczypospolitej Polskiej. Potrzeba ich wdrożenia wynikała z istotnej zmiany, jaką było funkcjonowanie państwa w warunkach samodzielności obronnej. W związku z rozpadem dwubiegunowego układu polityczno-militarnego zaprzestano eksponować zagrożenie wojną globalną, natomiast wskazywano na groźbę

konfliktów zbrojnych posiadających charakter lokalny oraz regionalny[3]. Niemniej, jak pisze Stanisław Koziej „Zaniechanie dostosowywania prawa do radykalnie i szybko zmieniającej się rzeczywistości ustrojowej, gospodarczej i społecznej doprowadziło do sytuacji, w której realizacja zadań obronnych zależała niemal wyłącznie od woli poszczególnych wykonawców”[4]. W tych warunkach utrudnione było również zadbanie o sprawy obrony cywilnej.

W latach 90. ubiegłego wieku strategicznym celem Polski było członkostwo w Sojuszu Północnoatlantyckim oraz w Unii Europejskiej, a jednocześnie przemiany ustrojowe oraz gospodarcze, jakie miały miejsce w Polsce powodowały okresowy wzrost zagrożeń wewnętrznych o charakterze politycznym, społecznym i ekonomicznym. Uzasadnionym jest twierdzić, że te właśnie zagrożenia stanowiły priorytetowy obszar skupienia uwagi władz państwowych. Jednocześnie rozpad ZSRR spowodował wzrost obaw o możliwość wciągnięcia Polski w konflikty zbrojne na tle granicznym, etnicznym lub ekonomicznym między nowo tworzącymi się podmiotami politycznymi.

Istotnym jest, że w jednym z kolejnych aktów wyznaczających ramy strategiczne umacniania polskiego bezpieczeństwa, jakim była Strategia Bezpieczeństwa Rzeczypospolitej Polskiej z 2000 r. zawarto zapisy mówiące, że „W dającej się przewidzieć przyszłości niepodległy byt Polski nie jest zagrożony, kraj nasz nie jest narażony na bezpośrednią agresję militarną”[5]. Uznano najwidoczniej, że członkostwo Polski w NATO wzmocniło potencjał odstraszania oraz zmniejszyło groźbę potencjalnej agresji zbrojnej na nasz kraj. W Strategii podkreślono zmniejszenie zagrożenia wojną na skalę globalną. Wszystko to stanowiło argument za ograniczeniem wydatków na obronność[6], a zarazem dawało argument za odłożeniem spraw obrony cywilnej na plan dalszy.

Z kolei koncepcyjne podstawy Strategii Bezpieczeństwa Narodowego z 2014 r. zostały wypracowane podczas kompleksowego Strategicznego Przeglądu Bezpieczeństwa przeprowadzonego w latach 2010-2012. W 2013 r.

---

3 S. Koziej, *Obronność Polski w warunkach samodzielności strategicznej lat 90. XX wieku*, Bezpieczeństwo Narodowe, nr 21, 2012, s. 25-26.

4 Ibidem, s. 28-29.

5 Strategia Bezpieczeństwa Rzeczypospolitej Polskiej 2000 r., p. 2.1.

6 S. Koziej, A. Brzozowski, *Strategie bezpieczeństwa narodowego RP 1990-2014. Refleksja na ćwierćwiecze,* [w:] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej pierwsze 25 lat*, R. Kupiecki (red. nauk.), Wojskowe Centrum Edukacji Obywatelskiej im. płk. dypl. Mariana Porwita, Warszawa 2015, s. 26.

opracowano „Białą Księgę Bezpieczeństwa Narodowego RP”[7], popularyzującą wyniki powyższego przeglądu. W Strategii Bezpieczeństwa Narodowego z 2014 r. podkreślano nasilanie konfrontacyjnej polityki Federacji Rosyjskiej, a na potwierdzenie tego podano przykład konfliktu z Ukrainą oraz aneksję Krymu[8]. W Strategii wskazywano również na zagrożenia wynikające z ekstremizmu i terroryzmu oraz na potrzebę wdrożenia „rozwiązań prawnych i organizacyjnych w zakresie systemu ochrony ludności oraz obrony cywilnej”[9]. Wskazano też, że: „Powiązany z problematyką ochrony ludności obszar obrony cywilnej wymaga kompleksowej transformacji i dostosowania do obecnej sytuacji społeczno-gospodarczej, w tym zobowiązań międzynarodowych”[10]. Mimo tego zapisu 4 lata później w 2018 r. „Najwyższa Izba Kontroli po raz kolejny wskazuje, że struktury obrony cywilnej nie są przygotowane do skutecznej realizacji zadań w zakresie ochrony ludności, wynikających z I Protokołu Dodatkowego do Konwencji Genewskich z dnia 12 sierpnia 1949 r. Struktura i organizacja obrony cywilnej jest archaiczna. Liczba formacji obrony cywilnej jest nieadekwatna do zidentyfikowanych zagrożeń i z każdym kolejnym rokiem maleje, a wyposażenie istniejących formacji jest niekompletne i przestarzałe”[11]. Jednocześnie istotnym problemem jest deficyt schronów dla ludności[12] (nad schronami dominuje liczba ukryć i miejsc doraźnego schronienia).

W Strategii Bezpieczeństwa Narodowego z 2020 r., jako najpoważniejsze zagrożenie dla Polski uznano neoimperialną politykę władz Federacji Rosyjskiej[13]. W Strategii podkreślono potrzebę zapewnienia powszechnego charakteru obrony cywilnej[14]. Znalazł się w niej zapis wskazujący na konieczność opracowania ustawy, która kompleksowo regulowałaby problematykę

---

7 *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.

8 Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014, Warszawa 2014 r., pkt 41.

9 Ibidem, pkt 12.

10 Ibidem, pkt 134.

11 Informacja o wynikach kontroli. *Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej,* KPB.430.009.2017, Nr ewid. 147/2018/P/17/039/KPB, Najwyższa Izba kontroli, Departament Porządku i Bezpieczeństwa Publicznego, Warszawa 2018, s. 9.

12 Zob. Raport dotyczący budowli ochronnych, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2023.

13 Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020…, dz. cyt., s. 6.

14 Ibidem, pkt 2.2. oraz 2.6.

obrony cywilnej[15]. Niemniej ustawa regulująca sprawy ochrony ludności i obrony cywilnej na gruncie prawa krajowego została uchwalona dopiero pod koniec 2024 roku[16].

Zadania obrony cywilnej

Zgodnie z zapisami protokołu dodatkowego do Konwencji genewskich, „obrona cywilna" oznacza wypełnianie wszystkich lub niektórych zadań humanitarnych wymienionych w artykule 61. Zadania te mają na celu „ochronę ludności cywilnej przed niebezpieczeństwami wynikającymi z działań zbrojnych lub klęsk żywiołowych i przezwyciężanie ich bezpośrednich następstw, jak też zapewnienie warunków koniecznych do przetrwania"[17]. Zadania obrony cywilnej obejmują znacznie szerszy zakres działań niż tylko ratownictwo. Należą bowiem do nich: służba ostrzegawcza, ewakuacja, przygotowanie i organizowane schronów, obsługa środków zaciemnienia, ratownictwo, służby medyczne (włączając w to pierwszą pomoc oraz opiekę religijną), walka z pożarami, wykonywanie i oznaczanie stref niebezpiecznych, odkażanie i inne podobne działania ochronne, dostarczanie doraźnych pomieszczeń i zaopatrzenia, doraźna pomoc dla przywrócenia i utrzymania porządku w strefach dotkniętych klęskami, doraźne przywrócenie działania niezbędnych służb użyteczności publicznej, doraźne grzebanie zmarłych, pomoc w ratowaniu dóbr niezbędnych dla przetrwania, dodatkowe rodzaje działalności (niezbędne dla wypełnienia któregoś z zadań wyżej wymienionych, w tym planowanie i prace organizacyjne)[18].

Niemniej edukacja w XXI wieku i w dobie działań hybrydowych nabiera nowego znaczenia dla obrony cywilnej. Oddziaływania w sferze psychologicznej i informacyjnej na cywilów były prowadzone od początku historii wojen, ale obecny postęp technologiczny przysporzył sposobów i możliwości

[15] Ibidem, pkt 2.6.

[16] Ustawa z dnia 5 grudnia 2024 r. *o ochronie ludności i obronie cywilnej* (Dz.U. 2024 poz. 1907).

[17] Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r.*, dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych* (Protokół I), oraz Protokół dodatkowy do Konwencji Genewskich z dnia 12 sierpnia 1949 r., *dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych* (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r. (Dz.U. 1992, nr 41, poz. 175), art. 61.

[18] Ibidem, art. 61.

oddziaływania na ludność cywilną w znacznie większym zakresie. W tych warunkach działalność edukacyjna prowadzona w ramach obrony cywilnej musi wybiegać poza tradycyjnie wyznaczone ramy. Oprócz przekazywania wiedzy i nauczania praktycznych umiejętności, jak zachować się w czasie zagrożeń będących wynikiem prowadzonych działań zbrojnych, awarii technicznych lub klęsk żywiołowych, działania edukacyjne muszą uwzględniać konieczność ochrony informacji o znaczeniu militarnym. Ponadto powinny przyczyniać się do wzmocnienia odporności na wrogie oddziaływania informacyjne, które mogą m.in. propagować nieprawdziwe komunikaty i treści mające na celu dyskredytowanie władz publicznych, kluczowych dowódców oraz Sił Zbrojnych RP. Przeciwnik może próbować podburzać środowiska cywilne i wojskowe do protestów i aktów nieposłuszeństwa wobec władz wojskowych i publicznych obniżając jednocześnie zdolności obronne i ochronne państwa.

Jednym z wyżej wymienionych zadań obrony cywilnej jest ewakuacja ludności. Należy jednak podkreślić, że w czasie wojny należałoby ją prowadzić w sposób ograniczający gromadzenie się osób oczekujących w okolicy głównych węzłów komunikacyjnych[19]. Mogłyby one stać się celem ataków przeciwnika. Niemniej podmioty obrony cywilnej zmuszone będą zapewnić ludziom warunki do przetrwania nie tylko w czasie ewakuacji, ale i w nowym miejscu bytowania, co wiąże się z licznymi wyzwaniami.

Oceniając obecny stan przygotowań obrony cywilnej należy wskazać, że wiele organizacji pozarządowych nie ma jeszcze przypisanych zadań na czas wojny. Te zadania dopiero należało będzie im przypisać, biorąc pod uwagę, że w obronie cywilnej występują określone specjalności.

System wykrywania, powiadamiania, ostrzegania i alarmowania o zagrożeniach

Bez wątpienia osiągnięcie wysokiej sprawności funkcjonalnej systemu wykrywania, powiadamiania, ostrzegania i alarmowania o zagrożeniach wymaga współpracy wielu podmiotów, które już w czasie pokoju powinny dysponować wszelkimi niezbędnymi zdolnościami. W związku z powyższym należy wykorzystać siły i środki pozostające w dyspozycji administracji

[19] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), art. 122.

publicznej, służb, przedsiębiorców, organizacji pozarządowych, nadawców programów radiowych i telewizyjnych oraz Sił Zbrojnych RP, które dysponują największymi możliwościami wykrywania zagrożeń. To właśnie Minister Obrony Narodowej może uruchomić krajowy system wykrywania skażeń i alarmowania, (KSWSiA)[20]. W skład tego systemu wchodzą: system wykrywania skażeń Sił Zbrojnych Rzeczypospolitej Polskiej, sieci i systemy nadzoru epidemiologicznego i kontroli chorób zakaźnych[21], system stacji wczesnego wykrywania skażeń promieniotwórczych i placówek prowadzących pomiary skażeń promieniotwórczych[22], wojewódzkie systemy wykrywania i alarmowania oraz systemy wczesnego ostrzegania ludności[23], systemy nadzoru epizootycznego, fitosanitarnego, nadzoru nad bezpieczeństwem produktów pochodzenia zwierzęcego i paszami oraz nadzoru nad produktami rolno-spożywczymi[24,25].

W skład systemu powiadamiania, ostrzegania i alarmowania mogą wchodzić m.in. syreny alarmowe i urządzenia nagłaśniające, krajowe, regionalne i lokalne systemy ostrzegania, jak np. kanały nadawców programów radiowych i telewizyjnych, Regionalny System Ostrzegania (RSO), system ALERT RCB, środki dystrybucji informacji należące do wydawców dzienników, technologie cyfrowe, serwisy informacyjne oraz Internet[26]. Cały czas jednak dużym wyzwaniem pozostaje osiągnięcie wysokiej skuteczności systemów alarmowych poprzez włączenie do zautomatyzowanego systemu syren i urządzeń nagłaśniających pozostających w dyspozycji administracji publicznej, służb, przedsiębiorców oraz organizacji pozarządowych, które gotowe są włączyć do tego systemu własne urządzenia.

---

[20] Rozporządzenie Rady Ministrów z dnia 23 lutego 2024 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach (Dz.U. 2024 poz. 290), § 3, pkt 1, ppkt 4.

[21] Nadzorowane przez ministra właściwego do spraw zdrowia.

[22] Ich działania koordynuje Prezes Państwowej Agencji Atomistyki.

[23] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122 z późn. zm.), art. 16 ust. 2 pkt 3.

[24] Nadzorowane przez ministrów właściwych do spraw rolnictwa i rynków rolnych oraz zdrowia.

[25] Rozporządzenie Rady Ministrów z dnia 23 lutego 2024 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach (Dz.U. 2024 poz. 290), § 4 pkt 1.

[26] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), art. 71.1.

Jak pokazują doświadczenia wojny w Ukrainie, czyli wojny najbardziej zbliżonej w swoim przebiegu do wojny, która potencjalnie mogłaby wybuchnąć na terytorium Rzeczypospolitej Polskiej, kluczowym jest system powszechnego ostrzegania wojsk oraz ludności o zagrożeniu z powietrza. Osiągnięcie wysokiej sprawności funkcjonalnej tego systemu jest kluczowe ze względów bezpieczeństwa. W tym kontekście współpraca cywilno-wojskowa stanowi niezwykle istotny czynnik w przeciwstawianiu się zagrożeniom godzącym zarówno w bezpieczeństwo obywateli, jak i instytucji państwa. Niezbędnym więc jest wyposażenie poszczególnych cywilnych ogniw alarmowania i ostrzegania w urządzenia do prowadzenia nasłuchu komunikatów radiowych o zagrożeniach z powietrza. Od skuteczności przekazywania sygnałów przez te ogniwa zależeć będzie skuteczność systemów na poziomie funkcjonowania administracji publicznej. Niemniej znajomość zasad zachowania się po usłyszeniu sygnału jest wypadkową skuteczności systemu szkolenia ludności cywilnej.

Organizacja obrony cywilnej

Zgodnie z zapisami ujętymi we wstępie protokołu dodatkowego do Konwencji genewskich z dnia 12 sierpnia 1949 r., dotyczącego ochrony ofiar międzynarodowych konfliktów zbrojnych „Wysokie Umawiające się Strony" wyraziły wolę, aby między narodami panował pokój. Podkreśla się także obowiązek powstrzymania się od użycia siły, a nawet samej groźby jej użycia przeciwko suwerenności, integralności terytorialnej lub niezawisłości politycznej innego państwa (w sposób niezgodny z celami Narodów Zjednoczonych) w stosunkach międzynarodowych[27]. Niemniej mimo wyrażenia woli dążenia do pokoju między narodami, jak pokazują doświadczenia praktyczne, wojna pozostaje jednym z narzędzi osiągania celów. W związku z powyższym niezbędnym jest stworzenie warunków do przetrwania ludności cywilnej w czasie wojny lub konfliktu zbrojnego. Zorganizowanie efektywnie działającego systemu ochrony ludności i obrony cywilnej bez wątpienia wymaga interwencji instytucji państwa. W pierwszej kolejności niezbędnym jest stworzenie stosownych podstaw prawnych na gruncie prawa międzynarodowego oraz krajowego.

[27] Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r..., dz. cyt.

Od niedawna na gruncie prawa krajowego funkcjonowanie obrony cywilnej i powszechnej samoobrony reguluje ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej[28] oraz akty wykonawcze do niej. Bez wątpienia prace nad aktami prawnymi na gruncie prawa krajowego zostały przyśpieszone w związku z eskalacją wojny w Ukrainie, czyli kraju graniczącego z Rzeczpospolitą Polską. Wojna ta wpłynęła na środowisko bezpieczeństwa Polski i unaoczniła zagrożenia ludności cywilnej. Niemniej uchwalenie powyższej ustawy nie stanowi wystarczającej podstawy prawnej regulującej całościowo funkcjonowanie obrony cywilnej na gruncie prawa krajowego. Akty wykonawcze do tej ustawy będą pełniły bardzo ważną rolę w prawnym uregulowaniu całościowego funkcjonowania obrony cywilnej. Przepisy te mają z założenia przyczynić się do zapewnienia warunków i możliwości sprawnego działania.

Istotnym postanowieniem ww. ustawy jest to, że „z chwilą wprowadzenia stanu wojennego i w czasie wojny:

- ochrona ludności staje się obroną cywilną,
- organy ochrony ludności stają się organami obrony cywilnej,
- podmioty ochrony ludności stają się podmiotami obrony cywilnej,
- zasoby ochrony ludności stają się zasobami obrony cywilnej”[29].

Jednocześnie zgodnie z zapisami ustawy organami ochrony ludności są organy administracji publicznej. Obrona cywilna funkcjonuje w oparciu o organy, podmioty oraz zasoby stworzone już w czasie pokoju. Jednocześnie ustawa nie odnosi się do kwestii zarządzania kryzysowego oraz stanów nadzwyczajnych. Ta materia jest uregulowana w obecnie obowiązujących ustawach. Będą one obowiązywały także w czasie wojny. Innymi słowy, zarządzanie kryzysowe w określonych sytuacjach będzie prowadzone także w czasie wojny na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2023 poz. 122 z późn. zm.). Doświadczenia praktyczne dowodzą, że w czasie wojny często mamy do czynienia z koniecznością „zarządzania

[28] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907).

[29] Ibidem, art. 2.3.

kryzysowego”[30] ze względu na występowanie dużej liczby „sytuacji kryzysowych”[31] związanych z nieadekwatnością posiadanych sił i środków.

Analiza zapisów ustawy pozwala wyodrębnić filary ochrony ludności i obrony cywilnej. Należy do nich system monitorowania zagrożeń oraz powiadamiania, ostrzegania i alarmowania ludności. Filarami są także ewakuacja, przyjęcie ludności oraz organizowanie miejsc ich doraźnej dyslokacji, budowanie i doprowadzanie do stanu używalności już istniejących schronów[32] i ukryć[33] dla ludności oraz ich ewidencja i utrzymanie. Kolejnymi filarami są: wzmacnianie społecznej odporności m.in. poprzez powszechną samoobronę oraz organizowanie szkoleń, gromadzenie zasobów, budowanie struktur ochrony ludności i obrony cywilnej na różnych szczeblach administracji publicznej, a także funkcjonowanie ochrony ludności w czasie wojny. Ostatnim kluczowym filarem jest finansowanie ochrony ludności i obrony cywilnej, bez którego zapisy ustawowe nie znalazłyby zastosowania w praktyce.

Dla funkcjonowania obrony cywilnej kluczowym jest, że w czasie wojny zachowuje ona neutralność zbrojną. Jej zadaniem jest pomoc ludności cywilnej zarówno na terenach będących pod kontrolą własnego państwa, jak i na terenach zajętych przez nieprzyjaciela. Niemniej w okresie wojny

[30] Zgodnie z ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2023 poz. 122 z późn. zm.), art. 2:
„Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej”.

[31] Ibidem, art. 3:
„sytuacji kryzysowej – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków”.

[32] Zgodnie z ustawą z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), art. 83.3.: „Schron to uznany za budowlę ochronną obiekt budowlany albo część obiektu budowlanego o konstrukcji zamkniętej i hermetycznej, wyposażony w urządzenia filtrowentylacyjne lub pochłaniacze regeneracyjne”.

[33] Ibidem, art. 83.4.: „Ukrycie to uznany za budowlę ochronną obiekt budowlany albo część obiektu budowlanego o konstrukcji niehermetycznej”.
Art. 84.: „Miejsca doraźnego schronienia to obiekty zbiorowej ochrony będące obiektami budowlanymi, przystosowane do tymczasowego ukrycia ludzi, organizowane na zasadach określonych w art. 102”.

„organizacje obrony cywilnej”[34], a także formacje utworzone przez władze do wypełniania zadań wymienionych w art. 61 pkt (a)[35]mających na celu ochronę ludności cywilnej, posiadają prawo do ochrony. Innymi słowy, organizacje te nie powinny być celem ataków. Niemniej ochrona ustaje w przypadku określonym w artykule 65 Konwencji: „Ustanie ochrony ust. 1. Ochrona, do jakiej mają prawo cywilne organizacje obrony cywilnej, ich personel, budynki, schrony oraz ich materiały, może ustać tylko w wypadku prowadzenia działań szkodliwych dla nieprzyjaciela lub wykorzystywania ich, poza ich właściwymi zadaniami, do takich działań. Jednakże ochrona ustanie jedynie wtedy, gdy ostrzeżenie ustalające, jeśli to jest celowe, uzasadniony termin pozostanie nieskuteczne”[36,37]. Natomiast artykuł 51, ust. 3 stanowi, że osoby cywilne nie mają prawa do korzystania z ochrony określonej Konwencją, jeśli bezpośrednio uczestniczą w działaniach zbrojnych, przez cały czas trwania tego uczestnictwa[38].

W kontekście funkcjonowania obrony cywilnej należy pamiętać o budowaniu jej odporności na zakłócenia w komunikacji. Przeciwnik bowiem będzie skupiał wysiłek na obezwładnianiu i dezorganizacji systemów dowodzenia, łączności oraz transmisji danych. W związku z powyższym, kluczowy element dla koordynacji działań, dowodzenia i zarządzania, może i z dużą dozą pewności zostanie porażony, również w odniesieniu do funkcjonowania obrony

[34] Zgodnie z protokołami dodatkowymi do Konwencji genewskich z 12 sierpnia 1949 r…, dz. cyt., art. 61(b):
(b) określenie „organizacje obrony cywilnej” obejmuje obiekty oraz formacje utworzone przez uprawnione władze strony konfliktu lub działające z ich upoważnienia dla wypełnienia któregokolwiek z zadań wymienionych w punkcie (a) i wyznaczone wyłącznie do tych zadań;

[35] Ibidem, art. 61(a):
(a) określenie „obrona cywilna” oznacza wypełnianie wszystkich lub niektórych zadań humanitarnych wymienionych niżej, mających na celu ochronę ludności cywilnej przed niebezpieczeństwami wynikającymi z działań zbrojnych lub klęsk żywiołowych, i przezwyciężanie ich bezpośrednich następstw, jak też zapewnienie warunków koniecznych do przetrwania. Są to następujące zadania: […].

[36] Ibidem, art. 65 ust. 1.

[37] Ibidem, art. 61(c):
(c) określenie „personel” organizacji obrony cywilnej obejmuje osoby, które strona konfliktu zatrudnia wyłącznie do wykonywania zadań wyliczonych w punkcie (a), w tym personel wyznaczony przez uprawnioną władzę tej strony wyłącznie do zarządzania tymi organizacjami;

[38] Ibidem, art. 51 ust. 3.

cywilnej. W tych warunkach znalezienie zastępczego sposobu zarządzania i koordynacji działań poszczególnych formacji i służb będzie kluczowe dla skuteczności systemu.

Skuteczna ochrona ludności w czasie wojny wymaga stworzenia zasobów, dlatego terytorialne organy ochrony ludności, czyli np. wojewodowie, starostowie, wójtowie, burmistrzowie, prezydenci miast zobowiązani są tworzyć oraz utrzymywać niezbędne zasoby obejmujące m.in. zapasy wody i żywności, zapasowe źródła energii, odzież, środki sanitarne i higieniczne, wyroby medyczne[39]. Istotnym jest, że „wójt (burmistrz, prezydent miasta), starosta oraz wojewoda zapewniają zasoby ochrony ludności niezbędne do wykonywania przez co najmniej 3 dni trwania zagrożenia zadań ochrony ludności i obrony cywilnej…"[40].

Jednoczenie należy pamiętać, że za realizację zadań obrony cywilnej w zakładach pracy odpowiedzialni są ich właściciele lub kierownicy, natomiast organizacje społeczne wykonują zadania obrony cywilnej w zakresie wynikającym z ich statusów.

Rozważając funkcjonowanie obrony cywilnej trzeba podkreślić, że w każdym mieście, gminie czy powiecie będą występowały inne priorytety, niemniej wydaje się, że w większości przypadków kluczowym będzie utrzymanie oraz budowa obiektów zbiorowej ochrony. Ponadto istnieje potrzeba szybkiego stworzenia normatywów wyposażania w sprzęt przeciwchemiczny, jak maski przeciwchemiczne i środki ochrony skóry. Jednak wciąż nie ustalono, jakiemu odsetkowi ludności zapewni się tego rodzaju ochronę.

Rola powszechnej samoobrony

Instytucja państwa jest najważniejszym podmiotem będącym w stanie zapewnić wysoki jakościowo poziom ochrony ludności. Należy jednak pamiętać, że w czasie wojny priorytetowym obszarem działalności państwa oraz władz publicznych stanie się zabezpieczenie potrzeb systemu obronnego[41].

[39] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), art. 33, pkt 1.

[40] Ibidem, art. 33, pkt 3.

[41] W. Kitler, *Funkcjonowanie ludności w warunkach zewnętrznego zagrożenia państwa oraz w czasie wojny. Rozważania prawne i organizacyjne,* [w:] *Funkcjonowanie…*, red. W. Kitler, P. Hac, dz. cyt., s. 272.

Jak pokazują doświadczenia praktyczne w czasie wojny lub konfliktu zbrojnego, należy spodziewać się wystąpienia rozległych zniszczeń infrastruktury logistycznej, drogowo-mostowej, domów mieszkalnych oraz ośrodków przemysłowych. Ponadto występowały będę zakłócenia w funkcjonowaniu administracji publicznej, podczas gdy wiele zdarzeń wymagało będzie realizacji zadań na poziomie zarządzania kryzysowego[42], będącego elementem kierowania bezpieczeństwem narodowym. W tych warunkach zdolność do terminowego świadczenia pomocy ludności dotkniętej sutkami wojny zostanie znacząco ograniczona. Innymi słowy, wielu potrzebujących nie otrzyma niezbędnej pomocy na czas, a w związku z powyższym, olbrzymie znaczenie dla zapewnienia przetrwania obywateli będzie miała powszechna samoobrona. Przygotowanie obywateli do realizacji działań m.in. w ramach powszechnej samoobrony jest rolą państwa. W tym kontekście ważnym jest, że na podstawie ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907) wydano Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 6 lutego 2025 r. w sprawie programów szkoleń z zakresu ochrony ludności i obrony cywilnej oraz wymagań dla podmiotów prowadzących szkolenia[43].

Niemniej państwo nakłada również na obywateli obowiązek zabezpieczenia określonych zasobów i zdolności. Zgodnie z ustawą z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej „W czasie stanu wojennego i w czasie wojny osoby zamieszkujące na obszarze, na którym wprowadzono stan wojenny, albo zamieszkujące strefę bezpośrednich działań wojennych w ramach przygotowania obrony cywilnej zabezpieczają:

1) miejsce zamieszkania oraz mienie osobiste,
2) zapasy własne wody pitnej oraz środków spożywczych,
3) zapasy własne środków sanitarnych, higienicznych oraz medycznych”[44].

[42] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2023 poz. 122 z późn. zm.).

[43] Rozporządzenie Ministra Spraw Wewnętrznych I Administracji z dnia 6 lutego 2025 r. w sprawie programów szkoleń z zakresu ochrony ludności i obrony cywilnej oraz wymagań dla podmiotów prowadzących szkolenia (Dz.U. 2025 poz. 162).

[44] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), art. 121.

W czasie wojny nie można wykluczyć możliwości użycia przez przeciwnika broni CBRN[45] w przestrzeni publicznej. Szkolenia z zakresu zabezpieczenie się przed zagrożeniami CBRN, Bojowymi Środkami Trującymi[46] oraz HazMat[47] stanowią ważny obszar problemowy edukacji. Ataki środkami walki przenoszącymi broń chemiczną lub ataki na zakłady przemysłowe, w których przetwarza się niebezpieczne dla zdrowia i życia ludzi toksyczne środki przemysłowe, mogą doprowadzić do powstania rozległych stref skażeń. W takich przypadkach szybka ewakuacja lub zdolność zabezpieczenia mieszkania przed przedostaniem się tych środków do pomieszczeń, w których przebywają ludzie mogą okazać się kluczowe dla przetrwania. Jednocześnie, jak pokazują doświadczenia praktyczne, kluczowym dla zwiększenia bezpieczeństwa ludności cywilnej jest posiadanie wiedzy i umiejętności postępowania podczas zagrożenia z powietrza.

Należy zwrócić uwagę, że w czasie wojny wykrywanie prób dywersji, zbierania informacji na rzecz obcych sił zbrojnych oraz sabotażu staje się ważnym aspektem wzmacniania odporności na działania przeciwnika. W związku z powyższym w ramach powszechnej samoobrony należy uwzględniać szkolenie obywateli w zakresie identyfikacji osób i zdarzeń potencjalnie niebezpiecznych.

Podsumowanie

Zapewnienie przetrwania ludności w czasie wojny jest kluczowym obowiązkiem państwa. Tylko instytucja państwa jest w stanie zapewnić optymalne i synergiczne wykorzystanie zasobów umożliwiających osiągnięcie tego celu. To określone przez władze państwowe ramy strategiczne polskiego bezpieczeństwa kształtowały funkcjonowanie ochrony ludności i obrony cywilnej w Polsce. Należy jednak stwierdzić, że obecnie stan przygotowania obrony cywilnej i powszechnej samoobrony do funkcjonowania w czasie wojny jest niezadowalający. Od dawna wyczekiwana ustawa o ochronie ludności i obronie

[45] Akronim utworzony od pierwszych liter angielskich słów chemical, biological, radiological, and nuclear odnoszące się do zagrożeń chemicznych, biologicznych, radiacyjnych i nuklearnych.

[46] https://encyklopedia.pwn.pl/haslo/bojowe-srodki-trujace;3879123.html, [dostęp: 21.04.2025]. Hasło: *Bojowe środki trujące, BŚT, związki chemiczne o dużej toksyczności, które użyte na polu walki mogą wywołać u ludzi zatrucia, śmierć lub mieć działanie obezwładniające;*

[47] Z języka angielskiego „hazardous materials".

cywilnej została uchwalona dopiero pod koniec 2024 r. Obecnie tworzone są ważne akty wykonawcze do tej ustawy, które będą szczegółowo regulowały funkcjonowanie obrony cywilnej na gruncie prawa krajowego. Jednocześnie wciąż oczekujemy na możliwość skorzystania ze środków finansowych przewidzianych w ustawie.

Jednym z najistotniejszych elementów obrony cywilnej jest funkcjonowanie systemu wykrywania, powiadamiania, ostrzegania i alarmowania o zagrożeniach. Aby osiągnąć wysoką skuteczność systemu alarmowego należy go m.in. zautomatyzować oraz włączyć do niego urządzenia nagłaśniające pozostające w dyspozycji administracji publicznej, służb, przedsiębiorców oraz organizacji pozarządowych.

Należy wziąć pod uwagę, że wobec zagrożeń i zniszczeń będących efektem potencjalnej wojny, nie zawsze będzie istniała możliwość udzielenia pomocy osobom jej potrzebującym. W tym przypadku powszechna samoobrona będzie stanowiła bardzo ważny element wzmacniania i tworzenia odporności ludności cywilnej na zagrożenia wojenne.

Uzasadnionym jest twierdzić, że system obrony cywilnej wymaga dalszego doskonalenia funkcjonowania zarówno swoich organów, jak i podmiotów oraz przygotowania adekwatnych do zagrożenia zasobów niezbędnych dla przetrwania ludności.

Literatura

1. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2013.
1. Encyclopedia PWN, https://encyklopedia.pwn.pl/haslo/bojowe-srodki-trujace;3879123.html
2. Informacja o wynikach kontroli. *Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej,* KPB.430.009.2017, Nr ewid. 147/2018/P/17/039/KPB, Najwyższa Izba kontroli, Departament Porządku i Bezpieczeństwa Publicznego, Warszawa 2018.
3. Kitler W., Hac P. (red.), *Funkcjonowanie państwa w warunkach zewnętrznego zagrożenia państwa i w czasie wojny*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2022.
4. Koziej S., *Obronność Polski w warunkach samodzielności strategicznej lat 90. XX wieku*, Bezpieczeństwo Narodowe, nr 21, s. 25-26, 2012.
5. Kupiecki R. (red. nauk.), *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej pierwsze 25 lat*, Wojskowe Centrum Edukacji Obywatelskiej im. płk. dypl. Mariana Porwita, Warszawa 2015.

6. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483 z późn. zm.).
7. Protokoły dodatkowe do Konwencji genewskich z 12 sierpnia 1949 r., dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 r. (Dz.U. 1992, nr 41, poz. 175).
8. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 6 lutego 2025 r. w sprawie programów szkoleń z zakresu ochrony ludności i obrony cywilnej oraz wymagań dla podmiotów prowadzących szkolenia (Dz.U. 2025 poz. 162).
9. Rozporządzenie Rady Ministrów z dnia 23 lutego 2024 r. w sprawie systemów wykrywania skażeń i powiadamiania o ich wystąpieniu oraz właściwości organów w tych sprawach (Dz.U. 2024 poz. 290).
10. *Raport dotyczący budowli ochronnych*, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2023.
11. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020.
12. *Strategia Bezpieczeństwa Rzeczypospolitej Polskiej 2014*, Warszawa 2014.
13. Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907).
14. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2023 poz. 122 z późn. zm.).

Karina Dmyterko
Państwowa Wyższa Szkoła Zawodowa w Koszalinie
https://doi.org/10.29316/9788368103205_11

BEZPIECZEŃSTWO LUDNOŚCI CYWILNEJ W POLSCE W KONTEKŚCIE BRAKU MIEJSC SCHRONIENIA PRZED ATAKIEM ZBROJNYM

SECURITY OF THE CIVILIAN POPULATION IN POLAND IN THE CONTEXT OF THE LACK OF PLACES OF REFUGE AGAINST ARMED ATTACK

Streszczenie

Celem rozdziału jest analiza stopnia przygotowania Polski do ochrony ludności cywilnej na wypadek ataku zbrojnego, ze szczególnym uwzględnieniem dostępności miejsc schronienia oraz przewidywanych reakcji społecznych w sytuacji nagłego zagrożenia. W części wprowadzającej opisano podstawy prawne i obowiązki państwa oraz samorządów w zakresie ochrony cywilnej. Kolejna część została poświęcona szczegółowej analizie infrastruktury ochronnej w Polsce, opartej na raportach Najwyższej Izby Kontroli i Państwowej Straży Pożarnej, wskazując na niedobory w liczbie i stanie technicznym schronów. Przykład miasta Kołobrzeg zilustrował, jak niedostateczna infrastruktura może wpływać na realne szanse mieszkańców na przetrwanie. Następnie

Summary

The aim of the chapter is to analyze the degree of Polish preparation to protect civilians in the event of an armed attack, with particular emphasis on the availability of places of refuge and anticipated social reactions in the event of a sudden threat. The introductory part describes the legal basis and obligations of the state and local governments in the field of civil protection. The next part is devoted to a detailed analysis of the protective infrastructure in Poland, based on the reports of the Supreme Audit Office and the State Fire Service, pointing to shortages in the number and technical condition of shelters. The example of the city of Kołobrzeg illustrated how insufficient infrastructure can affect the real chances of survival of residents. It then presents the psychological aspects of how

przedstawiono psychologiczne aspekty reagowania ludzi na ekstremalne zagrożenia, w tym panikę, psychozę i altruizm, analizując zarówno historyczne, jak i współczesne przykłady z Polski i Ukrainy. Ważną częścią rozdziału była także rola percepcji i świadomości sytuacyjnej w podejmowaniu decyzji w warunkach skrajnego stresu. Badania ankietowe przeprowadzone wśród mieszkańców Kołobrzegu ujawniły niski poziom wiedzy o lokalnych miejscach schronienia oraz sygnałach alarmowych. Główna hipoteza zakładała, że niedobór infrastruktury ochronnej oraz brak wystarczającej edukacji społecznej mogą skutkować chaosem i paniką podczas realnego zagrożenia. Wyniki badań oraz analizy pozwoliły wysunąć wniosek, że Polska nie jest odpowiednio przygotowana do ochrony cywilnej w czasie wojny, a poprawę bezpieczeństwa należy oprzeć zarówno na rozwoju infrastruktury schronowej, jak i edukacji społeczeństwa w zakresie reagowania na sytuacje kryzysowe. W pracy wykorzystano metody analizy dokumentów i aktów prawnych, badanie ankietowe oraz studia przypadków i relacje świadków jako metody teoretyczne i badawcze.

Słowa klucze: bezpieczeństwo, panika, percepcja, kryzys, ochrona cywilna, społeczeństwo

people respond to extreme threats, including panic, psychosis, and altruism, analyzing both historical and contemporary examples from Poland and Ukraine. An important part of the chapter was also the role of perception and situational awareness in decision-making under conditions of extreme stress. Surveys conducted among the residents of Kołobrzeg revealed a low level of knowledge about local places of refuge and alarm signals. The main hypothesis was that the lack of protective infrastructure and the lack of sufficient public education could result in chaos and panic during a real threat. The results of the research and analyses led to the conclusion that Poland is not adequately prepared for civil protection during wartime, and the improvement of security should be based on both the development of shelter infrastructure and the education of the public in responding to crisis situations. The paper uses methods of analysis of documents and legal acts, a survey as well as case studies and witness accounts as theoretical and research methods.

Keywords: security, panic, perception, crisis, civil protection, society

Wstęp

Bezpieczeństwo wewnętrzne to stan porządku państwa, polegający na ochronie jego obywateli przed zagrożeniami, mogącymi powstać w tym państwie. Ochrona ta jest wielowymiarowa i obejmuje takie dziedziny życia społecznego jak porządek publiczny i ochrona prawna, ochrona przed szeroko rozumianym terroryzmem, ochrona infrastruktury krytycznej, ochrona granic i kontrolowanie ruchu granicznego, zarządzanie kryzysowe[1]. W zależności

[1] Definicja własna.

od skali zagrożeń w danej dziedzinie, działania państwa intensyfikują się w zakresie danego problemu i jego rozwiązania, na podstawie Ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, w której czytamy: „Art. 2. 1. Ochrona ludności to system składający się z organów administracji publicznej wykonujących zadania mające na celu zapewnienie bezpieczeństwa ludności przez ochronę życia i zdrowia ludzi, mienia, w tym zwierząt, infrastruktury niezbędnej do zaspokojenia potrzeb bytowych, dóbr kultury i środowiska w sytuacji zagrożenia, zwanych dalej „organami ochrony ludności", podmiotów wykonujących te zadania, zwanych dalej „podmiotami ochrony ludności", oraz zasobów ochrony ludności." Wg autorki oznacza to, że wszyscy ludzie znajdujący się w danej chwili w strefie zagrożenia będą ochronieni, a ich potrzeby bytowe na czas zagrożenia będą zaspokojone.

W Art. 4 tej ustawy między innymi czytamy, że organy administracji publicznej są prawidłowo przygotowane do realizacji zadań ochrony ludności i obrony cywilnej, a także ludność jest odpowiednio przygotowana do właściwego reagowania w przypadku wystąpienia zagrożenia, przez posiadanie informacji o potencjalnych i aktualnych zagrożeniach mających wpływ na bezpieczeństwo, edukację w zakresie ochrony ludności i obrony cywilnej, instrukcje ewakuacji, instrukcję przestrzegania bezpieczeństwa oraz zachowania się w sytuacjach zagrożenia, planowaniu i przygotowaniu warunków do ewakuacji ludności, a także miejsc doraźnego schronienia oraz budowli ochronnych. Tym samym ochrona ludności staje się podstawowym obowiązkiem państwa, a priorytetem jest ochrona życia i zdrowia ludzi znajdujących się w strefie wszelkiego zagrożenia przez całodobowy i kompleksowy system ochrony ludności i obrony cywilnej na terenie naszego kraju.

Zawarte w ustawie rozwiązania na rzecz bezpieczeństwa nie mogą wpływać na swobody i prawa obywatelskie, a każdy człowiek powinien mieć zapewniony jednakowy poziom ochrony w czasie pokoju, jak i wojny. System ochrony ludności opiera się na już działających strukturach z wykorzystaniem istniejących zasobów, takich jak potencjał Państwowej Straży Pożarnej, Ochotniczych Straży Pożarnych, struktur zarządzania kryzysowego, systemu powiadamiania ratunkowego, Państwowego Ratownictwa Medycznego oraz organizacji pozarządowych. Nowa ustawa wzmacnia kompetencje samorządów i nakłada nań odpowiedzialność za sprawne działanie systemu bezpieczeństwa przez odpowiedzialność za wykrywanie zagrożeń, ostrzeganie mieszkańców,

organizowanie schronienia i zapewnienie środków ochrony, przygotowanie obrony cywilnej na wypadek wojny lub innych kryzysów[2].

Autorka rozdziału zadała sobie pytanie, czy dzięki temu Polacy są bezpieczniejsi, a Państwo rzeczywiście może skutecznie chronić ludność w razie kryzysu? Próbuje także przewidzieć zachowanie ludzi, w sytuacji nagłego zagrożenia życia i zdrowia w wyniku napaści zbrojnej.

Obiekty ochronne w Polsce

W dniu 13 marca 2024 r. o 7:00 Najwyższa Izba Kontroli (NIK), opublikowała artykuł podsumowujący kontrolę pod kątem zapewnienia przez Państwo obywatelom miejsc schronienia w budowlach ochronnych na wypadek wystąpienia zagrożenia pod tytułem: „W schronie się nie schronisz”[3]. Postawiono jedno główne pytanie definiujące cel kontroli: „Czy kontrolowane jednostki stworzyły właściwe warunki do rozwoju budownictwa ochronnego i zapewniły mieszkańcom wystarczającą liczbę odpowiednich i bezpiecznych miejsc schronienia i ukrycia w razie wystąpienia zagrożenia?”.

W ocenie ogólnej czytamy, że NIK negatywnie oceniła projekt Ministerstwa Spraw Wewnętrznych i Administracji dotyczący obrony cywilnej i budownictwa ochronnego z powodu braku aktów prawnych regulujących obszar obrony cywilnej i budownictwa ochronnego, co było przyczyną dalszych braków podstaw prawnych dla samorządów do finansowania budowy, modernizacji i utrzymania infrastruktur budowli ochronnych. Kontrolowane jednostki nie wykazały poniesionych kosztów związanych z budową, modernizacją czy utrzymaniem budowli ochronnych, co spowodowało degradację już istniejących budynków lub całkowite ich zburzenie.

Powszechnie nie stosowano się także do wytycznych z 4 grudnia 2018 r. w sprawie zasad postępowania z zasobami budownictwa ochronnego, co należało do Komendanta Głównego Państwowej Straży Pożarnej, wojewodów, starostów, wójtów lub burmistrzów, prezydentów miast, Szefa Obrony Cywilnej Kraju oraz szefów obrony cywilnej województw, powiatów i gmin. Z tego

[2] Ustawa o ochronie ludności i obronie cywilnej z dnia 05.12.2024 r. (Dz. U. z 2024 r. poz. 1907).

[3] *W schronie się nie schronisz,* Raport Najwyższej Izby Kontroli z 13 marca 2024, https://www.nik.gov.pl/najnowsze-informacje-o-wynikach-kontroli/budowle-ochronne-miejsca-ukrycia.html, [dostęp: 25.04.2025].

powodu negatywnie oceniono istniejące warunki bytowania w miejscach schronienia przeznaczonych na czas zagrożenia, ze względu na brak wystarczającej ilości miejsc schronienia w budowlach ochronnych.

Należy jednak zaznaczyć, iż najnowsza Ustawa o ochronie ludności i obronie cywilnej, która weszła w życie 1 stycznia 2025 r., daje podstawy prawne do budowania nowych obiektów, w tym schronów, utrzymania oraz modernizacji istniejących obiektów ochrony ludności na czas zagrożenia, jednak nie zobowiązuje do organizacji schronów i miejsc schronienia dla całej populacji. W art. 90 ustawy czytamy, że organy samorządowe planują niezbędną ilość miejsc schronienia z uwzględnieniem liczby ludności i rodzaju zagrożenia, jednak pojemność budowli ochronnych to:

- w granicach administracyjnych miast dla co najmniej 50% ludności, w tym w budowlach ochronnych dla co najmniej 25 %,
- poza granicami administracyjnymi miast we wszystkich obiektach zbiorowej ochrony dla co najmniej 25 %, w tym w budowlach ochronnych dla co najmniej 15 %.

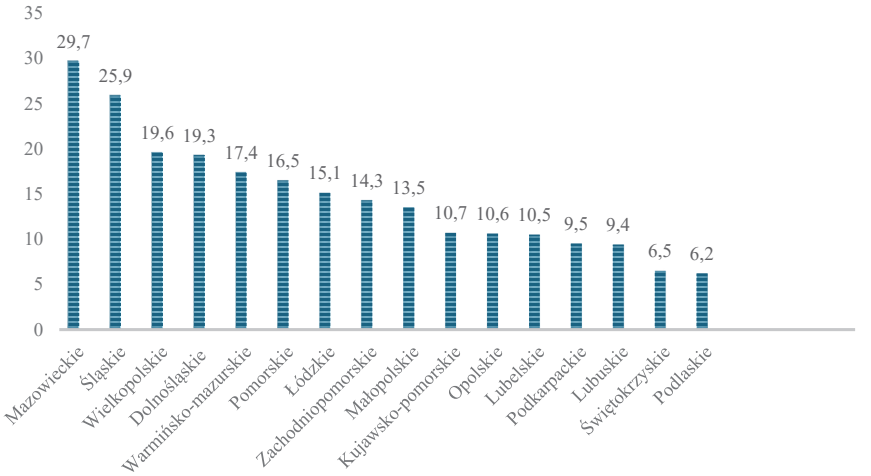
Art. 83. 1 definiuje czym są obiekty zbiorowej ochrony. Obiekt budowlany lub jego wyznaczona część może spełniać swoją rolę ochronną, po ocenie przez właściwy organ ochrony ludności, po uzgodnieniu porozumienia z zarządcą budynku. Taki budynek musi zostać skategoryzowany jako schron, miejsce ukrycia lub miejsce doraźnego ukrycia po zatwierdzeniu kategorii odporności budynku.

- Schronem (S) nazywamy obiekt lub jego część, który charakteryzuje się zamkniętą i hermetyczną konstrukcją budowlaną i jest wyposażony w urządzenia filtrowentylacyjne lub pochłaniacze regeneracyjne, zapewniające powietrze.
- Miejsce ukrycia (U) jest budowlą bez konstrukcji hermetycznej, służącą ochronie ludności, zasobów materiałowych, dóbr materialnych przed rażeniem i mogą to być garaże podziemne, stacje metra czy piwnice.
- Miejsca doraźnego schronienia (MDS) to obiekty budowlane, które tylko czasowo mają zapewnić bezpieczeństwo ludzi i tworzyć zabezpieczenie przed ekstremalnymi zjawiskami pogodowymi. Są to najczęściej piwnice, kościoły, szkoły czy garaże podziemne.

W 2022 r. wiceminister spraw wewnętrznych i administracji, wydał ustnie zamiast pisemnie polecenie przeprowadzenia w Polsce inwentaryzacji

budowli ochronnych skierowane do Państwowej Straży Pożarnej (PSP). W 2023 r. PSP na podstawie wytycznych szefa Obrony Cywilnej Kraju z 4 grudnia 2018 r. w sprawie zasad postępowania z zasobami budownictwa ochronnego, złożyła raport dotyczący budowli ochronnych. W terminie od października 2022 r. do lutego 2023 r., PSP jako służba przeznaczona do działań kryzysowych w ramach działań prewencyjnych zinwentaryzowała obiekty na terenie całego kraju w ramach tzw. rozpoznania operacyjnego. Skupiono się przede wszystkim na miejscach doraźnego schronienia (MDS), które mają chronić ludność w sytuacji ekstremalnych zjawisk przyrodniczych, ale inwentaryzacji podlegały także miejsca ukrycia (U) oraz schrony cywilne (S), zgodnie z definicją ujętą w konwencji genewskiej.

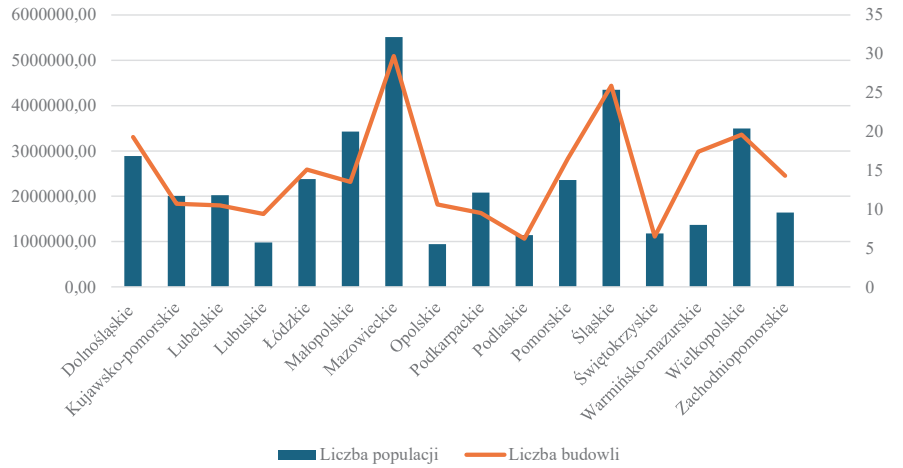
PSP zbadała pod względem technicznym i zewidencjonowała 234735 obiektów budowlanych na terenie kraju. W województwie mazowieckim odnotowano największą ilość obiektów: 29,7 tys., a następnie w województwie śląskim: 25,9 tys. Najmniejsza liczba budowli ochronnych przypadła na województwo podlaskie i było to 6,2 tys. Łączna powierzchnia budowli ochronnych, mogących służyć do doraźnej ochrony wyniosła 74 mln m².



Rysunek 1. Liczba zinwentaryzowanych obiektów ochronnych w Polsce 2023 wg województw, na podstawie danych Raportu Komendy Głównej Państwowej Straży Pożarnej dotyczącego budowli ochronnych. Wartości wyrażone w tysiącach

Źródło: Raport dotyczący budowli ochronnych 2023, Komenda Główna Straży Pożarnej.

Wg Głównego Urzędu Statystycznego (GUS), liczba ludności w Polsce w roku 2023 wynosiła 37mln. 637 tys. osób, a gęstość zaludnienia wynosi 120 osób na 1 km2[4]. Najwięcej dostępnych w Polsce schronień jest Miejsc Doraźnego Ukrycia (MDS), jest to 224 113. Te obiekty pomieszczą 49 mln osób, co przekracza liczbę ludności o 30%. Najwięcej tego typu miejsc znajduje się w piwnicach budynków żelbetonowych i jest to 87 tys. Piwnice budynków z wielkiej płyty stanowią doraźne schronienie dla 67 tys. osób[5]. Jednak MDS to jedynie doraźne, tymczasowe rozwiązanie, głównie w sytuacji katastrofy naturalnej.



Rysunek 2. Liczba ludności w Polsce 2023 r. wg województw

Źródło: opracowanie na podstawie danych Głównego Urzędu Statystycznego w porównaniu do liczby budowli ochronnych.

Bezpieczeństwo w czasie kryzysu i wojny

W związku z niedostateczną ilością schronów i miejsc ukrycia dla całej populacji naszego kraju, należy przyjąć ryzyko, że zapewnienie bezpieczeństwa pozostanie we własnym zakresie. W Poradniku na czas kryzysu i wojny czytamy, jak odróżnić kryzys od wojny. Wg autora/autorów „kryzys to zdarzenie nagłe, które zagraża życiu, zdrowiu, mieniu lub środowisku człowieka.

[4] Główny Urząd Statystyczny *Powierzchnia i ludność w przekroju terytorialnym w 2023 r.* Warszawa 2023

[5] *Raport dotyczący budowli ochronnych 2023,* Komenda Główna Straży Pożarnej, Warszawa 2023.

Przeciwstawienie się mu wymaga sił i środków przekraczających standardowe możliwości i oznacza zmaganie się, walkę, w której konieczne jest działanie pod presją czasu. To punkt zwrotny do zmiany na lepsze lub gorsze". Natomiast „Wojna to zorganizowany konflikt zbrojny między państwami, narodami lub grupami etnicznymi, religijnymi i społecznymi. Brak jest jednak jednoznacznej, powszechnie uznanej definicji wojny. Współczesne definicje nie uznają jej za zjawisko czysto militarne, lecz łączące obszary polityki wewnętrznej i zagranicznej, gospodarki, działań militarnych oraz informacyjnych". Postępowanie w obu przypadkach jest podobne. Między innymi należy wyznaczyć bezpieczne miejsce w domu, w miejscu pracy lub w budynku, w którym przebywamy. Miejsce to powinno być z dostępem do świeżego powietrza, najlepiej bez okien. W poradniku nie ma informacji o schronach i miejscach ukrycia, mimo że poradnik traktuje o zachowaniu podczas wybuchu czy strzelaniny. W poradniku znajdują się informacje na temat sygnałów dźwiękowych oznaczających alarm oraz jego odwołanie[6].

Umiejętność prawidłowego rozpoznania sygnałów jest kluczowa w ocenie zagrożenia, co przekłada się na odporność społeczną w sytuacji kryzysowej lub wojny. Pozwala na zminimalizowanie paniki oraz szybkie podjęcie działań prewencyjnych. Społeczeństwo, które potrafi rozpoznać sygnały alarmowe i prawidłowo podjąć działania prewencyjne ma większe szanse na przetrwanie. Prawidłowo przebiegająca komunikacja między obywatelami a rządem zmniejsza poziom chaosu oraz ryzyko propagandy informacyjnej wroga. Ludność szybko się zaadoptuje do nowych warunków przez zrozumiałe komunikaty, które wszędzie oznaczają to samo, przez co zwiększy się odporność społeczna. Prawidłowe rozumienie sygnałów przez jak największą liczbę osób umożliwia wczesne ostrzeganie i szybkie korzystanie z infrastruktury bezpieczeństwa, co odgrywa kluczową rolę w ograniczaniu strat w ludziach.

Miasto Kołobrzeg jako przykład braku ochrony cywilnej

Autorka rozdziału za pośrednictwem mediów społecznościowych zadała mieszkańcom miasta Kołobrzeg, w którym mieszka, trzy poniższe pytania:

[6] *Bądź gotowy! Poradnik na czas wojny i kryzysu* 2022, Rządowe Centrum Bezpieczeństwa, https://www.gov.pl/web/rcb/badz-gotowy--poradnik-na-czas-kryzysu-i-wojny, [dostęp: 27.04.2025].

1. Czy znasz miejsce schronienia w okolicy Twojego domu, w razie zagrożenia atakiem zbrojnym?
2. Czy znasz adresy schronów w Kołobrzegu?
3. Czy potrafisz rozpoznać dźwiękowe sygnały alarmowe?

42 użytkowników portalu społecznościowego i mieszkańców Kołobrzegu, przystąpiło do ankiety dobrowolnie udzielając odpowiedzi: tak lub nie. Na pytanie pierwsze: „czy znasz miejsce schronienia w okolicy Twojego domu, w razie zagrożenia atakiem zbrojnym?" 6 osób odpowiedziało twierdząco, a 36 osób udzieliło negatywnej odpowiedzi. Na pytanie drugie: „czy znasz adresy schronów w Kołobrzegu?" 4 osoby odpowiedziały: tak, natomiast 38 osób odpowiedziało: nie. (w Kołobrzegu znajdują się jedynie dwa schrony: przy ul. Unii Lubelskiej, mogący pomieścić 140 osób, jednak jego stan techniczny wymaga poprawy, oraz przy ul. Ratuszowej 13, czyli w piwnicach Urzędu Miasta Kołobrzeg, przeznaczony dla 70 osób). W odpowiedzi na trzecie pytanie: „czy potrafisz rozpoznać dźwiękowe sygnały alarmowe?" uzyskano najwięcej potwierdzających odpowiedzi, i było to 12 osób, 30 ankietowanych nie potrafi rozpoznać dźwiękowych sygnałów alarmowych. Autorka nie zdecydowała się zapytać o wiek ani status społeczny ankietowanych celowo, uznając sytuację zagrożenia atakiem zbrojnym, jako ogólnie zagrożenie dla populacji miasta Kołobrzeg, bez względu na wiek, status i stan wiedzy.

Wg raportu NIK wynika, że populacja miasta Kołobrzeg w roku 2023 wynosiła 40543 osób a dostępna liczba miejsc w budowlach ochronnych to 210 miejsc. W przypadku Kołobrzegu miejsce schronienia znajdzie zaledwie 0,52% osób[7]. Kołobrzeg nie jest odosobnionym miejscem w tak złej sytuacji stanu obrony cywilnej. Jak wynika z raportu NIK w ubiegłych latach Obroną Cywilną zarządzało 48 szefów i żaden z nich nie zabezpieczył żadnej budowli ochronnej w celu przystosowania do stanowiska kierowania obroną cywilną[8]. Z raportu PSP po inwentaryzacji budowli ochronnych wynika, że w Polsce jest 10622 – schronów i ukryć dla 1428369 obywateli, oznacza to, że schronienie znajdzie jedynie 3,78% populacji całego kraju. Do informacji publicznej

[7] Dane na podstawie inwentaryzacji budowli ochronnych w Kołobrzegu, przeprowadzonej przez PSP Kołobrzeg w ramach działań Komendy Głównej Straży Pożarnej do Raportu dotyczącego budowli ochronnych 2023.

[8] *W schronie się nie schronisz,* Raport Najwyższej Izby Kontroli z 13 marca 2024, https://www.nik.gov.pl/najnowsze-informacje-o-wynikach-kontroli/budowle-ochronne-miejsca-ukrycia.html, [dostęp: 27.04.2025].

podano skróconą wersję raportu, bez kluczowej informacji, że to nie PSP ponosi odpowiedzialność za stan obiektów, oraz ile osób znajdzie w nich schronienie podczas konfliktu o charakterze zbrojnym. Kontrola NIK ujawniła także, że dane w raporcie PSP są nierzetelne, ponieważ spisano również takie obiekty, które są dla ludności faktycznie niedostępne[9].

Miasto Kołobrzeg jest szczególnym miejscem ze względu na swoje walory turystyczne. Według danych GUS, w 2024 r. w miesiącach lipcu i sierpniu ze wszystkich miejscowości nadmorskich najwięcej noclegów turystom udzielono w Kołobrzegu i było to 967,8 tys., co stanowiło ponad 1/10 wszystkich noclegów udzielonych w obszarze nadmorskim. Z noclegów skorzystało 183,6 tys. osób. W przeliczeniu na 100 mieszkańców Kołobrzegu przypadło 423 turystów w czasie dwóch wakacyjnych miesięcy. Faktyczna ilość osób przebywających na terenie miasta, wzrasta więc 3,5 krotnie w okresie wakacji, a liczby te nie uwzględniają osób odwiedzających, którzy nie korzystają z noclegów w Kołobrzegu. Statystki GUS podają, że gmina wiejska Kołobrzeg udzieliła dodatkowych 390,5 tys. noclegów w lipcu i sierpniu 2024 r[10]. Należy wziąć pod uwagę z dużym prawdopodobieństwem, że te osoby również wielokrotnie przebywały na terenie miasta Kołobrzeg. Miasto Kołobrzeg, jest przykładem braku odpowiedniego przygotowania w zakresie ochrony cywilnej:

- brak infrastruktury schronowej: Kołobrzeg nie posiada w zasobach ochrony cywilnej wystarczającej ilości schronów lub miejsc ukrycia,
- większość obiektów nie jest utrzymywana w stanie gotowości, pochodzą z czasów PRL,
- w razie ataku zbrojnego tylko 0,52% ludności znajdzie schronienie, nie wliczając w to potencjalnej liczby turystów, którzy mogliby utrudnić ewakuacje mieszkańców,
- brak szkoleń dla ludności cywilnej w zakresie procedur ewakuacyjnych,
- niska wiedza mieszkańców na temat miejsc schronienia i sygnałów alarmowych,
- miasto nie posiada cyfrowego systemu ostrzegania mieszkańców, nie wykorzystuje żadnej aplikacji ani możliwości powiadamiania przez sms,

[9] Ibidem.

[10] *Turystyczne obiekty noclegowe na obszarach nadmorskich w lipcu i sierpniu 2024 r.,* Główny Urząd Statystyczny, Warszawa 2024.

ewentualne komunikaty ostrzegawcze i sygnały alarmowe zostaną przekazane przez środki masowego przekazu[11].

W przypadku ataku zbrojnego, a położenie geograficzne miasta każe brać taką ewentualność pod uwagę, bardzo prawdopodobne są wysokie straty w ludziach, chaos i panika wynikające z braku informacji i wystarczającej ilości miejsc schronienia z dużym prawdopodobieństwem uniemożliwią ewakuację mieszkańców.

Objawy paniki jako efekt nagłej sytuacji zagrożenia życia i zdrowia

Osoby, które doświadczą nagłej sytuacji zagrożenia życia odczują zalewający cały organizm głęboki niepokój, realną obawę o życie i zdrowie własne i bliskich, szczególnie tych, którzy są w innym miejscu, poczucie odrealnienia, trudności z oddychaniem. To pierwsze objawy paniki. W sytuacji ataku zbrojnego, panika dotknie nie tylko pojedyncze jednostki, ale także grupy. W definicji medycznej panika to intensywny atak lękowy, spowodowany impulsem zdarzenia lub powstały z niesprecyzowanej przyczyny. W znaczeniu społecznym, duże grupy, a nawet naród zaatakowanego państwa w wyniku paniki, tracą kontrolę nad sytuacją. Poczucie chaosu może być rzeczywiste lub wyobrażone, ale jest traumatyczne, ponieważ znika kontrola w znaczeniu poznawczym. Nowa rzeczywistość jest zaskakująca, nieprzewidywalna, niezrozumiała, ludzie nie potrafią przewidzieć dalszych skutków ani nie znają przyczyny danej sytuacji. Pojawia się potrzeba odzyskania kontroli. W nowej, groźnej rzeczywistości jednostka szuka informacji, które powiedzą co robić, aby uchronić się przed utratą życia i zdrowia. Informacja wyświetlona na ekranie telefonu komórkowego, że bateria jest wyczerpana, jest sygnałem pozytywnym, ponieważ rozwiązanie jest proste: wystarczy ponownie naładować baterię. Jednak, jeśli otrzymamy komunikat, o zbliżającej się przerwie w dostawie prądu, bez podania zakończenia przerwy, to wszyscy zaczną robić to samo: ładować baterie, w obawie, że nie zdążą naładować jej w pełni.

Kontrola nad sytuacją będzie znacznie obniżona, co spowoduje poczucie zbiorowego lęku, a nawet paniki. Społeczeństwo staje się wtedy słabe i podatne na dezinformację oraz kontrolę. Zaczyna działać mechanizm paniki,

[11] Starostwo Powiatowe w Kołobrzegu, Biuletyn Informacji Publicznej *System Ostrzegania i Alarmowania dla mieszańców miasta Kołobrzeg*, https://www.spkolobrzeg.finn.pl/bip-kod/27552961, [dostęp: 02.05.2025].

który pojawił się w organizmie człowieka, w czasach prehistorycznych. Wówczas panika i reakcja na sytuacje zagrożenia były życiem, albo śmiercią. Życie zależało od szybkości reakcji na bodźce, których nie było wiele. Obecnie ten mechanizm działa tak samo, jednak ilość negatywnych bodźców jest nieporównywalnie większa[12].

Międzynarodowa klasyfikacja chorób Classification of Diseases (ICD)[13], wskazuje na trzy podstawowe reakcje na sytuację ekstremalnie trudną: ostrą reakcję na stres, zaburzenie stresowe pourazowe, zaburzenie adaptacyjne. Objawy silnej reakcji na stres pojawią się w ciągu godziny od zadziałania czynnika stresogennego. W tych pierwszych chwilach osoba, która doświadczyła silnego zagrożenia życia i zdrowia odczuje oszołomienie, dezorientację, doświadczy ograniczonego pola świadomości i uwagi, problemów ze zrozumieniem informacji płynących z otoczenia, lęku przed brakiem pomocy, pustki, poczucia odcięcia od świata, znalezienia się w potrzasku, jej zachowanie może być irracjonalne, bezskuteczne, odrealnione.

W poczuciu zagubienia i bezsilności może mieć problem ze zrozumieniem komunikatów i zachować się w sposób nieprzewidywalny. Mogą pojawić się także problemy z oddychaniem, nagłym skokiem ciśnienia, uczuciem kołatania serca, drżenie ciała, niewyraźna mowa, suchość w ustach, wystąpienie nagłego potu, a nawet poczucie dławienia się czy wymioty. W późniejszym czasie w reakcji na silny stres pojawia się głębokie poczucie rozpaczy i beznadziei, płacz, smutek, niemożność snu i odpoczynku, bóle mięśni spowodowane długotrwałym ich napięciem, złość, agresja, poczucie braku kontroli nad ciałem. Jeżeli osoba zostanie ewakuowana z miejsca zdarzenia stosunkowo szybko, objawy powinny ustąpić w ciągu 8 godzin. Jeżeli pomoc nie nadejdzie szybko, a sytuacja stresowa będzie przedłużona, potrwa to nawet do 24godzin. U ofiar wojny w Ukrainie, objawy, szczególnie na tle psychicznym utrzymywały się nawet do 6 tygodni[14].

Włodzimierz Korsak, świadek wybuchu II Wojny Światowej, w momencie napaści miał 10 lat. To, czego doświadczył, opisał jako psychozę społeczną:

[12] T. Grzyb, *Panika – jak sobie z nią radzić w sytuacji wojny,* Uniwersytet SWPS, Wrocław 2022.

[13] System klasyfikacji chorób i problemów zdrowotnych opracowany przez Światową Organizację Zdrowia (WHO).

[14] A. Artych, *Reakcja emocjonalna w obliczu wojny,* Stowarzyszenie Pielęgniarki Cyfrowe, https://www.pielegniarkicyfrowe.pl, [dostęp: 28.04.2025].

„Psychoza była taka, że szpiedzy niemieccy wskazują, gdzie, co należy bombardować. Ludzie, którzy byli odziani w kurtki skórzane bądź płaszcze skórzane, bądź mężczyźni o dobrej konstrukcji, nie jacyś mali tylko wysocy, byli posądzani o szpiegostwo. Łapali ich, trzymali, dopóki żandarmeria czy policja ich nie zabrała i nie sprawdziła czy oni faktycznie są czy nie są szpiegami. Tak samo psychozą było budowanie zasieków. Wiadomo, że w zasieki, które były robione przez ludność cywilną, to czołg wjedzie tak, jak gdyby w pudełko kartonu wjechać samochodem. A ludzie wynosili meble, stare, dobre i taka hałda. Jak był pożar jakiegoś budynku straż pożarna nie mogła dojechać, bo były zasieki, ale psychoza była, że budujemy. Nie było ustalone, w których miejscach, no że w poprzek ulicy robimy, ktoś tam inicjatywę taką podjął, no i wszyscy to robili. Dlatego mówię, że psychoza bardzo łatwo się rozprzestrzenia, obojętnie kto jaki da sygnał tak się robi”[15].

Stan psychozy, którego doświadczył Włodzimierz Korsak, to z punku widzenia psychologii stan chwilowej utraty kontroli nad sobą i poddanie się wpływowi środowiska, w sytuacji nagłego, traumatycznego zdarzenia. To również brak prawidłowego analizowania rzeczywistości z powodu urojeń i zaburzeń racjonalnego myślenia. Często psychoza diagnozowana jest jako choroba psychiczna[16].

Julita Bergman, która w czasie ataku na World Trade Center w 2011 r. pracowała na 82 piętrze wieży północnej, przeżyła atak terrorystyczny na centrum także w 1993 r. Dzięki czemu, jej świadomość pozwoliła na szybką ocenę sytuacji. Jej pierwsze myśli skierowane były, ku odnalezieniu drogi ucieczki: „na schodach spotkałam Billy’ego i Roberta którzy pracowali na 85. piętrze, dwie kondygnacje niżej od miejsca, w które wbił się kadłub samolotu. Mówili, że czubek skrzydła walnął w ich biuro i opuszczenie go zajęło im pięć minut, bo nic nie było widać. Akurat, kiedy dotarliśmy do centrum handlowego z hukiem zawaliła się południowa wieża. Biegliśmy z Billym i Robertem, aż nagle potężny podmuch powalił nas na posadzkę. Robert wylądował na mnie. Czułam, że się duszę. Raptownie zapadła ciemność. Byłam gotowa na śmierć. Zaakceptowałam to, że umrę, choć nie byłam z tego powodu szczęśliwa. Modliłam się krótko do Pana Boga. Prosiłam, żeby przynajmniej dwaj młodsi mężczyźni, którzy mi pomagali przeżyli. Kilkanaście osób złapało się

[15] W. Korsak, *Archiwum Programu Historia Mówiona* pod red. M. Radek, Ośrodek „Brama Grodzka - Teatr NN” 2019 r.

[16] A. Grzywa, *Oblicza psychozy,* Wydawnictwo Czelej, Lublin 2005, s. 16-17.

wraz z nami za ręce usiłując się wydostać na zewnątrz. Pomogło nam pojawienie się strażaka z latarką. Wyszliśmy na skrzyżowaniu ulic Vesey i Chambers. Dotarcie tam zajęło nam godzinę i piętnaście minut. Wszystko było szare. Wyglądało jak krajobraz na księżycu. Przenieśli mnie stamtąd do pobliskiego szpitala Beekman. Nawdychałam się dymu i podali mi tam dużo tlenu i jakieś antydepresanty. Pielęgniarka zadzwoniła do mojego męża. Ponieważ mieszkam w New Jersey, a wszystkie mosty były zamknięte przenocowałam u koleżanki. Następnego dnia mąż zabrał mnie do domu" – wspomina ocalona[17].

Najczęściej w przypadku nagłej sytuacji kryzysowej spodziewamy się „masowej paniki", jednak osoby ocalałe z masowych sytuacji kryzysowych, relacjonują odczucie siły solidarności i więzi społecznych. Wzrasta znaczenie udzielania pomocy osobie znajdującej się obok, niezależnie od sytuacji kryzysowej. Pokazują to relacje osób, które przeżyły II Wojnę Światową, ataki z 11 września 2001 r., huragan Katrina w 2005 r., ataki terrorystyczne w Paryżu w 2015 r. i Brukseli w 2016 r., czy wybuch pandemii COVID-19 w 2020 r. Z relacji świadków wynika, że odczuwali nieodpartą potrzebę niesienia pomocy innym osobom, znajdującym się w tej samej sytuacji. Część badawcza psychologii zajmująca się zachowaniem tłumu, określa działanie jednostek w grupach.

Zaobserwowane reakcje jednostek są często inne, niż miałoby to miejsce w sytuacji, w której znalazłyby się tylko one. Oglądanie reakcji tłumu „przez lupę" stało się przedmiotem zainteresowania Gustava Le Bon[18], dzięki któremu pod koniec XIX i na początku XX wieku dziedzina ta zyskała znaczenie w świecie psychologii i socjologii. Gustav Le Bon uważał, że siła tłumu może wpłynąć na jednostkę w takim stopniu, iż straci ona samodzielne myślenie i stanie się podatna na wszelkie sugestie. Zmienność sugestii jest dynamiczna i zależy od intencji zgromadzenia, więc siła tłumu może być zarówno konstruktywna, jak i destrukcyjna. Koncepcja teorii społecznej mówi, że ludzie czerpią swoją tożsamość ze swojej przynależności do danej grupy społecznej,

[17] A. Dobrowolski *Ocalała z zamachu 11 września,* https://www.pap.pl/aktualnosci/news%2C944824%2Cocalala-z-zamachu-11-wrzesnia-od-razu-wiedzialam-ze-atak-terrorystyczny, Polska Agencja Prasowa PAP, [dostęp: 30.04.2025].

[18] Gustave Le Bon żył w latach 1841-1931. Francuski socjolog i psycholog w okresie renesansu. Z wykształcenia lekarz, z zmiłowania podróżnik i autor wielu prac z dziedziny archeologii i antropologii. Zasłynął z opisania koncepcji psychologii tłumu oraz wielu innych prac psychologicznych poświęconych rozwojowi zbiorowości w różnych ujęciach. https://antyksobieski.pl/en/18011.html, [dostęp: 30.04.2025].

a więc w tłumie tożsamość osobista maleje na rzecz tożsamości grupowej. Występujący często w tłumie efekt widza[19], czyli rozproszenie odpowiedzialności, pokazuje wahanie się przed udzieleniem pomocy, wierząc, że zrobi to ktoś inny. Psychologia tłumu wyjaśnia więc złożone interakcje między zachowaniem jednostki w grupie, samej grupy w kontekście dynamiki nagłych sytuacji oraz ich wpływu na wyniki zdarzeń[20].

Krwawa niedziela w Ukrainie

Mimo, że wojna w Ukrainie trwa od 3 lat, wielu obywateli ukraińskich nadal stara się żyć w ojczyźnie. Świadomi stałego zagrożenia, pozostają w swoich domach i starają się żyć „normalnie". Atak rakietowy na miasto Sumy w Ukrainie, który miał miejsce około godziny 10 rano w dniu 13 kwietnia 2025 r. i wielu Ukraińców zaskoczył podczas nabożeństwa Niedzieli Palmowej. Na Sumy spadły dwie rakiety balistyczne[21], wypełnione amunicją kasetową, czyli ostrymi odłamkami metalu, które mają za zadanie poranić ciało ofiary lub doprowadzić do rozczłonkowania. Broń ta została zaprojektowana w celu maksymalizacji ofiar w ludziach. W wyniku ataku zabitych zostało 34 osoby, w tym 2 dzieci, a 117 osób zostało rannych, w tym 15 dzieci[22]. W przestrzeni prasowej pojawiły się zdjęcia, na których widać leżące na ziemi ciała, płonące samochody i zniszczone budynki, oraz Ukraińców, którzy klęczą przy przykrytych ciałach swoich bliskich[23].

---

[19] Efekt widza: wraz ze wzrostem obserwatorów, spada ilość osób niosących pomoc (*bystander apathy*). Działa on w ten sposób, że obserwatorzy, widząc innych obserwatorów, doświadczają rozproszenia odpowiedzialności. https://psychosfera.net, [dostęp: 30.04.2025].

[20] Frantz, Cynthia McPherson *Psychologia tłumu* 2024 r. https://www.ebsco.com/research-starters/psychology/crowd-psychology, [dostęp: 30.04.2025].

[21] Rakiety balistyczna to grupa pocisków o napędzie rakietowym zasilanym paliwem stałym, ciekłym lub hybrydowym. Ich konstrukcja została przystosowana do profilu lotu jakim się poruszają, m. in. krzywej balistycznej. Posiadają wbudowany system nakierowania na cel bazujący na naprowadzaniu inercyjnym, astronawigacyjnym, komendowym bądź satelitarnym. Pokonują grawitację Ziemi, osiągając dolną granicę przestrzeni kosmicznej, lecąc z prędkością hiperdźwiękową, https://space24.pl/, [dostęp: 01.05.2025].

[22] Dane Państwowej Służby ds. Sytuacji Nadzwyczajnych Ukrainy dla Państwowej Agencji Prasowej PAP z dnia 13.04.2025 r.

[23] J. Junko, *Atak rakietowy Rosji na Ukrainę,* https://www.pap.pl/aktualnosci/atak-rakietowy-rosji-na-ukraine-wzrosla-liczba-zabitych, Polska Agencja Prasowa PAP, [dostęp: 01.05.2025].

Analizując doniesienia prasowe z tego tragicznego wydarzenia, autorka rozdziału nie znalazła wzmianki o wybuchu zbiorowej paniki. Przeciwnie, wiele artykułów donosi o heroicznych czynach, które ratowały ludzkie życie. 13-letni Kyryło Iliaszenko, który w chwili ataku podróżował ze swoją matką autobusem, zobaczył przez okno zakrwawioną i zszokowaną 76-letnią Ałłę Szyrtokałę, która szła obok. Próbował wysiąść z autobusu, ale drzwi były zablokowane. Wydostał się więc przez okno i otworzył je od zewnątrz. Uratował dzięki temu Ałłę i wielu pasażerów uwięzionych w autobusie. W innym przypadku na pomoc ruszyli goście kawiarni i po chwili sami zginęli zasypani gruzami. Dwie kobiety, udzielały pomocy rannym i zginęły w trakcie[24]. Po tych wydarzeniach mieszkańcy 20 tyś. miasta Sumy solidaryzują się w żałobie, nadal udzielając sobie wzajemnie wsparcia. Zachowanie tego młodego człowieka i wielu innych dorosłych osób to akt bohaterstwa czy wynik irracjonalnego zachowania, pod wpływem silnego stresora jakim był atak rakietowy? W atakach z 11 września 2001 r. w Stanach Zjednoczonych podczas udzielania ratunku innym, zginęło czterystu trzech nowojorskich strażaków i policjantów, oraz wielu cywili. Ludzie ratowali siebie nawzajem.

Każda pomoc innym nazywa się zachowaniem prospołecznym, ale zazwyczaj u ludzi jest ono poprzedzone chęcią otrzymania czegoś dla siebie, choćby uznania. W sytuacji napaści zbrojnej, ta potrzeba zanika i kosztem własnego życia ludzie są gotowi ratować innych. To zachowanie nazywamy altruizmem[25]. Altruizm to kierowanie się w swym postępowaniu dobrem innych, gotowość do poświęceń[26]. Jest to bezinteresowna troska o drugiego człowieka, znajdującego się w potrzebie. Altruizm w trakcie napaści zbrojnej ma miejsce „tu i teraz" i to bez względu na warunki i okoliczności, następuje w bezpośrednim kontakcie z osobą potrzebującą. Altruizm jest wynikiem percepcji, tak samo jak poddanie się „efektowi widza".

[24] G. Mamonova, *To było podłe. Uderzyli w serce Sum***,** https://oko.press/sumy-po-rosyjskim-ataku, Polska Agencja Prasowa SA OKO Press, [dostęp: 01.05.2025].

[25] A. Dymanus-Gaudyn, *Dlaczego ludzie pomagają?* https://psychologia-spoleczna.pl/aktualnosci/1935-dlaczego-ludzie-pomagaja.html, [dostęp: 01.05.2025].

[26] Słownik Języka Polskiego PWN, Wydawnictwo Naukowe PWN, Warszawa 2007.

Percepcja

Psychologia definiuje percepcję jako zachodzące w człowieku procesy zmysłowe, które interpretują informacje przychodzącą od zmysłów, oraz inne bodźce pochodzące ze świata zewnętrznego, do umysłu. Przetworzenie przez percepcję tych danych pozwala podjąć decyzję, a następnie zainicjować akcję lub reakcję na otoczenie i „bieg zdarzeń". Jest to model podejmowania decyzji OODA, czyli: Obserwacja → Orientacja → Decyzja → Akcja. 13-letni ukraiński bohater Kyryło Iliaszenko zaobserwował kobietę, zorientował się, że jest ranna, zdecydował się jej pomóc i wyskoczył przez okno autobusu. U tego młodego człowieka zadziałało sensorium, za pomocą którego pobrał i przetworzył dane zmysłowe. Sensorium to komplet wszystkich zmysłów i połączeń nerwowych, które powiadomiło go o istnieniu człowieka w zagrożeniu życia. Sensorium można rozwijać przez trening poznawczy, przy użyciu lornetek, radarów, mikroskopów, ale w przypadku ofiar wojny sensorium wyczula zmysły na obserwowanie i interpretowanie zagrożenia. Dzięki niemu człowiek pod ostrzałem rakietowym podejmuje decyzję: zostać czy uciekać. Faza procesu przetwarzania informacji w ekstremalnych warunkach ulega znacznemu przyspieszeniu, ponieważ nie ma potrzeby oglądania sytuacji z różnych punktów widzenia. W warunkach poczucia bezpieczeństwa ciągle podlegamy potencjalnym błędom poznawczym z powodu selektywnej percepcji, ale w sytuacji bezpośredniego zagrożenia życia, percepcja człowieka jest precyzyjna i pozwala jedynie na pozostanie lub uciekanie z miejsca zdarzenia. Zarówno jak ludzie, tak zwierzęta wykorzystują sensorium do przetrwania (przejście w stan homeostazy). W przypadku ludzi w warunkach pokoju sensorium sprawia, że budujemy cywilizacje i tworzymy społeczności. W sytuacji ataku, o podjęciu działania decyduje przekonanie, że wysiłek przyniesie zamierzony cel, np. ocalenie życia. Jeżeli jednostka nie doświadczy psychozy lub ataku paniki, podjęte przez nią altruistyczne działanie w wyniku percepcji, która otrzymała i przetworzyła prawidłowo informacje dzięki sensorium, jest w stanie ocalić życie i zdrowie osobom pozostającym w sytuacji zagrożenia życia wynikającej z tego samego czynnika, przy jednoczesnym narażeniu własnego. Istnieje także pojęcie świadomości sytuacyjnej, czyli orientacji w dynamicznej sytuacji, pozwalającej na skuteczną reakcję.

Jest to ocena własnej przewagi lub słabości, na podstawie której można podjąć skuteczne działanie. Osoba w podeszłym wieku, z ograniczoną

mobilnością, z dużym prawdopodobieństwem nie ruszy na pomoc osobom zasypanym gruzem zbombardowanego budynku, a znajdując się w subiektywnie bezpieczniejszym miejscu podejmie próbę utrzymania homeostazy[27]. Należy założyć, że ludzie w obliczu nagłego zdarzenia, są na nie całkowicie nieprzygotowani. Odczuwają lęk, przed utratą zdrowa i życia. Mają poczucie bezradności z powodu braku instrumentów do odzyskania kontroli nad sytuacją. Brak przygotowania na atak wroga dla ludności cywilnej jest naturalny. Większość z nas nie ma przekonania o tym, że wojna wybuchnie w Polsce, mimo wiedzy, że toczy się tuż za naszą wschodnią granicą, a Rosja jest do nas wrogo nastawiona. Nie ulegamy więc psychozie ani panice. Nie odczuwamy również lęku, który wywołuje „zamrożenie". Można więc wysunąć wniosek, że percepcja przeciętnego Polaka, nie pobiera z otoczenia informacji o zagrożeniu, ponieważ takie realnie nie występuje bezpośrednio. Czy poczucie bezpieczeństwa jest więc powodem, dla którego mieszkańcy Kołobrzegu nie czują potrzeby edukacji na temat miejsc schronień, a sam ratusz również wykazuje w tym temacie niewielką aktywność? Zdaniem autorki, można wysunąć wnioski, że zarówno Kołobrzeżanie, jak i w większości Polacy, a także cudzoziemcy mieszkający w Polsce, mają wysokie poczucie bezpieczeństwa. Historia I czy II Wojny Światowej wydaje się odległa, tak samo jak wizja ataku zbrojnego we współczesnym świecie.

Potrzeba poczucia bezpieczeństwa jest drugą w hierarchii potrzeb ludzkich. Jest fundamentalna. Poczucie bezpieczeństwa a bycie bezpiecznym mogą być dwiema odrębnymi kwestiami. Istnieje także wiele definicji tego pojęcia, a każdy człowiek może stworzyć własną, ze względu na subiektywizm zjawiska. Nagła utrata zarówno poczucia bezpieczeństwa, jak i faktycznie bezpieczeństwa, wyzwala w człowieku różne reakcje, a żadna z nich nie jest prawidłowa lub nieprawidłowa, ponieważ każda jednostka jest wyposażona w inne mechanizmy, doświadczenia i narzędzie radzenia sobie w tak ekstremalnej sytuacji zagrożenie życia. XXI wiek nie jest wyjątkowy pod względem wojny czy wystąpienia pandemii. Historia pokazuje, że wojna jest obecna od zarania dziejów, a pandemie występują średnio co jeden wiek, przynajmniej od XIV w. n.e. Zagrożenia są stałym zjawiskiem, ale w odczuciu każdego pokolenia mogą być nagłe.

[27] P. Plebaniak, *Sun Zi i jego Sztuka wojny Filozofia i praktyka oddziaływania na bieg zdarzeń,* MT Biznes, Warszawa 2023, s. 1-12.

Czas pokoju w rzeczywistości nie jest wartością daną ludzkości na zawsze, ale w odczuciu jednego pokolenia może być czymś niezbywalnym. Wnioski płynące z literatury, doniesień prasowych i własnego doświadczenia autorki mówią, że każdy człowiek ma własne, subiektywne odczucie tego co jest dla niego zagrożeniem. Dokonuje indywidualnej oceny tego co widzi, słyszy i czuje i ocenia w sposób subiektywny szanse na przetrwanie i powodzenie podejmowanej akcji, ponieważ każdy człowiek wykazuje inną wrażliwości i podatność na działanie ekstremalnych sytuacji. Choć atak zbrojny jest bezspornym czynnikiem zagrażającym człowiekowi, i tak jego reakcja będzie indywidulana, nawet mimo wielu innych osób reagujących podobnie. Oznacza to jedynie to, że wrażliwość tych osób jest podobna. Altruiści odpowiednio do sytuacji przeciwstawią się często własnej percepcji i mimo zagrożenia życia ruszają na pomoc, nie oczekując nic w zamian. Często ich zachowanie jest irracjonalne jak w przypadku psychozy, ale zgoła odwrotne do paniki. Potrzeba odzyskania kontroli nad sytuacją, która pojawiła się nagle jak atak rakietowy jest silniejsza niż racjonalne myślenie i tylko słabości ograniczają człowieka w działaniu. Słabości natury fizycznej: starość lub psychicznej: reakcja na stres w postaci „zamrożenia".

Możemy więc mówić o dwóch kategoriach reakcji przyczynowo – skutkowej. Po pierwsze przyczyny wewnętrzne, które mają swoje źródła w człowieku, wykreowane doświadczeniem życiowym i charakterem, oraz zewnętrzne, pochodzące spoza świata wewnętrznego, które są wynikiem okoliczności, niejako są przymusem, ale podparte percepcją i wiedzą. Osoby żyjące w strefie konfliktu, będące pod wpływem stałego zagrożenia, nabywają doświadczenia, które zmienia ich percepcję z narzędzia pozwalającego na spokojną analizę otoczenia na oręż „super bohatera", który staje się liderem akcji ratunkowej wprowadzając poczucie kontroli. Cechy ludzkie, które determinują ostrożne zachowania, jak płeć, wiek, status społeczny, poziom wiedzy i świadomości, to czynniki wpływające na ocenę zagrożenia i swoich szans na przetrwanie. Ocena jest subiektywna, tak samo jak poczucie bezpieczeństwa.

Podsumowanie

Stworzenie bezpiecznego państwa czy miasta to nie to samo co stworzenie sprawnego państwa czy miasta. Można przygotować społeczeństwo na różne zagrożenia przez edukację i profilaktykę, oraz stworzenie warunków do przetrwania, czyli schronów i miejsc ukrycia. Ludzie reagują różnie na

ekstremalne zdarzenia, których nie mogą kontrolować, ale należy zwiększać świadomość oraz wiedzę praktyczną w społeczeństwie, co ustawowo jest obowiązkiem samorządów. Systemy zarządzania bezpieczeństwem mają większe szanse zadziałać prawidłowo na każdym poziomie, od wczesnego ostrzegania po ewakuację, jeśli ludzie nie ulegną panice i będą prawidłowo interpretować komunikaty.

Literatura

1. Artych A., *Reakcja emocjonalna w obliczu wojny,* Stowarzyszenie Pielęgniarki Cyfrowe.
2. *Bądź gotowy! Poradnik na czas wojny i kryzysu,* Rządowe Centrum Bezpieczeństwa 2022.
3. Dobrowolski A., *Ocalała z zamachu 11 września,* Państwowa Agencja Prasowa PAP.
4. Dymanus-Gaudyn A., *Dlaczego ludzie pomagają?* www.psychologia-spoleczna.pl
5. Grzyb T., *Panika – jak sobie z nią radzić w sytuacji wojny* Uniwersytet SWPS Wrocław 2022.
6. Grzywa A., *Oblicza psychozy* Wydawnictwo Czelej, Lublin 2005.
7. Junko J. *Atak rakietowy Rosji na Ukrainę,* Państwowa Agencja Prasowa PAP.
8. Korsak W. *Archiwum Programu Historia Mówiona* pod red. M. Radek, Ośrodek „Brama Grodzka - Teatr NN", 2019.
9. McPherson F. C., *Psychologia tłumu,* 2024.
10. Mamonova G., *To było podłe. Uderzyli w serce Sum,* Polska Agencja Prasowa SA OKO Press.
11. Plebaniak P., *Sun Zi i jego Sztuka wojny Filozofia i praktyka oddziaływania na bieg zdarzeń*. MT Biznes, Warszawa 2023.
12. *Powierzchnia i ludność w przekroju terytorialnym w 2023 r.,* Główny Urząd Statystyczny, Warszawa 2023.
13. *Raport dotyczący budowli ochronnych 2023,* Komenda Główna Straży Pożarnej, Warszawa 2023.
14. Raport PSP Kołobrzeg w ramach działań Komendy Głównej Straży Pożarnej do Raportu dotyczącego budowli ochronnych 2023.
15. Słownik Języka Polskiego PWN, Wydawnictwo Naukowe PWN, Warszawa 2012.
16. *System Ostrzegania i Alarmowania dla mieszańców miasta Kołobrzeg,* Starostwo Powiatowe w Kołobrzegu, Biuletyn Informacji Publicznej.
17. *System klasyfikacji chorób i problemów zdrowotnych,* Światowa Organizację Zdrowia (WHO).
18. *Turystyczne obiekty noclegowe na obszarach nadmorskich w lipcu i sierpniu 2024 r.,* Główny Urząd Statystyczny.
19. Ustawa o ochronie ludności i obronie cywilnej z dnia 05.12.2024 r. Dz. U. 2024 poz. 1907.
20. *W schronie się nie schronisz,* Raport NIK, 13 marca 2024.

mgr inż. Ewa Brodacz
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0002-6469-9159

dr inż. Ewa Stamirowska-Krzaczek
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0002-6653-9055

dr inż. Justyna Siwiela-Tomaszczyk
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0002-2303-9285

Evelina Demianchuk
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0000-5382-1011

Oleksandr Hubar
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0009-0008-8453-1963

https://doi.org/10.29316/9788368103205_12

BEZPIECZEŃSTWO ŻYWNOŚCIOWE JAKO FUNDAMENT ODPORNOŚCI PAŃSTWA: ROLA DIETETYKI W KSZTAŁTOWANIU STRATEGII BEZPIECZEŃSTWA WEWNĘTRZNEGO

FOOD SECURITY AS A FOUNDATION OF STATE RESILIENCE: THE ROLE OF DIETETICS IN SHAPING INTERNAL SECURITY STRATEGIES

Streszczenie

W niniejszym rozdziale omówiono rolę bezpieczeństwa żywnościowego jako kluczowego elementu odporności państwa

Summary

This chapter explores the role of food security as a key element of state resilience in the context of public health, social stability, and

w kontekście zdrowia publicznego, stabilności społecznej oraz zdolności państwa do reagowania na kryzysy. Na podstawie przeglądu literatury naukowej oraz analizy przypadków czterech państw (Finlandii, Japonii, Szwecji i Holandii), wykazano, że odpowiednia polityka żywieniowa oraz edukacja dietetyczna istotnie przyczyniają się do ograniczenia chorób dietozależnych, zwiększenia kapitału zdrowotnego społeczeństwa i wzmocnienia zdolności adaptacyjnych w obliczu zagrożeń. Szczególną uwagę poświęcono roli dietetyki jako strategicznej dziedziny wspierającej polityki publiczne w zakresie profilaktyki zdrowotnej. W części końcowej zaproponowano rekomendacje dla Polski dotyczące integracji polityki żywieniowej z systemem bezpieczeństwa wewnętrznego. Rozdział wpisuje się w nurt interdyscyplinarnych badań nad zdrowiem populacyjnym, polityką żywnościową i bezpieczeństwem narodowym.

Słowa kluczowe: bezpieczeństwo żywnościowe, odporność państwa, dietetyka, zdrowie publiczne, choroby dietozależne, polityka żywieniowa

the state's ability to respond to crises. Based on a review of scientific literature and a comparative analysis of four countries (Finland, Japan, Sweden, and the Netherlands), the study demonstrates that appropriate food policies and nutritional education significantly contribute to reducing diet-related diseases, increasing the population's health capital, and strengthening adaptive capacity in the face of threats. Particular attention is given to the strategic importance of dietetics as a discipline supporting public health prevention policies. The final section offers recommendations for integrating food policy into Poland's internal security system. The chapter contributes to interdisciplinary research on population health, food policy, and national security.

Keywords: food security, state resilience, dietetics, public health, diet-related diseases, food policy

Wstęp

Bezpieczeństwo żywnościowe od dekad uznawane jest za fundament stabilności społeczno-gospodarczej, zdrowotnej i politycznej państw. Choć pierwotnie kojarzone głównie z zapewnieniem odpowiedniej ilości pożywienia, w ostatnich latach jego definicja została znacząco rozszerzona i zyskała strategiczny wymiar. Organizacja Narodów Zjednoczonych do spraw Wyżywienia i Rolnictwa (FAO) definiuje bezpieczeństwo żywnościowe jako stan, w którym „wszyscy ludzie, przez cały czas, mają fizyczny, społeczny i ekonomiczny dostęp do wystarczającej, bezpiecznej i pożywnej żywności, która zaspokaja ich potrzeby żywieniowe i preferencje żywieniowe w celu

prowadzenia aktywnego i zdrowego życia”[1]. Definicja ta obejmuje cztery kluczowe filary: dostępność żywności, fizyczny i ekonomiczny dostęp do niej, stabilność dostaw oraz akceptowalność kulturową[2].

Współcześnie bezpieczeństwo żywnościowe nie może być analizowane w oderwaniu od szerszego kontekstu społeczno-politycznego. Szczególnie istotny jest jego związek z pojęciem odporności państwa, rozumianej jako zdolność do przeciwdziałania zagrożeniom, ich adaptacyjnego przetrwania oraz odbudowy funkcji społecznych i gospodarczych po kryzysie[3]. W Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2020 r. podkreślono, że odporność państwa opiera się m.in. na zdolności do zapewnienia podstawowych potrzeb obywateli, w tym dostępu do bezpiecznej żywności i usług zdrowotnych. W tym ujęciu bezpieczeństwo żywnościowe staje się nie tylko kwestią zdrowia publicznego, lecz także integralnym komponentem strategii bezpieczeństwa wewnętrznego.

W dobie globalizacji, urbanizacji oraz zmian w stylu życia i wzorcach konsumpcji obserwuje się jednoczesne występowanie problemów niedożywienia oraz nadmiernego spożycia żywności niskiej jakości. Zjawisko to określane jest mianem „podwójnego obciążenia malnutricją” (double burden of malnutrition) – z jednej strony obejmuje niedobory energii i mikroskładników, a z drugiej – nadmiar kalorii i niezdrowych składników diety[4] [5]. W Polsce – podobnie jak w innych krajach o średnich i wysokich dochodach – rośnie liczba osób cierpiących na otyłość i choroby dietozależne, szczególnie wśród dzieci i młodzieży[6]. Według danych Głównego Urzędu Statystycznego, w 2022 r. nadwagę miało 54% dorosłych mężczyzn i 43% kobiet, a otyłość występowała już u co czwartego Polaka[7].

---

1 *Policy Brief: Food Security*, Food and Agriculture Organization, FAO, 2006.

2 D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem żywności: Teoria i praktyka,* Wydawnictwo Naukowe PWN, Warszawa 2010.

3 R. Rey, *Społeczeństwo odporne na zagrożenia*, Rządowe Centrum Bezpieczeństwa, Warszawa 2020.

4 A. Afshin i in., *Health effects of dietary risks in 195 countries, 1990-2017*, The Lancet, nr 393(10184), 2019, s. 1958-1972.

5 M. Niewczas-Dobrowolska, *Jakość i bezpieczeństwo żywności: Systemy – postawy – konsumenci*, Problemy Higieny i Epidemiologii, nr 102(1), 2021, s. 43-50.

6 L. Kłosiewicz-Latoszek, W. B. Szostak, *Żywienie a choroby sercowo-naczyniowe – fakty i mity*, Forum Profilaktyki nr 1(10), 2008, s. 1-4.

7 *Stan zdrowia ludności Polski w 2021 roku*, Główny Urząd Statystyczny, Warszawa 2022.

Jednocześnie w społeczeństwie utrzymują się przypadki niedożywienia wynikającego z ubóstwa i wykluczenia społecznego. Z raportu Federacji Polskich Banków Żywności[8] wynika, że nawet 683 tysiące dzieci w Polsce doświadcza ubóstwa żywnościowego, co oznacza ograniczony dostęp do żywności o odpowiedniej jakości i wartości odżywczej. Problem ten dotyczy również seniorów oraz osób z niepełnosprawnościami[9]. Takie zjawiska prowadzą do długoterminowych konsekwencji zdrowotnych i ekonomicznych: dzieci niedożywione rozwijają się wolniej, osiągają gorsze wyniki edukacyjne i w dorosłym życiu częściej cierpią na choroby przewlekłe, co obciąża system ochrony zdrowia i zmniejsza produktywność[10].

Warto podkreślić, że sposób odżywiania społeczeństwa jest jednym z najważniejszych czynników wpływających na występowanie chorób niezakaźnych, takich jak cukrzyca typu 2, nadciśnienie tętnicze, miażdżyca czy nowotwory jelita grubego[6]. Szacuje się, że nieprawidłowe nawyki żywieniowe są odpowiedzialne za około 11 milionów zgonów rocznie na świecie – więcej niż jakikolwiek inny pojedynczy czynnik ryzyka[4]. W polskich warunkach problem ten ma dodatkowy wymiar: choroby przewlekłe obniżają zdolność populacji do aktywnego udziału w rynku pracy, zwiększają absencję chorobową oraz koszty leczenia ponoszone przez państwo[11].

W tym kontekście dietetyka – jako interdyscyplinarna nauka o żywieniu człowieka – zyskuje strategiczne znaczenie. Jej rola wykracza poza indywidualne doradztwo żywieniowe i obejmuje projektowanie polityk publicznych, edukację zdrowotną oraz wspieranie populacyjnych interwencji dietetycznych[12]. Skuteczna polityka żywieniowa, oparta na dowodach naukowych i dostosowana kulturowo, może zmniejszyć częstość występowania chorób

[8] *Niedożywienie i głód w Polsce: Raport Banków Żywności*, Federacja Polskich Banków Żywności, Warszawa 2023.

[9] R. Szarfenberg, *Poverty Watch 2024: Ubóstwo dzieci w Polsce*, Europejska Sieć Przeciwdziałania Ubóstwu – Polska, Warszawa 2024.

[10] J. Hoddinott, H. Alderman, J. R. Behrman, L. Haddad, S. Horton, *The economic rationale for investing in stunting reduction*, Maternal & Child Nutrition, nr 9(S2), 2013, s. 69-82.

[11] A. Piekutowska, A. Skrzypek, *Zrównoważony rozwój i jakość życia jako elementy bezpieczeństwa społecznego*, Ekonomia i Środowisko, nr 3(50), 2014, s. 159-171.

[12] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.

dietozależnych, poprawić jakość życia obywateli oraz zwiększyć ich odporność biologiczną i ekonomiczną na sytuacje kryzysowe[13].

Celem niniejszego rozdziału jest wykazanie, że bezpieczeństwo żywnościowe, rozumiane nie tylko jako fizyczna dostępność żywności, ale jako stan sprzyjający zdrowemu odżywianiu się, stanowi jeden z filarów odporności państwa. W szczególności podjęto próbę odpowiedzi na pytania:

- w jaki sposób dieta wpływa na zdrowie publiczne i stabilność społeczną?
- jak państwa wykorzystują politykę żywieniową jako narzędzie bezpieczeństwa wewnętrznego?
- jakie wnioski dla Polski płyną z doświadczeń międzynarodowych?

Analiza została przeprowadzona w oparciu o dane porównawcze z wybranych państw (Finlandia, Japonia, Holandia, Szwecja) oraz przegląd literatury naukowej i raportów instytucji krajowych i międzynarodowych.

Kolejnym celem pracy było również zidentyfikowanie związków między polityką żywnościową a odpornością państwa, ze szczególnym uwzględnieniem roli dietetyki i edukacji żywieniowej jako elementów profilaktyki zdrowotnej oraz stabilizacji społeczno-ekonomicznej. Analiza miała na celu także ocenę skuteczności wybranych programów krajowych w zakresie poprawy stanu odżywienia społeczeństw i ich wpływu na bezpieczeństwo wewnętrzne.

W rozdziale zastosowano jakościową analizę porównawczą (*comparative qualitative analysis*, QCA), uwzględniającą dane statystyczne, wskaźniki epidemiologiczne i społeczno-ekonomiczne z różnych krajów. Porównano przypadki czterech państw, które wdrożyły długofalowe programy polityki żywieniowej z mierzalnymi efektami populacyjnymi: Finlandii, Japonii, Holandii i Szwecji.

W analizie zastosowano także elementy desk research, obejmujące przegląd dostępnej literatury naukowej oraz dokumentów strategicznych i raportów organizacji międzynarodowych, takich jak FAO, WHO, UNICEF, OECD oraz Narodowe Instytuty Zdrowia Publicznego.

Materiały wykorzystane w badaniu pochodziły z następujących źródeł:

- raporty FAO i WHO dotyczące bezpieczeństwa żywnościowego i chorób dietozależnych[14] [15],

[13] G. Śmigielska, W. J. Florkowski, *Systemy jakości żywności a dobrostan społeczny i bezpieczeństwo żywnościowe*, Problemy Rolnictwa Światowego, nr 15(1), 2015, s. 138-148.

[14] *Policy…,* op. cit.

[15] *Noncommunicable diseases: Key facts*, World Health Organization, Genewa 2024.

- dane epidemiologiczne z badań nad niedożywieniem i otyłością w populacjach dzieci i dorosłych[16, 17],
- polskie publikacje naukowe dotyczące zarządzania bezpieczeństwem żywności[18, 19],
- strategiczne dokumenty rządowe, w tym *Strategia Bezpieczeństwa Narodowego RP*[20] oraz raporty Rządowego Centrum Bezpieczeństwa[21],
- dane empiryczne i wskaźniki zdrowia populacyjnego pochodzące z krajowych instytutów zdrowia i statystyki (np. THL – Finlandia, NIJZ – Holandia, National Institute of Public Health – Japonia).

Przegląd literatury

Ewolucja pojęcia bezpieczeństwa żywnościowego. Pojęcie bezpieczeństwa żywnościowego po raz pierwszy sformułowano w kontekście zapewnienia wystarczającej podaży żywności na poziomie krajowym. Jednak od lat 80. XX wieku, a zwłaszcza po publikacjach FAO, zakres ten został znacząco rozszerzony. Obecnie obejmuje on nie tylko produkcję, ale również dostępność ekonomiczną, wartość odżywczą, stabilność podaży oraz kulturową akceptowalność pożywienia[22] [23]. W polskiej literaturze naukowej podkreśla się, że bezpieczeństwo żywnościowe należy analizować w kontekście systemowym,

[16] R. E. Black, C. G. Victora, S. P. Walker, Maternal and Child Nutrition Study Group, *Maternal and child undernutrition and overweight in low-income and middle-income countries*, The Lancet, nr 382(9890), 2013, s. 427-451.

[17] J. Hoddinott, H. Alderman, J. R. Behrman, L. Haddad, S. Horton, *The economic rationale for investing in stunting reduction*, Maternal & Child Nutrition, nr 9(S2), 2013, s. 69-82.

[18] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.

[19] M. Niewczas-Dobrowolska, *Jakość i bezpieczeństwo żywności: Systemy – postawy – konsumenci*, Problemy Higieny i Epidemiologii, nr 102(1), 2021, s. 43-50.

[20] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2020.

[21] R. Rey, *Społeczeństwo odporne na zagrożenia*, Rządowe Centrum Bezpieczeństwa, Warszawa 2020.

[22] *Policy…,* op. cit.

[23] A. Mikuła, *Bezpieczeństwo żywnościowe Polski*, Roczniki Naukowe Ekonomii Rolnictwa i Rozwoju Obszarów Wiejskich, nr 99(4), 2012, s. 38-48.

obejmującym powiązania między produkcją, logistyką, edukacją zdrowotną oraz polityką publiczną[24, 25].

Kozłowska-Burdziak[26] zwraca uwagę, że współczesne ujęcie bezpieczeństwa żywnościowego nie może ograniczać się jedynie do wskaźników produkcyjnych czy dostępności fizycznej – kluczowe znaczenie ma dostępność ekonomiczna, szczególnie w społeczeństwach o silnych nierównościach dochodowych. Podobnie Dąbrowska i Ozimek[27] zaznaczają, że percepcja bezpieczeństwa żywnościowego przez konsumentów coraz częściej wiąże się z jakością, składem odżywczym i zaufaniem do instytucji kontrolnych.

Stan bezpieczeństwa żywnościowego w Polsce. Polska należy do krajów samowystarczalnych żywnościowo – według danych Instytutu Ekonomiki Rolnictwa i Gospodarki Żywnościowej, produkcja krajowa pokrywa krajowe potrzeby w zakresie podstawowych produktów rolnych i spożywczych[28]. Niemniej jednak, jak zauważa Mikuła[29], bezpieczeństwo żywnościowe w Polsce jest nierównomiernie rozłożone terytorialnie i społecznie. Dane Głównego Urzędu Statystycznego wskazują, że ok. 1,6 mln Polaków doświadcza tzw. ubóstwa skrajnego, co przekłada się na brak regularnego dostępu do wartościowej żywności[30].

Według raportu Federacji Polskich Banków Żywności[31], w 2022 r. aż 683 tysiące dzieci oraz ponad 300 tysięcy osób starszych żyło w warunkach ubóstwa żywnościowego. Wynika to nie tylko z barier dochodowych, ale również z braku umiejętności planowania zakupów, gotowania i oceny wartości

[24] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.

[25] J. Omieciuch, *Jakość i bezpieczeństwo żywności w Polsce*, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, nr 3, 2016, s. 123-135.

[26] M. Kozłowska-Burdziak, *Warunki bezpieczeństwa żywnościowego Polski (ze szczególnym uwzględnieniem dostępności ekonomicznej)*, Optimum. Studia Ekonomiczne nr 3(99), 2019, s. 38-52.

[27] A. Dąbrowska, I. Ozimek, *Bezpieczeństwo żywnościowe konsumentów w Polsce – wybrane aspekty*, Handel Wewnętrzny, nr 4(351), 2014, s. 55-79.

[28] I. Szczepaniak, *Ocena bezpieczeństwa żywnościowego i samowystarczalności żywnościowej Polski na tle państw Unii Europejskiej*, International Business and Global Economy, nr 37, 2018, s. 168-182.

[29] A. Mikuła, *Bezpieczeństwo żywnościowe…*, op. cit.

[30] *Ubóstwo w Polsce w 2021 roku*, Główny Urząd Statystyczny, Warszawa 2022.

[31] *Niedożywienie i głód w Polsce: Raport Banków Żywności*, Federacja Polskich Banków Żywności, Warszawa 2023.

odżywczej produktów[32]. Autorzy raportów społecznych (np. Szarfenberg [33]) wskazują, że mimo ogólnego wzrostu poziomu życia, problem ubóstwa żywnościowego w Polsce pogłębia się w niektórych grupach, zwłaszcza wśród rodzin wielodzietnych i samotnych matek.

Kolejnym zagrożeniem dla bezpieczeństwa żywnościowego są zjawiska, takie jak marnowanie żywności, niska świadomość żywieniowa oraz wysoka konsumpcja produktów wysoko przetworzonych[34, 35]. Z raportów NIK[36] wynika, że w Polsce rocznie marnuje się ponad 4,8 miliona ton żywności, co stanowi zarówno stratę ekonomiczną, jak i społeczną.

Dietetyka jako element strategii bezpieczeństwa żywnościowego

W ostatnich latach w literaturze naukowej rośnie znaczenie dietetyki jako interdyscyplinarnego narzędzia w polityce zdrowotnej i żywnościowej. Dietetyka nie tylko opisuje fizjologiczne potrzeby żywieniowe, ale również wskazuje kierunki działań profilaktycznych i interwencyjnych na poziomie populacyjnym[37]. Jak podkreślają Śmigielska i Florkowski[38], integracja wiedzy dietetycznej z zarządzaniem jakością i dostępnością żywności stanowi jeden z filarów nowoczesnego podejścia do bezpieczeństwa żywnościowego.

W Polsce jednak brakuje narodowej strategii żywieniowej zintegrowanej z systemem opieki zdrowotnej i edukacji. Chociaż wprowadzono zalecenia żywieniowe (Piramida Zdrowego Żywienia i Aktywności Fizycznej), ich realizacja jest ograniczona – głównie z powodu niskiej świadomości społecznej i braku systematycznej edukacji zdrowotnej w szkołach[39].

Kołożyn-Krajewska i Sikora[40] wskazują, że skuteczność strategii żywieniowych zależy od ich zakotwiczenia instytucjonalnego – niezbędna jest współpraca między resortami zdrowia, edukacji, rolnictwa i finansów. Z kolei

[32] M. Niewczas-Dobrowolska, *Jakość…,* op. cit.

[33] R. Szarfenberg, *Poverty Watch 2024: Ubóstwo dzieci w Polsce*, Europejska Sieć Przeciwdziałania Ubóstwu – Polska, Warszawa 2024.

[34] A. Dąbrowska, I. Ozimek, *Bezpieczeństwo żywnościowe konsumentów…*, op. cit.

[35] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.

[36] *Informacja o wynikach kontroli: Marnowanie żywności w Polsce*, Najwyższa Izba Kontroli, Warszawa 2022.

[37] L. Kłosiewicz-Latoszek, W. B. Szostak, *Żywienie a choroby…,* op. cit.

[38] G. Śmigielska, W. J. Florkowski, *Systemy jakości…,* op. cit.

[39] M. Niewczas-Dobrowolska, *Jakość…,* op. cit.

[40] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.

Śmigielska i Florkowski[41] postulują włączenie dietetyków do zespołów decyzyjnych na szczeblu samorządowym i krajowym jako specjalistów w zakresie zdrowia publicznego.

Ważną kwestią jest także edukacja żywieniowa prowadzona w ramach kampanii publicznych. Badania pokazują, że odpowiednio zaprojektowane interwencje edukacyjne mogą zmienić nawyki żywieniowe i wpłynąć na wybory konsumenckie [42]. Jednak w Polsce działania te są rozproszone i często krótkoterminowe, co ogranicza ich efektywność.

Wyniki analizy porównawczej: strategie bezpieczeństwa żywnościowego w wybranych państwach

Finlandia – model odporności systemowej. Finlandia jest często wskazywana jako wzorcowy przykład integracji polityki żywnościowej z szeroko pojętym bezpieczeństwem narodowym. Kluczowym elementem fińskiego podejścia jest North Karelia Project, rozpoczęty w 1972 roku, który miał na celu redukcję chorób sercowo-naczyniowych poprzez zmianę nawyków żywieniowych społeczeństwa. W ciągu pierwszej dekady trwania projektu (1972-1982) średni poziom cholesterolu w populacji Północnej Karelii znacząco się obniżył – o około 17-21%. Spożycie tłuszczów nasyconych spadło prawie o połowę, m.in. dzięki temu, że mieszkańcy masowo przeszli z masła na margaryny miękkie i oleje roślinne do smarowania pieczywa. Udział osób używających masła do gotowania zmalał z około 70% do 20%, podczas gdy wykorzystanie oleju rzepakowego wzrosło wielokrotnie[43].

Ponadto, Finlandia wdrożyła system centralnej koordynacji bezpieczeństwa dostaw, który obejmuje współpracę między sektorem publicznym, prywatnym i organizacjami pozarządowymi. System ten nie tylko umożliwia zaopatrzenie w niezbędne towary, ale także poprawia odporność społeczeństwa na kryzysy[44].

---

41 G. Śmigielska, W. J. Florkowski, *Systemy jakości…,* op. cit.

42 M. Górnicka, K. Krupa-Kotara, *Wpływ edukacji zdrowotnej na wybory żywieniowe dzieci i młodzieży*, Problemy Higieny i Epidemiologii, nr 100(3), 2019, s. 201-206.

43 P. Puska, *North Karelia Project – jak odżywianie wpływa na choroby układu krążenia*, Narodowe Centrum Edukacji Żywieniowej, Warszawa 2016.

44 *Bezpieczeństwo kompleksowe Finlandii: znaczenie odporności społeczeństwa*, Instytut Europy Środkowej, Lublin 2023.

Japonia – innowacje technologiczne i tradycja żywieniowa. Japonia, mimo niskiej samowystarczalności żywnościowej (około 37% w ujęciu kalorycznym), skutecznie zarządza bezpieczeństwem żywnościowym poprzez połączenie innowacji technologicznych i tradycyjnych praktyk żywieniowych. Rząd japoński inwestuje w rozwój przemysłu mięsa hodowanego komórkowo, aby wzmocnić zrównoważone dostawy żywności [45].

Tradycyjna dieta japońska, szczególnie na Okinawie, charakteryzuje się wysokim spożyciem warzyw, ryb i produktów sojowych oraz niskim spożyciem mięsa i cukru. Dieta ta jest bogata w witaminy, składniki mineralne, błonnik i kwasy tłuszczowe omega-3, co przyczynia się do długowieczności mieszkańców [46].

Szwecja – zwiększenie krajowej produkcji żywności. Szwecja dąży do zwiększenia krajowej produkcji żywności w celu wzmocnienia bezpieczeństwa żywnościowego. Nowa strategia żywnościowa rządu ma na celu wzmocnienie konkurencyjności łańcucha żywnościowego i zwiększenie krajowej produkcji [47].

Szwedzka Agencja Żywności prowadzi intensywne kontrole jakości produktów spożywczych. W 2024 r. odnotowano rekordową liczbę wycofań produktów z rynku, co świadczy o zaostrzonej kontroli jakości i dbałości o bezpieczeństwo konsumentów[48].

Holandia – zaawansowane systemy kontroli i innowacje. Holandia jest liderem w dziedzinie bezpieczeństwa żywnościowego dzięki zaawansowanym systemom kontroli i innowacjom. W 2023 r. przeprowadzono liczne inspekcje bezpieczeństwa żywności, które przyczyniły się do wykrycia niezgodnych partii żywności[49].

Ponadto, Holandia wprowadziła nowe przepisy dotyczące oznaczania alergenów na etykietach produktów spożywczych, co ma na celu zwiększenie

[45] *Japonia inwestuje w przemysł mięsa hodowanego komórkowo, by wzmocnić zrównoważone dostawy żywności*, FoodFakty, 2023.

[46] Narodowe Centrum Edukacji Żywieniowej, *Dieta długowieczności z Okinawy*, PZH, Warszawa 2018.

[47] Farmer.pl, *Szwecja chce zwiększyć produkcję żywności*, 2025.

[48] SkandynawiaInfo, *Rekordowy rok wycofań produktów spożywczych w Szwecji – bezpieczeństwo żywności pod lupą*, 2024.

[49] *Inspekcje bezpieczeństwa żywności w Holandii – podsumowanie 2023 roku*, FoodFakty, 2024.

ochrony zdrowia konsumentów z alergiami poprzez transparentne informowanie o możliwej obecności alergenów[50].

Przedstawione przykłady państw pokazują, że skuteczna polityka żywieniowa, zintegrowana z systemem zdrowia publicznego i strategią bezpieczeństwa narodowego, może znacząco zwiększyć odporność społeczeństw na kryzysy zdrowotne, gospodarcze i społeczne. Szczególnie model fiński, bazujący na kompleksowej edukacji zdrowotnej, reformie rynku produktów spożywczych i silnej współpracy międzysektorowej, przyniósł długofalowe efekty w postaci redukcji chorób sercowo-naczyniowych i poprawy średniej długości życia[51, 52].

Podobnie doświadczenia Japonii i Szwecji pokazują, że bezpieczeństwo żywnościowe to nie tylko problem logistyki, lecz także kwestia kultury żywieniowej, świadomości konsumenckiej i instytucjonalnego nadzoru nad jakością żywności [53] [54]. W Polsce – mimo istotnych postępów w zakresie systemów kontroli bezpieczeństwa żywności – nadal występują istotne deficyty w zakresie polityki edukacyjnej, spójności działań resortowych oraz rozpoznawalności dietetyki jako strategicznej dziedziny nauki [55, 56].

Wnioski te korelują z ustaleniami Śmigielskiej i Florkowskiego[57], którzy zauważają, że krajowe strategie żywnościowe powinny być zintegrowane z celami zrównoważonego rozwoju i długofalowej polityki zdrowotnej. W literaturze krajowej rośnie również zainteresowanie koncepcją „zdrowia jako bezpieczeństwa" (health as security), która kładzie nacisk na rolę kapitału ludzkiego w budowie odporności państwa [58, 59].

W Polsce brakuje jednak strategicznych dokumentów polityki żywieniowej o randze ustawowej, które integrowałyby działania różnych resortów.

---

[50] *Oznaczania alergenów na etykietach produktów spożywczych – nowe przepisy w Holandii*, FoodFakty, 2025.

[51] P. Puska, *North Karelia Project – jak odżywianie wpływa…*, op. cit.

[52] E. Vartiainen, *The North Karelia Project: Cardiovascular disease prevention in Finland*, Global Cardiology Science & Practice, nr 2018(2), 2018, art. 13.

[53] Narodowe Centrum Edukacji Żywieniowej, *Dieta długowieczności z Okinawy*, op. cit.

[54] SkandynawiaInfo, *Rekordowy rok wycofań produktów spożywczych…*, op. cit.

[55] M. Niewczas-Dobrowolska, *Jakość i bezpieczeństwo…*, op. cit.

[56] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.

[57] G. Śmigielska, W. J. Florkowski, *Systemy jakości żywności…*, op. cit.

[58] D. Cichoń, *Zdrowie publiczne w kontekście polityki społecznej i bezpieczeństwa państwa*, Zdrowie i Bezpieczeństwo, nr 6(1), 2022, s. 45-56.

[59] J. Gierszewski, *Bezpieczeństwo wewnętrzne: Zarys systemu*, Znak, Warszawa 2013.

Zamiast tego występuje rozproszenie kompetencji między instytucjami – od Narodowego Instytutu Zdrowia Publicznego, przez Ministerstwo Zdrowia, po resort rolnictwa i edukacji[60]. Problemem jest również brak systematycznego wdrażania edukacji żywieniowej w szkołach, co potwierdzają badania nad świadomością dzieci i młodzieży[61].

Kolejnym wyzwaniem jest strukturalna nierówność w dostępie do żywności wysokiej jakości. Produkty wysoko przetworzone – tanie, lecz ubogie w składniki odżywcze – dominują w diecie osób o niskich dochodach, co prowadzi do jednoczesnego występowania otyłości i niedoborów mikroelementów[62, 63]. Zjawisko to wpisuje się w szerszy kontekst społeczny i powinno być traktowane jako czynnik ryzyka osłabiający potencjał zdrowotny i ekonomiczny kraju.

Podsumowanie

Z przeprowadzonych analiz wynika jednoznacznie, że bezpieczeństwo żywnościowe oraz jakość diety populacyjnej mają bezpośredni i systemowy wpływ na zdolność państwa do reagowania na zagrożenia, ochronę zdrowia publicznego oraz długofalowe utrzymanie stabilności społeczno-ekonomicznej. Kwestie żywieniowe przestają być domeną wyłącznie polityki zdrowotnej – stają się integralnym komponentem strategii bezpieczeństwa wewnętrznego. Państwa, które potraktowały politykę żywieniową w sposób strategiczny i międzysektorowy, osiągnęły mierzalne efekty: spadek częstości występowania chorób dietozależnych, zwiększenie oczekiwanej długości życia, poprawę sprawności systemu opieki zdrowotnej oraz obniżenie kosztów społecznych i budżetowych[64, 65].

Przykłady Finlandii, Japonii, Szwecji czy Holandii pokazują, że polityka żywnościowa może być skutecznym narzędziem nie tylko ochrony zdrowia, ale również budowania odporności społecznej – zdolności do adaptacji, regeneracji i reagowania w sytuacjach kryzysowych. W kontekście współczesnych

[60] R. Szarfenberg, *Poverty Watch 2024: Ubóstwo dzieci w Polsce*, op. cit.
[61] M. Górnicka, K. Krupa-Kotara, *Wpływ edukacji zdrowotnej…*, op. cit.
[62] L. Kłosiewicz-Latoszek, W. B. Szostak, *Żywienie a choroby sercowo-naczyniowe…*, op. cit.
[63] A. Piekutowska, A. Skrzypek, *Zrównoważony rozwój i jakość życia jako elementy bezpieczeństwa społecznego*, Ekonomia i Środowisko, nr 3(50), 2014, s. 159-171.
[64] P. Puska, *North Karelia Project – jak odżywianie wpływa…*, op. cit.
[65] *Noncommunicable diseases: Key facts*, World Health Organization, Genewa 2024.

wyzwań – takich jak pandemia COVID-19, niestabilność rynków żywnościowych, rosnące koszty zdrowia publicznego czy zmiany demograficzne – działania w obszarze żywienia powinny być traktowane jako inwestycja w bezpieczeństwo narodowe, a nie wyłącznie jako koszt społeczny.

Mając na uwadze aktualne deficyty systemowe w Polsce oraz dobre praktyki międzynarodowe, zasadne jest sformułowanie następujących rekomendacji:

Opracowanie i wdrożenie narodowej strategii żywieniowej

Niezbędne jest przygotowanie kompleksowego dokumentu strategicznego, który integrowałby działania resortów zdrowia, edukacji, rolnictwa, finansów i cyfryzacji. Strategia powinna opierać się na diagnozie epidemiologicznej i społecznej, zawierać jasno zdefiniowane cele operacyjne, mierzalne wskaźniki realizacji oraz przypisane źródła finansowania. Powinna również uwzględniać różnice regionalne, potrzeby grup wrażliwych (dzieci, seniorzy, osoby z niepełnosprawnościami) oraz mechanizmy monitorowania i korekty działań[66, 67].

Wzmocnienie edukacji żywieniowej

Wprowadzenie systemowej edukacji żywieniowej do podstaw programowych na wszystkich etapach edukacji (od przedszkola po szkoły średnie) powinno stanowić priorytet. Równolegle niezbędne jest prowadzenie długofalowych kampanii społecznych w mediach publicznych i lokalnych, promujących zdrowe nawyki żywieniowe i umiejętności kulinarne. Programy te powinny być prowadzone przez dietetyków i ekspertów zdrowia publicznego, a ich przekaz powinien być oparty na dowodach naukowych i dostosowany kulturowo do różnych grup społecznych[68, 69].

[66] D. Cichoń, *Zdrowie publiczne w kontekście polityki społecznej…*, op. cit.
[67] D. Kołożyn-Krajewska, T. Sikora, *Zarządzanie bezpieczeństwem…*, op. cit.
[68] M. Niewczas-Dobrowolska, *Jakość i bezpieczeństwo…*, op. cit.
[69] M. Górnicka, K. Krupa-Kotara, *Wpływ edukacji zdrowotnej…*, op. cit.

Stymulowanie zdrowych wyborów konsumenckich

Państwo może i powinno wspierać konsumentów w podejmowaniu zdrowych decyzji poprzez instrumenty fiskalne. Rekomenduje się:

- wprowadzenie ulg podatkowych lub subsydiów na produkty korzystne zdrowotnie (np. świeże warzywa i owoce, produkty pełnoziarniste, nabiał naturalny),
- ograniczenie promocji i reklamy żywności wysokoprzetworzonej, słodkich napojów i przekąsek w przestrzeni publicznej, w tym wokół szkół,
- standaryzację etykietowania żywności z uwzględnieniem wartości odżywczych i możliwych alergenów.

Takie działania mogą zmniejszyć presję ekonomiczną na grupy o niższych dochodach i zmniejszyć skalę nierówności żywieniowych[70, 71].

Instytucjonalne wzmocnienie dietetyki jako dziedziny strategicznej

Konieczne jest formalne uznanie dietetyki za strategiczny komponent polityki zdrowia publicznego i bezpieczeństwa państwa. Oznacza to m.in.:

- tworzenie etatów dietetyków w jednostkach samorządu terytorialnego, szkołach, szpitalach i ośrodkach pomocy społecznej,
- powoływanie ekspertów ds. żywienia do gremiów doradczych przy ministerstwach,
- finansowanie interdyscyplinarnych badań naukowych nad wpływem diety na zdrowie populacyjne i wydolność systemów publicznych[72].

Rozwój systemów monitorowania stanu odżywienia populacji

Skuteczna polityka żywieniowa wymaga bieżącej wiedzy o stanie zdrowia i nawykach żywieniowych obywateli. Rekomenduje się wdrożenie systematycznego, ogólnokrajowego monitoringu wskaźników żywieniowych, obejmującego:

- rozpowszechnienie nadwagi, otyłości, niedoborów mikroelementów,

[70] A. Dąbrowska, I. Ozimek, *Bezpieczeństwo żywnościowe konsumentów…*, op. cit.
[71] G. Śmigielska, W. J. Florkowski, *Systemy jakości żywności…*, op. cit.
[72] L. Kłosiewicz-Latoszek, W. B. Szostak, *Żywienie a choroby sercowo-naczyniowe…*, op. cit.

- częstotliwość spożycia produktów podstawowych i wysoko przetworzonych,
- wskaźniki ubóstwa żywnościowego i dostępności ekonomicznej.

Dane te powinny być zbierane z podziałem na regiony, grupy wiekowe i społeczno-ekonomiczne, a ich analiza publikowana corocznie w formie raportów państwowych[73, 74].

Podsumowując, żywienie populacyjne należy traktować jako komponent bezpieczeństwa wewnętrznego, a nie wyłącznie aspekt profilaktyki zdrowotnej. W dobie narastających wyzwań – takich jak zmiany demograficzne, migracje, kryzysy surowcowe, choroby cywilizacyjne – odżywianie staje się nie tylko kwestią zdrowia, ale również czynnikiem strategicznym dla przetrwania i rozwoju państwa. Włączenie dietetyki do głównego nurtu polityki publicznej jest zatem nie wyborem, lecz koniecznością.

Literatura

1. Afshin A. i in., *Health effects of dietary risks in 195 countries, 1990–2017*, The Lancet nr 393(10184), 1958-1972, 2019.
2. *Bezpieczeństwo kompleksowe Finlandii: znaczenie odporności społeczeństwa*, Instytut Europy Środkowej, Lublin 2023, https://ies.lublin.pl/komentarze/bezpieczenstwo-kompleksowe-finlandii-znaczenie-odpornosci-spoleczenstwa/
3. Biuro Bezpieczeństwa Narodowego, *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020.
4. Black R. E., Victora C. G., Walker S. P., Maternal and Child Nutrition Study Group, *Maternal and child undernutrition and overweight in low-income and middle-income countries*, The Lancet, nr 382(9890), 427-451, 2013.
5. Cichoń D., *Zdrowie publiczne w kontekście polityki społecznej i bezpieczeństwa państwa*, Zdrowie i Bezpieczeństwo, nr 6(1), 45-56, 2022.
6. Dąbrowska A., Ozimek I., *Bezpieczeństwo żywnościowe konsumentów w Polsce – wybrane aspekty*, Handel Wewnętrzny, nr 4(351), 55-79, 2014.
7. *Informacja o wynikach kontroli: Marnowanie żywności w Polsce*, Najwyższa Izba Kontroli, Warszawa 2022.
8. *Inspekcje bezpieczeństwa żywności w Holandii – podsumowanie 2023 roku*, FoodFakty, 2024, https://foodfakty.pl/inspekcje-bezpieczenstwa-zywnosci-w-holandii-podsumowanie-2023-roku.

[73] *Stan zdrowia ludności Polski w 2021 roku*, Główny Urząd Statystyczny, Warszawa 2022.

[74] *Niedożywienie i głód w Polsce: Raport Banków Żywności*, Federacja Polskich Banków Żywności, Warszawa 2023.

9. *Japonia inwestuje w przemysł mięsa hodowanego komórkowo, by wzmocnić zrównoważone dostawy żywności*, FoodFakty, 2023, https://foodfakty.pl/japonia-inwestuje-w-przemysl-miesa-hodowanego-komorkowo-by-wzmocnic-zrownowazone-dostawy-zywnosci.
10. *Oznaczania alergenów na etykietach produktów spożywczych – nowe przepisy w Holandii*, FoodFakty, 2025, https://foodfakty.pl/oznaczania-alergenow-na-etykietach-produktow-spozywczych-nowe-przepisy-w-holandii.
11. Górnicka M., Krupa-Kotara K., *Wpływ edukacji zdrowotnej na wybory żywieniowe dzieci i młodzieży*, Problemy Higieny i Epidemiologii, nr 100(3), 2019.
12. Hoddinott J., Alderman H., Behrman J. R., Haddad L., Horton S., *The economic rationale for investing in stunting reduction*, Maternal & Child Nutrition, nr 9(S2), 2013.
13. Kłosiewicz-Latoszek L., Szostak W. B., *Żywienie a choroby sercowo-naczyniowe – fakty i mity*, Forum Profilaktyki, nr 1(10), 2008.
14. Kołożyn-Krajewska D., Sikora T., *Zarządzanie bezpieczeństwem żywności: Teoria i praktyka*, Wydawnictwo Naukowe PWN, Warszawa 2010.
15. Kozłowska-Burdziak M., *Warunki bezpieczeństwa żywnościowego Polski (ze szczególnym uwzględnieniem dostępności ekonomicznej)*, Optimum. Studia Ekonomiczne, nr 3(99), 2019.
16. Niewczas-Dobrowolska M., *Jakość i bezpieczeństwo żywności: Systemy – postawy – konsumenci*, Wydawnictwo Naukowe PTTŻ, Kraków 2021.
17. *Noncommunicable diseases: Key facts*, World Health Organization, Genewa 2024.
18. *Niedożywienie i głód w Polsce: Raport Banków Żywności*, Federacja Polskich Banków Żywności, Warszawa 2023.
19. Piekutowska A., Skrzypek A., *Zrównoważony rozwój i jakość życia jako elementy bezpieczeństwa społecznego*, Ekonomia i Środowisko, nr 3(50), 2014.
20. *Policy Brief: Food Security*, Food and Agriculture Organization, Rzym 2006.
21. Puska P., *North Karelia Project – jak odżywianie wpływa na choroby układu krążenia*, Narodowe Centrum Edukacji Żywieniowej, 2016, https://ncez.pzh.gov.pl/choroba-a-dieta/north-karelia-project-jak-odzywianie-wplywa-na-choroby-ukladu-krazenia/.
22. PZH, *Dieta długowieczności z Okinawy*, Narodowe Centrum Edukacji Żywieniowej, 2018, https://ncez.pzh.gov.pl/abc-zywienia/dieta-dlugowiecznosci-z-okinawy/.
23. Rey R., *Społeczeństwo odporne na zagrożenia*, Rządowe Centrum Bezpieczeństwa, Warszawa 2020.
24. *Rekordowy rok wycofań produktów spożywczych w Szwecji – bezpieczeństwo żywności pod lupą*, SkandynawiaInfo, 2024, https://skandynawiainfo.pl/rekordowy-rok-wycofan-produktow-spozywczych-w-szwecji-bezpieczenstwo-zywnosci-pod-lupa/.
25. *Stan zdrowia ludności Polski w 2021 roku*, Główny Urząd Statystyczny, Warszawa 2022.
26. Szarfenberg R., *Poverty Watch 2024: Ubóstwo dzieci w Polsce*, Europejska Sieć Przeciwdziałania Ubóstwu – Polska, Warszawa 2024.
27. Szczepaniak I., *Ocena bezpieczeństwa żywnościowego i samowystarczalności żywnościowej Polski na tle państw Unii Europejskiej*, International Business and Global Economy nr 37, 2018.

28. *Szwecja chce zwiększyć produkcję żywności*, Farmer, 2025, https://www.farmer.pl/agroskop/analizy-i-komentarze/szwecja-chce-zwiekszyc-produkcje-zywnosci%2C159539.html.
29. Śmigielska G., Florkowski W. J., *Systemy jakości żywności a dobrostan społeczny i bezpieczeństwo żywnościowe*, Problemy Rolnictwa Światowego, nr 15(1), 2015.
30. *Ubóstwo w Polsce w 2021 roku*, Główny Urząd Statystyczny, Warszawa 2022.

dr Małgorzata Waksmundzka-Szarek
Uniwersytet Rzeszowski
ORCID: 0000-0002-9609-8270

dr Piotr Zalewski
Uniwersytet Jana Kochanowskiego w Kielcach
ORCID: 0000-0002-0997-8561

https://doi.org/10.29316/9788368103205_13

BEZPIECZEŃSTWO INDYWIDUALNE MIESZKAŃCÓW WOJEWÓDZTWA PODKARPACKIEGO W KONTEKŚCIE WYDARZEŃ ZWIĄZANYCH Z DRUGIM ETAPEM WOJNY W UKRAINIE – WYBRANE ZAGADNIENIA

INDIVIDUAL SECURITY OF THE RESIDENTS OF THE PODKARPACKIE PROVINCE IN THE CONTEXT OF EVENTS RELATED TO THE SECOND STAGE OF THE WAR IN UKRAINE – SELECTED TOPICS

Streszczenie

Celem rozdziału jest analiza postrzegania bezpieczeństwa przez mieszkańców województwa podkarpackiego w kontekście wojny w Ukrainie oraz ocena ich reakcji i gotowości na potencjalne zagrożenia. Region ten od lutego 2022 r. pełni funkcję recepcyjną dla uchodźców oraz tranzytową

Summary

The aim of the chapter is to analyze the perception of security by the inhabitants of the Podkarpackie Voivodeship in the context of the war in Ukraine and to assess their response and readiness to potential threats. Since February 2022, this region has been a reception area for refugees and a transit

dla pomocy międzynarodowej, co istotnie wpłynęło na lokalne poczucie bezpieczeństwa. W rozdziale omówiono ewolucję pojęcia bezpieczeństwa – od klasycznego, państwowego wymiaru, do indywidualnego i subiektywnego odczuwania zagrożeń przez jednostkę. Problem badawczy sformułowano: W jaki sposób wojna w Ukrainie wpływa na poczucie bezpieczeństwa mieszkańców województwa podkarpackiego oraz ich gotowość do działań przygotowawczych? Przeprowadzone w 2024 r. badania empiryczne na próbie mieszkańców wykazały podzielone opinie: część respondentów dostrzegała wysoki poziom zagrożenia i wyrażała obawy, jednak większość nie podjęła konkretnych działań przygotowawczych. Respondenci częściej wskazywali sąsiednie województwa jako bezpieczniejsze od własnego. Pomimo realnego ryzyka nie zaobserwowano paniki, a badania odzwierciedliły etap przejściowy między reakcją kryzysową a oswojeniem z sytuacją. Wyniki podkreślają znaczenie większego zaangażowania społeczeństwa w działania zwiększające odporność oraz konieczność intensyfikacji edukacji w zakresie zarządzania kryzysowego. W rozdziale odniesiono się jedynie do wybranych wniosków. W badaniach wykorzystano metodę sondażu diagnostycznego z zastosowaniem techniki ankietowania opartej na autorskim kwestionariuszu ankiety.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo indywidualne, poczucie bezpieczeństwa, migracja, uchodźcy

service for international aid, which has significantly affected the local sense of security. The chapter discusses the evolution of the concept of security – from the classical, state dimension to the individual and subjective perception of threats by the individual. The research problem was formulated: How does the war in Ukraine affect the sense of security of the inhabitants of the Podkarpackie Voivodeship and their readiness for preparatory activities? Empirical research conducted in 2024 on a sample of residents showed divided opinions: some respondents perceived a high level of threat and expressed concerns, but most did not take specific preparatory measures. Respondents more often indicated the neighbouring voivodeships as safer than their own. Despite the real risk, no panic was observed, and the research reflected a transitional stage between crisis response and familiarization. The results highlight the importance of greater public involvement in resilience activities and the need to intensify crisis management education. The chapter refers only to selected conclusions. The study used the method of a diagnostic survey with the use of a questionnaire technique based on the author's questionnaire.

Keywords: security, individual security, sense of security, migration, refugees

Wstęp

Bezpieczeństwo, to jedno z tych słów, które od zawsze odmieniane jest przez człowieka przez wszystkie przypadki, ale jest to również pojęcie odnoszące się do szerokiego spektrum działań i zaniechań człowieka jako jednostki

albo społeczeństw oraz tworów instytucjonalnych. Historycznie, pojęcie bezpieczeństwa łączone było z państwem jako podmiotem bezpieczeństwa i zwykle ograniczało się do zagadnień związanych z wojną i konfliktem, ponieważ przez wiele stuleci wojny były podstawowym instrumentem „polityki bezpieczeństwa" państwa, którego aktywność w tym zakresie sprowadzała się do przygotowań obronnych przed obcą agresją albo do budowania potencjału swoich możliwości ofensywnych. Przełom w szerokim postrzeganiu bezpieczeństwa nastąpił dopiero w XX wieku, kiedy to w wyniku trwającej „zimnej wojny" bezpieczeństwo zaczęto rozumieć również inaczej niż tylko jako określony stan rzeczy. W stosunkach międzynarodowych i dyskursie naukowym bezpieczeństwo zaczęło być traktowane jako fenomen społeczno-kulturowy o zmiennej dynamice i intensywności, którego podmiotem stał się człowiek[1]. Zatem identyfikowanie i eliminowanie zagrożeń poprzez zaangażowanie i aktywność podmiotów bezpieczeństwa stało się podstawowym celem samym w sobie, który w konsekwencji powinien zapewniać „możliwości przetrwania i swobody realizacji własnych interesów w konkretnych warunkach, wykorzystując okoliczności sprzyjające (szanse), podejmując wyzwania, redukując ryzyka oraz przeciwdziałając (zapobiegając, przeciwstawiając się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów"[2].

Bezpieczeństwo rozpatrywane z perspektywy jednostki ludzkiej określane jest jako bezpieczeństwo personalne lub osobiste. Wiąże się ono z pojęciem bezpieczeństwa humanitarnego, które najogólniej dotyczy bezpieczeństwa człowieka niezależnie od jego rasy, płci czy narodowości. Współcześnie rozumiane jest także jako „wolność od zagrożeń i wolność od potrzeb" (ang. *freedom from fear and freedom from want*)[3]. Działania podejmowane przez Organizację Narodów Zjednoczonych (ONZ), których wyrazem był raport Narodów Zjednoczonych ds. Rozwoju (UNDP) upowszechniły koncepcję *human security*, jako paradygmatu wszelkich działań państwa i organizacji międzynarodowych na rzecz ochrony każdego człowieka[4]. W rozdziale jako

[1] A. Kołodziejczyk, *Bezpieczeństwo jako fenomen społeczny. Pojęcie bezpieczeństwa, jego interpretacje i odmiany*, Saeculum Christianum, vol. 4, nr 1, 2007, s. 223-252.

[2] S. Koziej, *Podstawy bezpieczeństwa międzynarodowego i narodowego*, Myśl Wojskowa, nr 4, 2005, s. 8.

[3] L. Chojnowski, *Bezpieczeństwo. Zarys teorii*, Uniwersytet Pomorski w Słupsku, Słupsk 2015, s 120.

[4] United Nations Development Program, *Human Development Report 1994*, New York 1994.

punkt odniesienia przyjęto postrzeganie bezpieczeństwa indywidualnego przez mieszkańców zamieszkujących województwo podkarpackie, które jako jednostka administracyjnego podziału Polski oraz regionu geograficznego, znajduje się w bezpośrednim sąsiedztwie z Ukrainą. Wykorzystano metody analityczno-opisowe, które pozwoliły na identyfikację i kategoryzację kluczowych pojęć, a także analizę systemową wpływu migracji uchodźczej i działań zbrojnych na terenie Ukrainy, na działania administracji publicznej w Polsce.

Człowiek jako podmiot bezpieczeństwa

Człowiek jako podmiot bezpieczeństwa przedstawiony został w literaturze przedmiotu szczegółowo. Należy jednak zauważyć, że człowiek jako jednostka w większości definicji odnoszących się do bezpieczeństwa nie występuje indywidualnie, ale jako część narodu. O procesowym wymiarze bezpieczeństwa, w którym ważną rolę odgrywają podmioty pisze R. Zięba, który definiuje pojęcie bezpieczeństwa w następujący sposób „w najogólniejszym znaczeniu bezpieczeństwo można więc określić jako pewność istnienia i przetrwania, stanu posiadania oraz rozwoju podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń (ich niewystępowania lub eliminowania). Powstaje także wskutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego”[5]. Pewność, to wszystko co człowiek ceni najbardziej, a więc życie (istnienie), zdrowie, wolność, niezależność, jakość życia, stan posiadania czy możliwość rozwoju. Zatem możliwość częściowej lub całkowitej utraty tych istotnych dla jednostki wartości spowoduje sytuację zagrożenia – braku bezpieczeństwa.

Bogdan M. Szulc zaważył, że istotę bezpieczeństwa trafnie określił trójwymiarowo – podmiotowo, przedmiotowo i procesualnie J. Kukułka,[6]. J. Kukułka stwierdził również, że: niezaspokojona potrzeba bezpieczeństwa wyrządza szkody jednostce czy grupie społecznej, gdyż destabilizuje jej tożsamość i funkcjonowanie. Przejawiają one wówczas tendencję do zmiany istniejącego stanu rzeczy, do oporu wobec niekorzystnych zmian w sferze

[5] R. Zięba (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008, s. 16.

[6] B. M. Szulc, *Bezpieczeństwo a nauki o bezpieczeństwie*, Wydawnictwo Adam Marszałek, Toruń 2024 r., s. 112.

zewnętrznej i do stosowania środków ochronnych, mogących przywrócić im poczucie bezpieczeństwa. Tendencje tego rodzaju dowodzą, że bezpieczeństwo jest nie tylko określonym stanem rzeczy, ile ciągłym procesem społecznym, w ramach którego działające podmioty starają się doskonalić mechanizmy zapewniające im poczucie bezpieczeństwa"[7]. Najbardziej zatem realnym podmiotem bezpieczeństwa pozostaje tym samym jednostka, która w zależności od swoich potrzeb i możliwości łączy się w grupy, tworząc zbiorowości społeczne. Każdy natomiast może inaczej postrzegać pożądany stan bezpieczeństwa.

W przedmiotowej literaturze można odnaleźć sporo informacji na temat podmiotów bezpieczeństwa, które definiowane są zwykle przez rozmaite kryteria. Autorzy, na potrzeby przyjętego celu badawczego posłużyli się koncepcją poziomów analizy bezpieczeństwa zaproponowaną przez B. Buzana, O. Wævera i J. de Wilda, którzy wyróżnili: poziom systemu międzynarodowego – dotyczący bezpieczeństwa w wymiarze globalnym; podsystem międzynarodowy, który obejmuje bezpieczeństwo regionalne; poziom jednostki, który odnosi się głównie do bezpieczeństwa państwa i narodu, lecz także innych podmiotów, które wywierają wpływ na podsystem międzynarodowy; poziom podmiotów funkcjonujących w państwie, który dotyczy bezpieczeństwa np. rodziny, społeczności lokalnych, grup etnicznych i mniejszości narodowych; poziom jednostki ludzkiej, który obejmuje bezpieczeństwo osobiste, personalne czy też humanitarne[8].

Najprostszym wyrazem bezpieczeństwa personalnego będzie określenie tego pojęcia jako stanu, kiedy jednostka nie odczuwa żadnych zagrożeń, chociaż one potencjalnie istnieją, to jednak nie są uświadomione w danym momencie, przez co jednostka ich nie odczuwa. Szczególnie, jeżeli weźmiemy pod uwagę wszelkie zagrożenia związane z codzienną egzystencją człowieka zaczynając, a kończąc na potrzebach i wartościach. Zagrożenia rozumiane jako coś co negatywnie wpływa na funkcjonowanie jednostki, narusza jej funkcjonowanie, wartości oraz możliwość rozwoju. Analiza subiektywnego postrzegania

[7] J. Kukułka, *Nowe uwarunkowania i wymiary bezpieczeństwa międzynarodowego Polski*, „Wieś i Państwo", 1995, nr 1, s. 198-199. Cytat za: L. Chojnowski, *Bezpieczeństwo. Zarys teorii*, Wydawnictwo Akademii Pomorskiej w Słupsku, Słupsk 2012, s. 22.

[8] B. Buzan, O. Wæver, J. de Wilde, Security. A New Framework For Analysis, Lynne Rienner Publisher, Boulder-London 1998, s. 5-7. Za: L. Chojnowski, *Bezpieczeństwo. Zarys teorii*, Wydawnictwo Akademii Pomorskiej w Słupsku, Słupsk 2012, s. 87.

obiektywnych aspektów zagrożeń lub ich braku stanowi podstawę modelu oceny bezpieczeństwa D. Freia, dla którego subiektywizm ten może oznaczać brak bezpieczeństwa, w sytuacji występowania poważnych, rzeczywistych zagrożeń, przy ich prawidłowym postrzeganiu przez podmiot; stan bezpieczeństwa, w przypadku występowania nieznacznych zagrożeń lub ich brak, przy ich prawidłowym postrzeganiu; mispercepcję, czyli fałszywe postrzeganie bezpieczeństwa i błędne postrzeganie zagrożeń, które może oznaczać stan obsesji (odczuwanie zagrożeń w sytuacji, gdy w rzeczywistości one nie występują bądź też są nieznaczne, a postrzega się je jako duże, oceniane nieproporcjonalnie do skali ich rzeczywistego występowania), czy też stan fałszywego bezpieczeństwa, kiedy podmiot nie dostrzega obiektywnie występujących zagrożeń, ignoruje je bądź też błędnie interpretuje skalę ich występowania, co sprawia, że poważne zagrożenia postrzegane są jako niewielkie[9].

Wielu badaczy, również w Polsce[10] zwraca uwagę na pojęcie *kultury bezpieczeństwa*. Pierwszą definicję kultury w XIX wieku stworzył Edward Tylor[11], według którego kultura obejmuje wiedzę, wierzenia, sztukę, moralność, prawo, obyczaje i inne zdolności zdobyte przez człowieka jako członka społeczeństwa. Uzupełnia ją koncepcja kultury zaproponowana przez Alfreda Louisa Kroebera, która stanowi inspirację dla idei filarów kultury bezpieczeństwa – rzeczywistości materialnej, kultury społecznej i kultury etycznej oraz związanego z nią systemu wartości[12]. Natomiast w Polsce, Marian Cieślarczyk zauważył, że obronność przekracza granicę przygotowania militarnego,

[9] D. Frei, *Sicherheit. Grundfragen der Weltpolitik*, Verlag W. Kohlhammer, Stuttgart 1997, s. 17-21. Cytat za: L. Chojnowski, *Bezpieczeństwo. Zarys teorii* …, op. cit., s. 17.

[10] Marian Cieślarczyk zaproponował definicję kultury bezpieczeństwa i obronności, wg niego jest to „wzór podstawowych założeń, wartości, norm, reguł, symboli i przekonań, wpływających na sposób postrzegania wyzwań, szans i (lub) zagrożeń, a także sposób odczuwania bezpieczeństwa i myślenia o nim oraz związany z tym sposób zachowania i działań (współdziałania) podmiotów [bezpieczeństwa], w różny sposób przez te podmioty »wyuczonych« i wyartykułowanych w procesach szeroko rozumianej edukacji, w tym również w naturalnych procesach wewnętrznej integracji i zewnętrznej adaptacji oraz w innych procesach organizacyjnych, a także w procesie umacniania szeroko (nie tylko militarnie) rozumianej obronności, służących w miarę harmonijnemu rozwojowi tych podmiotów i osiąganiu przez nie najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie, ale i otoczenia", M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2010, s. 210.

[11] J. Piworwarski, *Trzy filary kultury bezpieczeństwa*, Kultura Bezpieczeństwa Nauka – Praktyka – Refleksje, Nr 30, 2018, s. 10.

[12] Ibidem, s. 10.

a odnosi się przede wszystkim do skutecznego przeciwdziałania i zapobiegania zaistnieniu zagrożeń oraz przeciwstawienie się zagrożeniom z chwilą ich realnego wystąpienia. Zapewnienie bezpieczeństwa jest warunkiem przetrwania dla jednostki oraz jej rozwoju, czyli również kultury.

K. Najder-Stefaniak zauważa, że pojęcie człowieka jako indywidualnego podmiotu bezpieczeństwa należy rozumieć w kontekście obiektywnym i subiektywnym, gdzie subiektywność oznacza wewnętrznie pojmowany stan pewności, spokoju, braku poczucia zagrożenia[13]. Subiektywne odczuwanie bezpieczeństwa lub jego braku, pomimo obiektywnie istniejącego otoczenia zewnętrznego i stanu wewnętrznego podmiotu, może prowadzić do jego fałszywego postrzegania (mispercepcja), co w znaczący sposób będzie wpływać na ocenę poziomu psychologicznie rozumianego bezpieczeństwa, nazywanego poczuciem bezpieczeństwa. Zdaniem P. Gromka w ujęciu ogólnym poczucia bezpieczeństwa istotny jest nie tyle sam fakt występowania zagrożenia, ale związane z nim ryzyko, do którego dany podmiot może się subiektywnie ustosunkować odczuwając niepewność lub lęk[14]. Subiektywne podejście do bezpieczeństwa w znacznym stopniu utrudnia rzeczywistą ocenę poziomu bezpieczeństwa obiektywnego. Wynika to z doświadczeń historycznych podmiotu i grup społecznych, bieżącej oceny trafności działań podejmowanych przez państwo w celu neutralizacji zagrożeń, zaufania lub jego braku do innych podmiotów, które mogą być traktowane jako przyjaciele bądź wrogowie.

Rozwijając powyższy pogląd R. Zięba uważa, że ten „psychologizujący model" przedstawia istotną wartość heurystyczną, ponieważ pozwala dokonywać analizy bezpieczeństwa, jako sytuacji konfliktowej, gdzie zagrożenia pojawiają się i występują obiektywnie w otaczającej podmiot rzeczywistości, natomiast ich subiektywne postrzeganie w sferze świadomości podmiotu kształtuje poczucie pewności i przetrwania, co w znacznym stopniu falsyfikuje lub uwiarygadnia politykę bezpieczeństwa realizowaną przez państwo i jego administrację[15].

[13] K. Najder-Stefaniak, *O bezpieczeństwie człowieka. Refleksja inspirowana filozofią Alberta Schweitzera*, [w:] *Wspólnotowość i postawa uniwersalistyczna 2010-2011*, red. A. Górski, nr 7, Wydawnictwo Polskie Towarzystwo Uniwersalizmu, Warszawa 2010, s. 55.

[14] P. Gromek, *Poczucie bezpieczeństwa a badania w dyscyplinie nauk o bezpieczeństwie*, Zeszyty Naukowe SGSP, nr 78, 2021, s. 40-41.

[15] R. Zięba, *Instytucjonalizacje bezpieczeństwa europejskiego*, Wydawnictwo Naukowe Scholar, Warszawa 1999, s. 27.

Wspomniany już wcześniej program Narodów Zjednoczonych do spraw Rozwoju (United Nations development Program – UNDP), który w latach 90-tych XX wieku spopularyzował termin *human security* (bezpieczeństwo jednostki, osobiste lub inaczej personalne) zakładał, że w pewnym sensie jest to koncepcja o charakterze uniwersalnym, która obejmuje wszystkich ludzi na świecie i odchodzi od bezpieczeństwa państwa, uważając, że bezpieczeństwo człowieka jest tutaj pierwszoplanowe i powinno koncentrować się na działaniach zapobiegawczych, bowiem działania interwencyjne są dużo bardziej problematyczne. Nawiązywało to do wcześniej prowadzonych badań nad bezpieczeństwem jednostki prowadzonych przez środowiska tzw. szkoły „japońskiej" i „kanadyjskiej"[16]. Współcześnie wydaje się, że obserwujemy odejście od koncepcji postrzegania bezpieczeństwa przez podmiot bezpieczeństwa, którym jest człowiek jako jednostka, na rzecz narodu, a przede wszystkim państwa, co wynika z sytuacji niepewności i wzrastania zagrożeń międzynarodowych w konwencjonalnym rozumieniu.

Bezpieczeństwo indywidualne mieszkańców województwa podkarpackiego w świetle badań własnych

W rozdziale ujęto wybrane wstępne wyniki badań empirycznych na temat postrzegania przez mieszkańców województwa podkarpackiego bezpieczeństwa w regionie, który zamieszkują, wobec sytuacji, kiedy od 24 lutego 2022 r., pełniło ono funkcję recepcyjną dla uchodźców wojennych z Ukrainy, a także tranzytową dla realizacji różnych form pomocy świadczonej Ukrainie przez społeczność międzynarodową. Kinetyczna faza konfliktu, jaka 24 lutego 2022 r., rozpoczęła się w Ukrainie, dała początek niespotykanej w historii Polski od czasów II wojny światowej fali migracji uchodźczej, której natężenie i skoncentrowanie się na terenie dwóch przygranicznych województw - podkarpackiego i lubelskiego, stało się ogromnym wyzwaniem dla całego państwa w wymiarze politycznym, administracyjnym oraz logistycznym.

[16] Szkoła „japońska" badania koncentruje wokół zagadnienia *freedom from want*, polegającego na organizowaniu wysiłków na rzecz wzmacniania obszarów, które by mogły zagrozić życiu ludzkiemu, natomiast szkoła „kanadyjska" zajmuje się kierunkiem *freedom from fear*, gdzie więcej uwagi poświęca się na konieczność realizacji misji humanitarnych również wojskowych w celu ochrony życia i praw człowieka, K. R. Zieliński, *Bezpieczeństwo indywidualne*, Pedagogika Społeczna, nr 3(85), 2022, s. 31.

Według danych Wysokiego Komisarza Narodów Zjednoczonych do spraw Uchodźców (UNHCR), począwszy od 24 lutego do końca marca 2022 r., Ukrainę opuściło 4,1 mln osób. Najwięcej osób wyjechało z Ukrainy na początku konfliktu, z kulminacją 6 i 7 marca, gdy kraj opuszczało ponad 200 tys. osób dziennie, następnie dzienna liczba uchodźców zaczęła maleć i ustabilizowała się w ostatnim tygodniu marca na ok. 50-60 tys. osób dziennie. Spośród państw graniczących z Ukrainą najwięcej osób wyjechało do Polski – 31 marca było to 2384,8 tys. osób, czyli 57,6% wszystkich osób, które wyjechały z Ukrainy. Kolejnym krajem pod tym względem była Rumunia z 623,6 tys. osób, Mołdawia z 390,2 tys. osób oraz Węgry z 374,5 tys. osób. W kwietniu odnotowano natomiast powroty uchodźców na Ukrainę. W połowie kwietnia ONZ szacowało, że do kraju wróciło 870 tys. uchodźców, z czego ok. 650 tys. przekroczyło granicę polsko-ukraińską[17]. Od samego początku wydarzeń województwo podkarpackie zostało doświadczone szeregiem wyzwań związanych z niesieniem działań pomocowych, nie tylko ze względu na swoje położenie przygraniczne, ale również z powodu posiadanej infrastruktury i znajdujących się tutaj drogowych przejść granicznych z Ukrainą w Medyce, Korczowej, Krościenku i Lubaczowie, kolejowego przejścia granicznego w Medyce ze stacją w Przemyślu oraz portu lotniczego w Rzeszowie Jasionce, który pełnił rolę *hubu* pomocowego i tranzytowego dla ruchu VIP. Na terenie województwa podkarpackiego rozlokowano również kwatery wojsk sojuszniczych NATO.

Podczas realizacji badań kierowano się założeniami teoretycznymi F. Znanieckiego, który uważał, że dla zbadania określonej rzeczywistości społecznej mniejsze znaczenie ma badanie obiektywnych faktów, zjawisk, procesów zachodzących w danej rzeczywistości, a większe znaczenie ma subiektywne postrzeganie zagrożeń danej rzeczywistości oraz jej ocena przez mieszkańców konkretnego regionu i terytorialnie powiązanej grupy społecznej[18]. W badaniach wykorzystano także metodę sondażu diagnostycznego z zastosowaniem techniki ankietowania opartej na autorskim kwestionariuszu ankiety.[19] Badania empiryczne mieszkańców podkarpacia realizowane były od

[17] Operational Data Portal UNHCR, *Ukraine Refuge Situation (since 24 February 2022)*, www.data.unhcr.org/en/situations/ukraine, [dostęp: 15.04.2025].

[18] F. Znaniecki, *Poznań w świadomości jego obywateli. Z badań Polskiego Instytutu Socjologicznego nad miastem Poznaniem*, Poznań 1931, s. 6-15.

[19] Wśród przedstawicieli nauki w Polsce temat badań bezpieczeństwa w społeczności lokalnej podejmowany był wielokrotnie przez m.in. E. Moczuk, *Postrzeganie bezpieczeństwa*

10 marca do 6 maja 2024 roku. Badania realizowane były za pomocą techniki ankiety. Narzędziem badawczym był kwestionariusz ankiety rozsyłany online (dzięki wygenerowanemu linkowi). Jako zmienne niezależne w ustalaniu niektórych zależności wyników badań od cech społeczno-demograficznych uwzględniono: płeć, wiek, miejsce zamieszkania, ocenę własnych warunków materialnych.

W badaniu wzięło udział 678 osób, spośród których 53,8% stanowiły kobiety, a 46,2% mężczyźni (tabela 1).

Tabela 1. Płeć respondentów

	Częstość	Procent
Kobieta	365	53,8%
Mężczyzna	313	46,2%
Ogółem	678	100%

Źródło: badania własne.

Tabela 2. Wiek respondentów

	Częstość	Procent
do 24 lat	29	4,3%
25–34 lata	33	4,9%
35–44 lata	401	59,1%
45–54 lata	165	24,3%
55–64 lata	31	4,6%
65 lat i więcej	19	2,8%
Ogółem	678	100%

Źródło: badania własne.

publicznego w środowisku lokalnym: raport z badań sondażowych, Rzeszów 2003; idem, *Mieszkańcy powiatu mieleckiego wobec problemów bezpieczeństwa lokalnego, Rzeszów 2007*. P. Mickiewicz, *Bezpieczeństwo społeczności lokalnych. Organizacja systemu i projektowanie działań*, Poznań 2020. M. Leszczyński [i in.], *Bezpieczeństwo w wymiarze lokalnym. Wybrane obszary*, Warszawa 2016. T. Serafin, S. Parszowski, *Bezpieczeństwo społeczności lokalnych. Programy prewencyjne w systemie bezpieczeństwa*, Warszawa 2011. A. Urban, *Bezpieczeństwo społeczności lokalnych*, Warszawa 2011. B. Bronisławska, *Zadania administracji samorządowej w zakresie bezpieczeństwa lokalnego*, „Zeszyty Naukowe WSEI seria: Administracja", 2012, nr 2; eadem, *Zadania administracji samorządowej w zakresie bezpieczeństwa publicznego – wybrane zagadnienia*, „Teka of Political Science and International Relations", 2021, nr 2. G. Bonusiak, D. Boratyn, *Bezpieczeństwo społeczności lokalnych*, Rzeszów 2020. E. Moczuk, D. Boratyn, *Postrzeganie bezpieczeństwa lokalnego przez mieszkańców województwa podkarpackiego – wyniki badań empirycznych w 2023 roku*, Polityka i społeczeństwo, 2(22), 2024.

W tabeli 2 przedstawiono wiek respondentów. Największy odsetek, bo 59,1% respondentów, mieścił się w przedziale wiekowym od 35 do 44 lat. Następne w kolejności były osoby w wieku od 45 do 54 lat (24,3%) oraz od 25 do 34 lat (4,9%). Osoby w wieku do 24 lat stanowiły 4,3% respondentów, a osoby w wieku od 55 do 64 lat – 4,6%. Najniższy odsetek, bo 2,8%, stanowiły osoby w wieku 65 lat i więcej. Na podstawie tych danych można przyjąć, że najwięcej respondentów mieściło się w średnim wieku, tj. między 35 a 44 rokiem życia.

Tabela 3. Wykształcenie respondentów

	Częstość	**Procent**
Podstawowe	3	0,5%
Zasadnicze zawodowe	2	0,3%
Średnie	169	25,4%
Wyższe	492	73,9%
Ogółem	666	100%

* 12 osób nie udzieliło odpowiedzi.

Źródło: badania własne.

W tabeli 3 przedstawiono poziom wykształcenia respondentów. Największy odsetek, bo aż 73,9% respondentów, posiadało wyższe wykształcenie. Kolejne 25,4% respondentów miało wykształcenie średnie. Pojedyncze przypadki stanowiły osoby z wykształceniem podstawowym (0,5%) oraz zasadniczym zawodowym (0,3%). Na podstawie tych danych można przyjąć, że większość respondentów posiadała wyższe wykształcenie.

Pytania metryczkowe odnosiły się również do miejsca zamieszkania respondentów (tabela 4). Najwyższy odsetek respondentów (32,5%), zamieszkiwał miasta powyżej 100 tysięcy mieszkańców. Kolejne 25,8% respondentów zamieszkiwało wieś. 17,7% respondentów było mieszkańcami miast do 25 tysięcy mieszkańców, a 15,3% w miastach od 50,1 do 100 tysięcy mieszkańców. Natomiast 8,7% respondentów mieszkało w miastach od 25,1 do 50 tysięcy mieszkańców. Na podstawie tych danych można zauważyć, że respondenci reprezentowali różne typy osadnictwa, ale najwyższy odsetek z nich mieszkał w dużych miastach.

Tabela 4. Miejsce zamieszkania respondentów

	Częstość	Procent
Wieś	175	25,8%
Miasto do 25 tys. mieszkańców	120	17,7%
Miasto 25,1 – 50 tys. mieszkańców	59	8,7%
Miasto 50,1– 100 tys. mieszkańców	104	15,3%
Miasto powyżej 100 tys. mieszkańców	220	32,5%
Ogółem	678	100%

Źródło: badania własne.

Respondentom zadano ponadto pytanie o ich stan cywilny (tabela 5). Najwyższy odsetek respondentów stanowiły osoby żonate lub zamężne (84,2%). 13,2% respondentów było kawalerami lub pannami. 1,8% respondentów było rozwiedzionych, a 0,8% to wdowcy lub wdowy. Na podstawie tych danych można stwierdzić, że większość respondentów pozostawało w związku małżeńskim.

Tabela 5. Stan cywilny respondentów

	Częstość	Procent
Kawaler/panna	88	13,2%
Żonaty/zamężna	561	84,2%
Rozwiedziony/rozwiedziona	12	1,8%
Wdowiec/wdowa	5	0,8%
Ogółem	666	100%

* 12 osób nie udzieliło odpowiedzi.

Źródło: badania własne.

Główna część kwestionariusza ankiety odnosiła się do badań właściwych, a mianowicie do określenia poczucia bezpieczeństwa badanych w ich społeczności lokalnej, w województwie podkarpackim. Pytaniem otwierającym ten blok tematyczny było pytanie „Czy czujesz się bezpiecznie mieszkając w województwie podkarpackim po inwazji Rosji na Ukrainę?" (tabela 6). Analizując odpowiedzi badanych wskazuje, że najwyższy odsetek respondentów, bo 27,7%, udzieliło odpowiedzi „raczej nie". Natomiast, 19 % stwierdziło, że „zdecydowanie nie" czują się bezpiecznie, 27,7% odpowiedziało „raczej tak", a 5,6% stwierdziło, że „zdecydowanie tak". Natomiast, 19,9% respondentów odpowiedziało „trudno powiedzieć". Na podstawie tych danych można stwierdzić, że opinie na temat poczucia bezpieczeństwa w województwie

podkarpackim po inwazji Rosji na Ukrainę były dosyć podzielone, przy czym znaczna część respondentów miała trudności z wyrażeniem jednoznacznej opinii, szczególnie, kiedy porównamy odpowiedzi raczej tak i raczej nie, z tym samym rezultatem.

Tabela 6. Rozkład odpowiedzi na pytanie: „Czy czujesz się bezpiecznie mieszkając w województwie podkarpackim po inwazji Rosji na Ukrainę?"

	Częstość	Procent
Zdecydowanie nie	129	19,0%
Raczej nie	188	27,7%
Trudno powiedzieć	135	19,9%
Raczej tak	188	27,7%
Zdecydowanie tak	38	5,6%
Ogółem	678	100%

Źródło: badania własne.

Następne ważne pytanie zadane respondentom odnosiło się do opinii badanych na temat bezpieczeństwa w województwach sąsiadujących z Podkarpaciem.

Tabela 7. Rozkład odpowiedzi na pytanie: „Czy województwa sąsiadujące z podkarpaciem uważasz za…?"

	Częstość	Procent
Mniej bezpieczne niż podkarpacie	20	3,1%
Tak samo bezpieczne/niebezpieczne jak podkarpacie	268	40,5%
Bardziej bezpieczne niż podkarpacie	373	56,4%
Ogółem	661	100%
* 17 osób nie udzieliło odpowiedzi		

Źródło: badania własne.

Tabela 7 prezentuje opinie uczestników badania na temat bezpieczeństwa w województwach sąsiadujących z Podkarpaciem. Większość ankietowanych, bo przeszło połowa – 56,4%, uważa, że województwa sąsiadujące z Podkarpaciem są „bardziej bezpieczne niż Podkarpacie". Natomiast, 40,5% respondentów uważa, że sąsiadujące województwa są „tak samo bezpieczne/niebezpieczne jak Podkarpacie". Jedynie niewielki odsetek, 3,1% respondentów, uważa, że są one „mniej bezpieczne niż Podkarpacie". Na podstawie tych

danych można stwierdzić, że większość respondentów uważa, że województwa sąsiadujące z Podkarpaciem są bardziej bezpieczne niż Podkarpacie.

Respondentów zapytano również o to, czy podjęli jakiekolwiek kroki mające na celu zwiększenie bezpieczeństwa swojego lub swojej rodziny w związku z konfliktem zbrojnym w Ukrainie, takie jak przygotowanie zapasów czy plan ewakuacji (tabela 8).

Tabela 8. Rozkład odpowiedzi na pytanie: „Czy podjąłeś/aś jakiekolwiek kroki mające na celu zwiększenie bezpieczeństwa swojego lub swojej rodziny w związku z konfliktem zbrojnym w Ukrainie? (np. przygotowanie zapasów, plan ewakuacji)"

	Częstość	Procent
Tak	263	38,8%
Nie	415	61,2%
Ogółem	678	100%

Źródło: badania własne.

Zdecydowana większość respondentów, bo aż 61,2%, nie podjęło takich kroków. Natomiast, 38,8% respondentów odpowiedziało, że tak, podjęli działania mające na celu zwiększenie bezpieczeństwa swojego lub swojej rodziny. Na podstawie tych danych można stwierdzić, że większość respondentów nie podjęła konkretnych działań mających na celu zwiększenie bezpieczeństwa w związku z konfliktem zbrojnym w Ukrainie. Badani poproszeni zostali również o ocenę poziomu zagrożenia dla województwa podkarpackiego w kontekście inwazji Rosji na Ukrainę.

Tabela 9. Rozkład odpowiedzi na pytanie: „Jak oceniasz poziom zagrożenia dla województwa podkarpackiego w kontekście inwazji Rosji na Ukrainę?"

	Częstość	Procent
Brak zagrożenia	18	2,7%
Niskie zagrożenie	34	5,1%
Średnie zagrożenie	178	26,6%
Wysokie zagrożenie	384	57,5%
Bardzo wysokie zagrożenie	54	8,1%
Ogółem	668	100%
* 10 osób nie udzieliło odpowiedzi		

Źródło: badania własne.

Analizując poziom zagrożenia dla województwa podkarpackiego w kontekście inwazji Rosji na Ukrainę (tabela 9), większość ankietowanych – 57,5%, zauważyło, że województwo podkarpackie jest „wysoko zagrożone", a 8,1% respondentów uważa, że jest „bardzo wysoko zagrożone". Natomiast, 26,6% respondentów określiło zagrożenie jako „średnie", a 5,1% jako „niskie". Tylko niewielki odsetek respondentów (2,7%), uznał, że zagrożenie dla województwa podkarpackiego nie występuje („brak zagrożenia"). Na podstawie tych danych można stwierdzić, że większość respondentów uważa, że województwo podkarpackie jest wysoko lub bardzo wysoko zagrożone w kontekście inwazji Rosji na Ukrainę.

Kolejne pytanie dotyczyło bezpośredniego wpływu konfliktu zbrojnego w Ukrainie na ich własne bezpieczeństwo i bezpieczeństwo ich bliskich.

Tabela 10. Rozkład odpowiedzi na pytanie: „Czy konflikt zbrojny w Ukrainie może mieć bezpośredni wypływ na bezpieczeństwo Twoje i Twoich bliskich?"

	Częstość	**Procent**
Zdecydowanie nie	26	3,9%
Raczej nie	68	10,2%
Trudno powiedzieć	99	14,8%
Raczej tak	294	43,9%
Zdecydowanie tak	182	27,2%
Ogółem	669	100%
* 9 osób nie udzieliło odpowiedzi		

Źródło: badania własne.

Tabela 10 zawiera opinie respondentów na temat bezpośredniego wpływu konfliktu zbrojnego w Ukrainie na ich własne bezpieczeństwo i bezpieczeństwo ich bliskich. Najwyższy odsetek badanych (43,9%) wskazał, że konflikt może mieć bezpośredni wpływ na ich bezpieczeństwo („raczej tak"), 27,2% respondentów stwierdziło, że konflikt zdecydowanie może mieć bezpośredni wpływ na ich bezpieczeństwo („zdecydowanie tak"), 10,2% respondentów odpowiedziało, że konflikt „raczej nie" będzie miał bezpośredniego wpływu na ich bezpieczeństwo, a 3,9% wybrało odpowiedź „zdecydowanie nie". Natomiast 14,8% respondentów odpowiedziało, że „trudno powiedzieć". Analiza danych wskazuje zatem, że większość badanych obawia się tego, że konflikt zbrojny w Ukrainie może mieć bezpośredni wpływ na ich własne bezpieczeństwo i bezpieczeństwo ich bliskich.

Warto w tym miejscu wspomnieć jeszcze o jednym pytaniu, a mianowicie „Czy i w jaki sposób konflikt w Ukrainie wpłynął na Twoje plany związane z miejscem zamieszkania?" Tabela 11 zawiera odpowiedzi respondentów na pytanie o to, czy i w jaki sposób konflikt w Ukrainie wpłynął na ich plany związane z miejscem zamieszkania. Większość ankietowanych (56,3%), planuje pozostać w swoim miejscu zamieszkania, 25,9% respondentów odpowiedziało, że nie zastanawiało się nad zmianą miejsca zamieszkania w związku z konfliktem w Ukrainie. Wśród badanych znalazły się jednak takie osoby, które planują wyemigrować do innego województwa (9,7%) lub nawet do innego kraju (8,1%) z powodu konfliktu w Ukrainie. Na podstawie tych danych można stwierdzić, że większość respondentów nie planuje zmieniać swojego miejsca zamieszkania z powodu konfliktu w Ukrainie.

Tabela 11. Rozkład odpowiedzi na pytanie: „Czy i w jaki sposób konflikt w Ukrainie wpłynął na Twoje plany związane z miejscem zamieszkania?"

	Częstość	**Procent**
Planuję pozostać w swoim miejscu zamieszkania	372	56,3%
Planuję wyemigrować do innego województwa	64	9,7%
Planuję wyemigrować do innego kraju	54	8,1%
Nie zastanawiałem/am się nad tym	171	25,9%
Ogółem	661	100%

* 17 osób nie udzieliło odpowiedzi

Źródło: badania własne.

Analizując te niektóre, przytoczone na potrzeby niniejszego opracowania wyniki badań własnych, warto je również zestawić z innymi badaniami, przeprowadzonymi kilka lat wcześniej a odnoszącymi się do kryzysu powodzi z 2010 roku, jakiego doświadczyli mieszkańcy województwa podkarpackiego oraz powodzi błyskawicznej z 2020 r[20]. Sytuacja obserwowana na terenie województwa podkarpackiego w związku z wydarzeniami w Ukrainie może być również rozpatrywana z perspektywy problematyki zarządzania kryzysowego. Analizując odpowiedzi respondentów na pytanie o czynione przygotowania mające na celu zwiększenie bezpieczeństwa swojego lub swojej rodziny w związku z konfliktem zbrojnym w Ukrainie, aż 61,2% badanych nie podjęło takich kroków, natomiast zaledwie 38,8% respondentów to uczyniło.

[20] M. Waksmundzka-Szarek, *Problemy komunikacji społecznej w zarządzaniu kryzysowym w województwie*, Wydawnictwo Uniwersytet Rzeszowskiego Rzeszów 2024.

W sytuacji, kiedy większość badanych jednak wskazuje na stan zagrożenia, jednocześnie nie czyni przygotowań, które mają na celu zwiększenie swoich szans w razie wystąpienia realnego zagrożenia.

Pomimo prowadzonej od lat narracji o potrzebie zmiany i profesjonalizacji również w powszechnym – społecznym wymiarze zagadnień dotyczących ochrony i obrony przed zagrożeniami, które powodują rozmaite współczesne wydarzenia, można przypuszczać, że społeczeństwo nadal całość tej odpowiedzialności przenosi na państwo i nie zamierza w tym uczestniczyć oczekując zapewnienia stabilizacji i bezpieczeństwa ze strony administracji i systemu państwowego. Wspomniane wyżej badania ankietowe przeprowadzone kilka lat wcześniej[21] pokazały, że wszyscy respondenci co do zasady rozumieli potrzebę skutecznego zarządzania kryzysowego, natomiast badania szczegółowe wskazały, że swojej roli nie do końca była świadoma sama administracja, która w systemie reagowania i zarządzania kryzysem odgrywa kluczową rolę. W kontekście tych badań istotne znaczenie miały dwa punkty odniesienia: pierwszy – administracyjny, czyli sektor publiczny i drugi – społeczny, ponieważ te dwa wyraźnie „odrębne światy" nie zawsze wskazują na potrzebę wspólnego działania w kryzysie, często wzajemnie utrudniają swoje działania, nie rozumiejąc swoich oczekiwań i obowiązków. Wobec zagrożeń występujących współcześnie należałoby dążyć do wzmocnienia obszaru zarządzania kryzysowego poprzez integrację wszelkich procesów i działań zespołowych, gdzie każdy czuje się odpowiedzialny – zarówno administracja, jak też społeczeństwo. Działania zintegrowane prowadzone świadomie w przyszłości mogłyby spowodować zbudowanie nowej jakości w społeczeństwie, które właściwie rozpoznaje zagrożenia, adekwatnie na nie reaguje oraz skutecznie współuczestniczy w ich zwalczaniu.

Podsumowanie

W rozdziale opisano kilka wybranych wyników badań wstępnych nad tym jak mieszkańcy województwa podkarpackiego postrzegają bezpieczeństwo w regionie, w którym żyją, ze względu na bliskość granicy z Ukrainą i rolą województwa w procesie przyjmowania uchodźców oraz różnych form pomocy świadczonej Ukrainie przez społeczność międzynarodową. Analiza

[21] Ibidem, s. 236.

tych wybranych wyników wskazuje, że nie wszyscy odczuwają swoje bezpieczeństwo jako wystarczające. Zauważają czynniki wpływające na obniżenie poczucia bezpieczeństwa, jednakże nie popadają w nadmierną panikę, która była istotnie zauważalna, zwłaszcza w marcu 2022 r., zaraz po wybuchu drugiego etapu wojny w Ukrainie. Obserwowaliśmy wówczas w Polsce długie kolejki przed urzędami wojewódzkimi w celu zrealizowania usługi polegającej na wyrobieniu paszportu. I tak, dla przykładu w samym tylko województwie podkarpackim odnotowano wówczas niemalże czterokrotny wzrost złożonych wniosków paszportowych w stosunku do marca roku poprzedniego. Zrealizowane badania w pewnym sensie ilustrują fragment nastrojów społecznych w tym czasie, a ponieważ przeprowadzone zostały w okresie od 10 marca do 6 maja 2024 r., powinny uwzględniać zarówno elementy reakcji, których podstawą mogły być działania naznaczone strachem i paniką, jak również czas względnej stabilizacji – oswojenia się z sytuacją zewnętrzną. Człowiek będący podmiotem bezpieczeństwa, jak przedstawił to w słynnej piramidzie potrzeb A. Maslow[22], zdolny jest do prawidłowego funkcjonowania oraz rozwoju społecznego wyłącznie, kiedy jego potrzeba bezpieczeństwa zostanie zaspokojona.

Literatura

1. *Bezpieczeństwo międzynarodowe po zimnej wojnie*, red. R. Zięba, Wyd. Akademickie i Profesjonalne, Warszawa 2008.
2. Chojnowski L., *Bezpieczeństwo. Zarys teorii*, Uniwersytet Pomorski w Słupsku, Słupsk 2015.
3. Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, Siedlce 2010.
4. Kołodziejczyk A., *Bezpieczeństwo jako fenomen społeczny. Pojęcie bezpieczeństwa, jego interpretacje i odmiany,* Saeculum Christianum, vol. 4, nr 1, 2007.
5. Koziej S., *Podstawy bezpieczeństwa międzynarodowego i narodowego*, Myśl wojskowa, nr 4, 2005.
6. Kukułka J., *Nowe uwarunkowania i wymiary bezpieczeństwa międzynarodowego Polski*, Wieś i Państwo, 1995, nr 1, s. 198-199. Cytat za: L. Chojnowski, Bezpieczeństwo. Zarys teorii, Wyd. Akademia Pomorska w Słupsku, Słupsk 2012.
7. Maslow A. H., *A Theory of Human Motivation,* Psychological Review 1943, t. 50, za: R. W. Griffin, *Podstawy zarządzania organizacjami*, tłum. M. Rusiński, Warszawa 1999.

[22] A. H. Maslow, *A Theory of Human Motivation,* Psychological Review, 1943, t. 50, s. 370-396, za: R. W. Griffin, *Podstawy zarządzania organizacjami*, Wydawnictwo Naukowe PWN, Warszawa 1999.

8. Najder-Stefaniak K., *O bezpieczeństwie człowieka. Refleksja inspirowana filozofią Alberta Schweitzera*, [w:] *Wspólnotowość i postawa uniwersalistyczna*, 2010-2011, red. A. Górski, nr 7, Wyd. Polskie Towarzystwo Uniwersalizmu, Warszawa 2010.
9. Operational Data Portal UNHCR, *Ukraine Refuge Situation (since 24 February 2022)*, www.data.unhcr.org/en/situations/ukraine.
10. Piworwarski J., *Trzy filary kultury bezpieczeństwa*, [w:] *Kultura Bezpieczeństwa Nauka – Praktyka – Refleksje,* Nr 30, Kraków 2018.
11. Stawicki R., Szweda E., *Bezpieczny człowiek w niepewnym świecie w trzeciej dekadzie XXI wieku*, Wydawnictwo Difin, Warszawa 2023.
12. Szulc Bogdan M., *Bezpieczeństwo a nauki o bezpieczeństwie,* Toruń 2024.
13. United Nations Development Program, *Human Development Report 1994*, New York 1994.
14. Waksmundzka-Szarek M., *Problemy komunikacji społecznej w zarządzaniu kryzysowym w województwie*, Rzeszów 2024.
15. Zieliński K. R., *Bezpieczeństwo indywidualne*, *Pedagogika Społeczna*, nr 3(85), Warszawa 2022.
16. Zięba R., *Instytucjonalizacje bezpieczeństwa europejskiego*, Wydawnictwo Naukowe Scholar, Warszawa 1999.
17. Znaniecki F., *Poznań w świadomości jego obywateli. Z badań Polskiego Instytutu Socjologicznego nad miastem Poznaniem*, Poznań 1931.

dr Marcin Oskierko
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0003-3450-6037

dr Sławomir Żurawski
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

dr Julia Kobets
Przykarpacki Uniwersytet Narodowy im. Wasyla Stefanyka
w Iwano-Frankiwsku
ORCID: 0000-0001-9492-6119

mgr Wiktoria Marcinek
ORCID: 0009-0009-0959-6182

https://doi.org/10.29316/9788368103205_14

METODY DZIAŁANIA I ŹRÓDŁA FINANSOWANIA WSPÓŁCZESNYCH ORGANIZACJI TERRORYSTYCZNYCH

METHODS OF OPERATION AND SOURCES OF FINANCING OF CONTEMPORARY TERRORIST ORGANIZATIONS

Streszczenie

Celem niniejszego rozdziału jest analiza metod działania współczesnych grup terrorystycznych oraz źródeł ich finansowania w kontekście rosnącego zagrożenia dla bezpieczeństwa państwowego i międzynarodowego. Problem badawczy ujęto w pytaniu: W jaki sposób współczesne organizacje

Summary

The aim of this chapter is to analyze the methods of operation of contemporary terrorist groups and the sources of their financing in the context of the growing threat to state and international security. The research problem is addressed in the question: How do contemporary terrorist organizations diversify

terrorystyczne różnicują swoje metody działania i pozyskiwania środków finansowych oraz jak wpływa to na skuteczność systemów przeciwdziałania terroryzmowi? Postawiono hipotezę, że im bardziej zróżnicowane i trudne do wykrycia są metody działania oraz finansowania organizacji terrorystycznych, tym większe wyzwania napotykają systemy bezpieczeństwa w zakresie przeciwdziałania terroryzmowi. W pracy wykorzystano metody teoretyczne, w tym analizę dokumentów źródłowych, przegląd literatury naukowej, analizę przypadków oraz studia porównawcze dotyczące działań terrorystycznych i mechanizmów ich finansowania. Główny wniosek wskazuje, że skuteczne przeciwdziałanie terroryzmowi wymaga zintegrowanego podejścia obejmującego działania legislacyjne, technologiczne i międzynarodową współpracę instytucjonalną, ze szczególnym uwzględnieniem nowych zagrożeń, takich jak cyberterroryzm czy finansowanie z użyciem kryptowalut.

Słowa kluczowe: terroryzm, finansowanie terroryzmu, cyberterroryzm, bezpieczeństwo narodowe, metody działań terrorystycznych

their methods of operation and obtaining funds, and how does it affect the effectiveness of counter-terrorism systems? It has been hypothesized that the more diverse and difficult to detect the methods of operation and financing of terrorist organizations, the greater the challenges faced by security systems in the field of counterterrorism. The paper uses theoretical methods, including the analysis of source documents, a review of scientific literature, case studies and comparative studies on terrorist activities and the mechanisms of their financing. The main conclusion is that effective counter-terrorism requires an integrated approach involving legislative, technological, and international institutional cooperation, with a particular focus on emerging threats such as cyberterrorism and cryptocurrency financing.

Keywords: terrorism, financing terrorism, cyberterrorism, national security, methods of terrorist activities

Wstęp

Terroryzm od dekad stanowi jedno z najpoważniejszych zagrożeń dla bezpieczeństwa międzynarodowego, narodowego i lokalnego. Jego ewolucja, zarówno w zakresie ideologii, jak i środków działania, sprawia, że współczesne państwa muszą nieustannie dostosowywać strategie przeciwdziałania oraz metody identyfikacji potencjalnych zagrożeń. W XXI wieku działalność grup terrorystycznych przybiera coraz bardziej zróżnicowane formy, obejmując zarówno klasyczne zamachy bombowe i porwania, jak i cyberataki, wykorzystanie broni biologicznej oraz działania prowadzone przez tzw. „samotne wilki". Kluczowym elementem skuteczności tych organizacji pozostaje jednak dostęp do źródeł finansowania – legalnych i nielegalnych – które umożliwiają realizację zamierzeń ideologicznych oraz prowadzenie działań operacyjnych.

Niniejszy rozdział ma na celu przybliżenie metod działania współczesnych grup terrorystycznych, z uwzględnieniem ich taktyki, środków przemocy oraz mechanizmów finansowania. Ukazuje także skalę zagrożeń wynikających z postępu technologicznego, jak również podejmowane środki przeciwdziałania, zarówno na poziomie krajowym, jak i międzynarodowym.

Metody i działania grup terrorystycznych

Zorganizowane grupy terrorystyczne nie tylko dokonują zamachów terrorystycznych, ale także prowadzą kampanie terrorystyczne. Zamachy mają charakter incydentalny, natomiast kampanie to umyślna i zamierzona seria ataków, które przeprowadzane są na dużą skalę w krótkim okresie. Grupy terrorystyczne działają w oparciu o metody działania, czyli charakterystyczne sposoby, za pomocą których dokonują zamachów[1].

Zamachy terrorystyczne, przeprowadzone w formie pojedynczego ataku czy też całej serii, różnią się przede wszystkim w zależności od zastosowanych środków przemocy. Wyodrębnia się:

- ataki bombowe,
- zamachy z wykorzystaniem broni palnej,
- zamachy z użyciem broni masowego rażenia – ładunku promieniotwórczego, środków chemicznych,
- ataki związane z cyberprzestrzenią – z wykorzystaniem sieci internetowej,
- ataki dokonane za pomocą wybranego środka transportu – powietrznego, lądowego lub nawodnego[2].

Działania terrorystyczne prowadzone przez zorganizowane grupy mogą być podejmowane nie tylko bezpośrednio wobec ludzi, ale również wobec infrastruktury. Szczególnie ataki skierowane w obiekty i systemy infrastruktury krytycznej powodują chaos i znaczną dezorganizację, co w konsekwencji prowadzi do zakłócenia minimalnego funkcjonowania państwa oraz jego gospodarki. Akty terrorystyczne wymierzone w obiekty infrastrukturalne przebiegają

[1] B. Bolechów, *Terroryzm w świecie podwubiegunowym,* Wydawnictwo Adam Marszałek, Toruń 2003, s. 39.

[2] P. Lubiewski, *Reguły i metody działania współczesnych organizacji terrorystycznych*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, Nr 29(4), 2018, s. 113-114.

zazwyczaj według podobnego schematu, zawierającego kolejno następujące po sobie fazy, takie jak:

- podejście do obiektu, który stanowi cel ataku,
- wejście na teren obiektu,
- dokonanie zniszczeń bądź uszkodzeń obiektu z możliwością uprowadzenia wybranej, zawartej w planie osoby,
- oddalenie się z miejsca ataku lub też dokonanie zamachu samobójczego[3].

Faktem jest, że organizacje terrorystyczne kierują swoje działania często bezpośrednio w ludzi, narażając ich zdrowie i pozbawiając życia w imię wyznawanej ideologii. Wykonawcy ataków terrorystycznych przyjmują w tym celu różną taktykę. Mogą zorganizować zasadzkę lub sieć zasadzek, przeprowadzić napad lub dokonać rabunku. Ich celem nierzadko są uprowadzenia, zabójstwa czy też przetrzymywanie zakładników, dzięki którym zamierzają wymusić określone zachowania[4].

Warto wspomnieć, że grupy terrorystyczne wykorzystują w swoich działaniach elementy psychologiczne, dzięki którym wywierają znaczący wpływ na stan psychiki przeciwnika oraz jego morale. Ponadto, działania te powodują wzrost poczucia przygnębienia oraz rezygnacji, a także wzmagają niepewność i osłabiają wolę walki wśród społeczeństwa będącego celem ataku. Terroryści do zrealizowania zamierzonych zadań wykorzystują techniki polegające na:

- szerzeniu propagandy poprzez rozpowszechnianie informacji, które kwestionują autorytet władz państwowych,
- przecenianiu znaczenia efektów realizacji swoich zadań, wzbudzaniu paniki, chaosu i niepewności, na przykład poprzez przekazywanie nieprawdziwych informacji za pomocą środków masowego przekazu[5].

Poza aspektem psychologicznym, strategie terrorystów, zawierają również inne elementy. Uogólniając, większość organizacji terrorystycznych, funkcjonuje w oparciu o takie zasady jak:

- nieprzestrzeganie ustanowionego prawa międzynarodowego w zakresie konfliktów zbrojnych,
- kierowanie ataków zazwyczaj w osoby niewinne i nieuzbrojone,

[3] Ibidem, s. 114.
[4] Ibidem.
[5] Ibidem.

- dokonywanie zamachów na terenach miejskich, wysoce zurbanizowanych, z uwagi na gęstość zaludnienia oraz obecność atrakcyjnych celów, na przykład ważnych kulturowo lub strategicznie budynków,
- odrzucenie wszelkich norm moralnych,
- działanie w celu zadania możliwie największych strat wśród ofiar i zyskania rozgłosu,
- wybieranie odpowiednich środków przemocy, które pokażą bezwzględność organizacji,
- planowanie tak zwanych sieci konspiracyjnych, na przykład ukrytych magazynów środków pieniężnych czy broni, lokali zajmowanych przez członków organizacji i wykonawców zamachu,
- stosowanie przemocy i siły w sposób jak najbardziej efektowny i spektakularny, z zamiarem zwrócenia uwagi społeczeństwa i osiągnięcia zamierzonych celów[6].

Jeden z punktów strategii dotyczy nieprzestrzegania przez terrorystów prawa międzynarodowego. Przejawia się to między innymi w świadomym dokonywaniu zamachów na osoby cywilne, chronione prawem międzynarodowym, w tym na dyplomatów, braniu zakładników i pozbawianiu ich życia. W ramach przyjętej przez poszczególne organizacje strategii, jej członkowie wykorzystują różne metody przeprowadzania zamachów. Jedną z najpopularniejszych technik stosowanych przez terrorystów w XXI wieku stanowią zamachy samobójcze. Osoby dokonujące takiego zamachu zazwyczaj ukrywają materiały wybuchowe pod ubraniem – jako tak zwany *pas szahida* lub w bagażach podręcznych, na przykład w plecakach czy torbach. Odnotowano również przypadki, kiedy ładunki wybuchowe w dużej ilości ukryte były w pojazdach, którymi poruszali się zamachowcy. Ataki te są szczególnie niebezpieczne, ponieważ powodują śmierć bardzo dużej ilości osób. Z tego względu są uważane przez terrorystów za efektowne i spektakularne, dlatego też ich powtarzalność jest coraz częstsza[7].

Z początkiem XXI wieku, między innymi islamscy fundamentaliści powrócili do znanej od tysięcy lat metody pozbawiania życia poprzez dekapitację, czyli uśmiercanie ofiary przez ścięcie głowy. Niegdyś była ona stosowana

[6] G. Nowacki, *Zagrożenia terrorystyczne na świecie*, Nierówności Społeczne a Wzrost Gospodarczy, Nr 44(4), 2015, s. 416-17.

[7] K. Karolczak, *Terroryzm XXI wieku – wybrane aspekty*, Terroryzm – Studia, Analizy, Prewencja 2022, Nr 1(1), s. 12.

nie tylko jako kara za faktycznie dokonane przestępstwa lub zbrodnie wyimaginowane, ale również jako forma ostrzeżenia dla osób planujących przeciwstawienie się ówcześnie panującej władzy. Terroryści wykorzystują tą metodę także jako ultimatum w sprawie uwolnienia więzionych terrorystów w zamian za darowanie życia przetrzymywanej przez nich ofiary[8].

Za przykład wyżej wymienionej techniki stosowanej przez terrorystów może posłużyć historia Daniela Pearl'a, amerykańskiego dziennikarza, pracującego dla Wall Street Journal. Mężczyzna został uprowadzony z własnego samochodu 23 stycznia 2002 r. w Pakistanie. Zabójstwa dziennikarza dokonano 1 lutego tego samego roku. Porywacze zamieścili w Internecie film, który ukazuje ostatnie minuty jego życia oraz drastyczną scenę przedstawiającą dekapitację. Ciało mężczyzny zostało odnalezione i zidentyfikowane kilka miesięcy później – 16 maja 2002 r. Mimo że do porwania i pozbawienia życia dziennikarza przyznała się organizacja National Movement for the Restoration of Pakistani Sovereignty, to pakistański rząd skierował oskarżenia ku członkom Al-Kaidy, których później aresztowano[9].

Warto pamiętać, że podobny los spotkał polskiego geologa, pracownika Geofizyki Kraków, Piotra Stańczaka. Tymczasowo przebywał on w Pakistanie w związku z kontraktem realizowanym przez krakowską firmę dla pakistańskiego przedsiębiorstwa Oil & Gas Development Company Limited. W momencie porwania, we wrześniu 2008 r., mężczyzna podróżował samochodem w rejonie Pind Sultani, miejscowości oddalonej około 100 km od stolicy Pakistanu. Jego porywaczami okazali się Talibowie, którzy żądali między innymi zwolnienia z pakistańskich więzień 110 talibów. W zamian za to, Piotr Stańczak, miał odzyskać wolność. Pakistański Rząd nie spełnił ultimatum, w związku z czym w lutym 2009 r. Talibowie powiadomili o zabójstwie Polaka poprzez dekapitację. Jego ciało z początkiem maja 2009 r., zgodnie z wolą rodziny, spoczęło na cmentarzu w Krośnie[10].

Wykorzystanie dekapitacji jako środka służącego do zastraszania przeciwnika i zmuszania go do wypełniania żądań stawianych przez ugrupowania

[8] Ibidem, s. 13.

[9] Ibidem.

[10] *Prezydent odznaczył zabitego przez talibów geologa*, 04 października 2010 r., https://www.prezydent.pl/kancelaria/archiwum/archiwum-bronislawa-komorowskiego/aktualnosci/ordery-i-odznaczenia/prezydent-odznaczyl-zabitego-przez-talibow-geologa,18399, [dostęp: 25.04.2025].

terrorystyczne nie dotyczy tylko pojedynczych jednostek. Przed dekadą, do globalnej opinii publicznej dotarły informacje o egzekucjach przeprowadzonych w taki sposób w okresie między 25 lipca 2014 r. a 10 sierpnia 2015 r. Ofiarami byli między innymi:

- żołnierze kurdyjscy oraz syryjscy,
- chrześcijańscy uchodźcy pochodzący z Etiopii,
- pracownicy organizacji humanitarnych,
- dziennikarze z różnych części świata[11].

Ogółem, w tym czasie, w 24 egzekucjach dokonanych przez Państwo Islamskie, śmierć poniosło co najmniej 300 osób. Jedną z kategorii terrorystów stanowią *samotne wilki,* czyli zamachowcy, którzy:

- nie są członkami żadnej organizacji,
- nie dążą do realizacji konkretnego, ogólnoświatowego planu,
- nie są zobligowani do wypełniania rozkazów dowódcy,
- planują i przeprowadzają zamachy samodzielnie[12].

Ofiarami *samotnych wilków* są najczęściej osoby przypadkowe i nieznane sprawcom. Należy jednak pamiętać, że nie każdy pojedynczy atak, przeprowadzony przez zamachowca w sposób samodzielny, jest atakiem o charakterze terrorystycznym. Warunkiem uznania go za czyn terrorystyczny jest fakt działania sprawcy w myśl określonej idei, kiedy przyczyną ataku jest na przykład motyw polityczny lub radykalny światopogląd.

Przykładem ataku terrorystycznego, dokonanego przez „samotnego wilka" jest zamach z 22 lipca 2011 r. Norweg Anders Breivik, najpierw w dniu zamachu opublikował w sieci internetowej swojego autorstwa manifest, noszący tytuł 2083 – Europejska Deklaracja Niepodległości. Stanowił on zbiór tekstów o charakterze ksenofobicznym, islamofobicznym, rasistowskim i antyfeministycznym. Następnie przeprowadził zamach bombowy na siedzibę norweskiego premiera w Oslo, w której śmierć poniosło 8 osób. Tego samego dnia, przemieścił się na wyspę Utøya, gdzie trwał obóz młodzieżowej sekcji norweskiej Partii Pracy. Anders Breivik za pomocą broni palnej dokonał masowej strzelaniny, w wyniku której zginęło 69 osób. Sprawcę uznano za poczytalnego w momencie dokonywania czynu. Zastosowano wobec niego najwyższy możliwy wymiar kary, skazując go na 21 lat pozbawienia wolności, z zachowaniem

[11] K. Karolczak, *Terroryzm XXI wieku – wybrane aspekty*, op. cit., s. 14.

[12] Ibidem.

możliwości nieograniczonego jej przedłużenia. Zamachowiec, wyznający poglądy skrajnie prawicowe, w trakcie procesu przyznał, że do ataku skłoniły go pobudki polityczne. Ponadto, wykonywał również charakterystyczne gesty faszystowskiego pozdrowienia. Zachowania oraz motyw sprawcy pozwalają uznać, że czyn, jakiego się dopuścił, miał charakter terrorystyczny[13].

Charakterystyczne metody stosują organizacje, działające w ramach bioterroryzmu. Stosowana przez nich broń biologiczna jest niezwykle niebezpieczna. Do przeprowadzenia ataków z jej użyciem wykorzystuje się patogenne mikroorganizmy, takie jak laseczki wąglika, wirusy albo toksyny pochodzenia biologicznego, na przykład rycynę czy botulinę. Produkcja broni biologicznej pochłania stosunkowo niskie koszty, a materiały wykorzystywane w procesie wytworzenia są łatwo dostępne, ponieważ niektóre z nich można pozyskać nawet z surowców naturalnych[14].

Broń biologiczna jest nie tylko wysoce skuteczna, ale także trudna do wykrycia. Wpływa na to między innymi szybkość rozprzestrzeniania się patogenu zakaźnego oraz szerokie możliwości jego transportu. Ponadto, nawet niewielka dawka środka biologicznego jest w stanie wywołać infekcje i choroby o ciężkim przebiegu, często odporne na podejmowane przez medyków leczenie. Ataki z wykorzystaniem broni biologicznej ukierunkowane są na wywołanie epidemii, nierzadko bardzo śmiercionośnej, która w konsekwencji doprowadzi do strat społecznych i gospodarczych, poczucia niepokoju w społeczeństwie, dezorganizacji władzy, a nawet destabilizacji sfery finansowej państwa[15].
Sprawcy zamachów, noszących znamiona bioterroryzmu, wybierają różne metody działania. Ataki mogą być przeprowadzone między innymi poprzez:

- skażenie powietrza,
- skażenie ujęć wody lub artykułów żywnościowych,
- ukrycie i przekazanie środków biologicznych w przesyłkach pocztowych[16].

Ponadto, dzięki rozwojowi inżynierii genetycznej i biotechnologii, bioterroryści zyskują nowe możliwości dostępu do broni biologicznej, co w przyszłości

[13] Ibidem, s. 15-16.
[14] P. Nowak, *Bioterroryzm i chemoterroryzm jako formy współczesnego terroryzmu. Zapobieganie atakom w Rzeczypospolitej Polskiej,* Kultura Bezpieczeństwa 2019, Nr 36, s. 48-49.
[15] Ibidem, s. 48-50.
[16] Ibidem, s. 50.

może spowodować, że staną się samowystarczalni w zakresie produkcji tego rodzaju broni. Zagrożenie wykorzystania badań, odkryć i eksperymentów naukowych z zakresu medycyny w sposób niewłaściwy, przez osoby do tego nieuprawnione, może spowodować, że potencjalne ataki z użyciem środków biologicznych osiągną w przyszłości zasięg globalny[17].

Cyberprzestrzeń postrzegana jest jako olbrzymia cyfrowa biblioteka[18], z której mogą korzystać wszyscy użytkownicy, również terroryści. Terroryści w ten sposób mają dostęp do ogromnej ilości informacji, których uzyskanie było wcześniej niezwykle utrudnione, choćby ze względu na ich rozproszenie geograficzne, jak i różnorodność form występowania[19]. Zwiększająca się dynamicznie liczba stron internetowych zapewnia dostęp do wiedzy, która może być wykorzystana zarówno w legalnych, jak i bezprawnych zamiarach również w aktach bezprawnej ingerencji[20]. W literaturze możemy odnaleźć dwa główne obszary wykorzystania Internetu jako źródła pozyskiwania przez terrorystów informacji[21]. Pierwszym obszarem są wszelkie legalnie dostępne w Internecie dane, które mogą posłużyć do rozpoznania potencjalnych obiektów ataku oraz pozwalają zapoznać się z ich otoczeniem, a także informacje, które mogą ułatwić planowanie i przygotowanie zamachu terrorystycznego. Źródła te mogą być różne[22]. Na przykład, na stronach internetowych często znajdują się szczegółowe mapy, zdjęcia oraz opisy infrastruktury krytycznej, takich jak lotniska, elektrownie, budynki rządowe czy obiekty wojskowe. Media społecznościowe umożliwiają monitorowanie działań osób, które mogą być celem ataków, oraz zdobycie informacji na temat rutynowych działań i zabezpieczeń stosowanych w różnych miejscach.

---

17 Ibidem.

18 M. Ranstorp, *The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation*, [w:] *International Relations and Security in the Digital Age*, J. Eriksson, G. Giacomello (red.), Routledge. London 2007, s. 40.

19 M. Conway, *Terrorist 'Use' of the Internet and Fighting Back*, Information & Security. An International Journal, vol.19, 2006, s. 16.

20 R. Hennig, *Cyberterroryzm miękki. Cz. 1, Internet jako źródło informacji i funduszy*, Przegląd Naukowo-Metodyczny, Edukacja dla bezpieczeństwa, Rok IX, nr 4 (29), 2015, s. 46.

21 D. Thelesklaf, M. Gercke, *Terrorist Use of the Internet and Legal Response.* F3 – Freedom From Fear Magazine, Issue 7, July 2010, s. 18.

22 B.W. Don et al., *Network Technologies for Networked Terrorists*, *Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, RAND Technical Report, 2007, s. 25.

Kolejnym źródłem są bazy danych i rejestry publiczne, które zawierają informacje o firmach, instytucjach oraz osobach prywatnych. Rejestry te mogą dostarczyć cennych informacji na temat struktury organizacyjnej, danych kontaktowych oraz lokalizacji potencjalnych celów. Dostęp do takich danych może być uzyskany legalnie, co utrudnia ich monitorowanie i kontrolę przez organy ścigania. Dodatkowo, informacje geolokalizacyjne dostępne poprzez usługi, takie jak Google Maps czy Bing Maps, pozwalają na dokładne zapoznanie się z topografią terenu oraz szczegółami dotyczącymi infrastruktury. Umożliwiają one terrorystom przygotowanie szczegółowych planów operacyjnych bez konieczności fizycznego rozpoznania terenu.

Warto również wspomnieć o publikacjach akademickich oraz raportach branżowych, które często zawierają szczegółowe analizy dotyczące zabezpieczeń oraz potencjalnych słabych punktów w różnych sektorach infrastruktury. Tego typu dokumenty, dostępne w bibliotekach i repozytoriach internetowych, mogą być wykorzystane do zdobycia specjalistycznej wiedzy niezbędnej do przeprowadzenia zamachu.

Wszystkie te źródła informacji są legalnie dostępne, co sprawia, że ich monitorowanie i kontrola są dużym wyzwaniem dla służb wywiadowczych i organów ścigania. Właśnie dlatego, w celu przeciwdziałania wykorzystywaniu tych danych przez terrorystów, konieczna jest współpraca międzynarodowa oraz wprowadzenie odpowiednich regulacji prawnych, które ograniczą dostęp do wrażliwych informacji oraz zwiększą świadomość społeczną na temat zagrożeń związanych z udostępnianiem danych w Internecie.

Organizacjami terrorystycznymi kierują różne motywy. Działają głównie w oparciu o przemoc w celu wywołania chaosu, niepokoju czy podważenia autorytetu władzy. Wykorzystywane przez terrorystów środki to najczęściej broń palna lub bomby, jednak rozwój technologiczny obserwowany w ciągu ostatnich lat powoduje pojawienie się nowych rozwiązań, za pomocą których zamachowcy mogą realizować stawiane im cele. Modyfikacje i ciągłe ulepszanie stosowanej broni wpływają na wzrost jej skuteczności. Stwarza to zagrożenie, że przyszłe potencjalne ataki terrorystyczne będą jeszcze tragiczniejsze w skutkach[23].

[23] J. Horgan, *Psychologia terroryzmu,* Wydawnictwo Naukowe PWN, Warszawa 2015, s. 28-29.

Źródła finansowania terroryzmu

Terroryzm jest złożonym zjawiskiem, którego istotnym elementem jest finansowanie. Bez odpowiednich środków finansowych organizacje terrorystyczne nie byłyby w stanie przeprowadzać operacji, rekrutować członków ani realizować swojej ideologii. Zrozumienie źródeł finansowania terroryzmu jest kluczowe dla skutecznego przeciwdziałania temu zagrożeniu.

Organizacje terrorystyczne finansują swoją działalność ze środków pochodzących z przestępstwa, jak również ze źródeł legalnych[24]. Do najważniejszych należą:

- przestępczość zorganizowana,
- przestępstwa finansowe,
- wsparcie państwowe,
- donacje i datki,
- własne działalności gospodarcze,
- zasoby naturalne[25].

W związku z koniecznością finansowania swojej działalności organizacje terrorystyczne w dużym stopniu współpracują z grupami przestępczymi zajmującymi się działalnością kryminalną[26].

Jednym z głównych źródeł finansowania jest przestępczość zorganizowana. Organizacje terrorystyczne często angażują się w handel narkotykami, przemyt broni, fałszerstwa oraz inne formy przestępczości, które dostarczają im znaczących środków finansowych[27]. Handel narkotykami, na przykład, jest szczególnie dochodowy, zwłaszcza w regionach takich jak Afganistan, gdzie produkcja opium stanowi istotne źródło dochodów dla grup terrorystycznych.

Przestępstwa finansowe również odgrywają istotną rolę w finansowaniu terroryzmu. Pranie pieniędzy, oszustwa podatkowe oraz cyberprzestępczość to popularne metody uzyskiwania funduszy. Organizacje terrorystyczne korzystają z zaawansowanych technik prania pieniędzy, aby legalizować swoje dochody i unikać wykrycia przez organy ścigania. Do zaistnienia przestępstwa

[24] K. Izak, M. Kluczyński, *Handel Narkotykami jako źródło finansowania terroryzmu*, Przegląd Bezpieczeństwa Wewnętrznego, nr 10, 2014, s. 38.

[25] T. Bąk, *Oblicza terroryzmu*, Wydawnictwo Konsorcjum Akademickie, Kraków-Rzeszów-Zamość 2011, s. 103-113.

[26] J. W. Wójcik, *Przeciwdziałanie finasowaniu terroryzmu*, Wolters Kluwer, Warszawa 2007, s. 82-83.

[27] K. Izak, M. Kluczyński, *Handel Narkotykami …*, op. cit., 39.

finansowania terroryzmu nie jest koniecznie występowanie przestępstwa bazowego. Ta różnica może być istotna dla systemów wykrywania obu przestępstw[28]. Jedną z kluczowych różnic między praniem pieniędzy a finansowaniem terroryzmu jest to, że w wypadku pierwszego chodzi o źródło funduszy, a drugiego o ich miejsce przeznaczenia[29].

W ostatnich latach rośnie także rola cyberprzestępczości, gdzie kradzież tożsamości, phishing oraz inne formy oszustw internetowych stają się coraz bardziej powszechne, co może się przerodzić w ataki terrorystyczne.

Cyberprzestępczość stała się popularną metodą uzyskiwania funduszy przez organizacje terrorystyczne, ze względu na anonimowość i globalny zasięg, które oferuje internet. Grupy terrorystyczne stosują różne techniki cyberprzestępcze, aby zdobyć środki finansowe na swoją działalność. Poniżej w tabeli przedstawiono rzeczywiste przykłady i źródła wykorzystywania cyberprzestępczości do finansowania swoich operacji.

Tabela 1. Rzeczywiste przykłady i źródła wykorzystywania cyberprzestępczości do finansowania operacji terrorystycznych.

Rodzaj i forma przestępstwa	Przykład wykorzystania
Ransomware (oprogramowanie wymuszające okup)	Grupa Lazarus (podejrzewana o powiązania z Koreą Północną): Grupa ta jest znana z ataków ransomware, takich jak atak WannaCry w 2017 roku, który zainfekował komputery na całym świecie, żądając okupu w Bitcoinach[30].
Phishing i kradzież tożsamości	ISIS: Grupy powiązane z ISIS przeprowadzały kampanie phishingowe, aby kraść dane osobowe i finansowe, które następnie były wykorzystywane do wyłudzania pieniędzy lub przeprowadzania oszustw finansowych[31].

[28] Ł. Krupa, *Przeciwdziałanie finansowaniu terroryzmu*, Cybersecurity and Law, nr 7, 2022, s. 98.

[29] Przeciwdziałanie praniu pieniędzy: Podstawy, https://www.pibr.org.pl/static/items/publishing/AML_cz.8_Trendy%20w%20przest-opczoCcci.pdf>, [dostęp: 24.04.2025].

[30] *Globalny atak ransomware WannaCry może być powiązane z grupą cyberprzestępczą Lazarus – komentarz Kaspersky Lab*, https://itreseller.com.pl/globalny-atak-ransomware-wannacry-moze-byc-powiazane-z-grupa-cyberprzestepcza-lazarus-komentarz-kaspersky-lab/, [dostęp: 16.05.2025].

[31] *Cyberarmia kalifatu*, https://polska-zbrojna.pl/Mobile/ArticleShow/30080, [dostęp: 16.05.2025].

Rodzaj i forma przestępstwa	Przykład wykorzystania
Oszuści finansowi (fraud):	Al-Kaida: Członkowie Al-Kaidy angażowali się w różne oszustwa finansowe, takie jak kartowe oszustwa bankowe, które przynosiły organizacji znaczne zyski[32].
Krypto-waluty:	Hezbollah: Używa kryptowalut do unikania tradycyjnych systemów finansowych i sankcji, ułatwiając transfery pieniędzy między sympatykami i członkami organizacji[33].

Źródło: opracowanie własne.

Przestępcy celowo szukają giełd o niskich wymaganiach w zakresie AML w przekonaniu, że można je bez większych przeszkód wykorzystać do transakcji między pieniędzmi FATF, a kryptowalutami lub pomiędzy różnymi kryptowalutami[34]. Cechy takich giełd są następujące:

- celowe lekceważenie przepisów i wymogów rejestracyjnych;
- umożliwienie klientom zakładania rachunków przy jednoczesnym niewielkim lub żadnym wymogu przedstawienia informacji identyfikacyjnych;
- klienci otwierający rachunki nie muszą przestrzegać przepisów w żadnej jurysdykcji;
- siedziba giełdy w kraju wysokiego ryzyka, do których należą:
  - kraje z wysokim ogólnym ryzykiem prania pieniędzy i finansowania terroryzmu – zwykle w Afryce, Europie Wschodniej lub na Bliskim Wschodzie,
  - kraje podlegające międzynarodowym sankcjom, embargu i innym ograniczeniom,
  - kraje na liście jurysdykcji wysokiego ryzyka i braku współpracy FATF,
  - kraje bez regulacji AML/CTF obejmujących kryptowaluty lub z nieefektywnymi ramami regulacyjnymi.

[32] L. Lisiecki, K. Kucharski, *Źródła finasowania Al-Kaidy*, Studia bezpieczeństwa narodowego, vol. 4, nr 1, 2013, s. 298.

[33] N. Malik, *Jak przestępcy i terroryści używają kryptowaluty: i jak to powstrzymać*, Forbes 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/, [dostęp: 16.05.2025].

[34] J. Wróblewski, C. Martysz, *Kryptowaluty a finansowanie przestępczości i pranie pieniędzy*, Studia i Prace Kolegium Zarządzania i Finansów, nr 193, 2023, s. 215.

Waluty cyfrowe mogą pomóc zarówno przestępcom, jak i terrorystom kupującym towary i usługi w Darknecie, którzy w przeciwnym razie byliby narażeni na oszustwa ze strony rywalizujących organizacji przestępczych[35].

Wsparcie państwowe jest kolejnym istotnym źródłem finansowania. Niektóre państwa, kierując się własnymi celami politycznymi lub ideologicznymi, świadomie wspierają organizacje terrorystyczne, dostarczając im funduszy, broni oraz zapewniając schronienie i logistykę. Pomoc finansowa dla terrorystów zapewniana przez państwa jest naturalną przyczyną politycznych aspektów działalności wywrotowej. Organizacje terrorystyczne przy definiowaniu swoich postulatów jasno wskazują, przeciwko komu walczą i co jest ich celem, zyskując przy tym sympatię jednych oraz wrogość innych krajów[36]. Przykłady takich działań można znaleźć w historii współpracy Iranu z Hezbollachem czy innych podobnych przypadków. W corocznych raportach Departamentu Stanu USA są wymieniane państwa oskarżane o sponsorowanie terroryzmu, przy czym lista tych państw zmieniała się przez ponad 40 lat. Obecnie są na niej cztery kraje:

- Syria – od 29 grudnia 1979 r.,
- Iran – od 16 stycznia 1984 r.,
- Koreańska Republika Ludowo-Demokratyczna – od 20 listopada 2017 r.,
- Kuba – od 12 stycznia 2021 r.

Wcześniej na liście zamieszczono również Libię, Irak, Jemen Południowy i Sudan[37].

Donacje i datki od sympatyków również odgrywają znaczącą rolę. Organizacje terrorystyczne często korzystają z darowizn od osób prywatnych oraz funduszy zbieranych pod pretekstem działalności charytatywnej. Fundacje i organizacje charytatywne mogą służyć jako przykrywki do zbierania funduszy na działalność terrorystyczną, co utrudnia ich wykrywanie i neutralizację. Również publikacja informacji dotyczących swojej działalności służy prowadzonej propagandzie i może wzmacniać źródło dochodu, jakim są dotacje od osób zewnętrznych[38].

---

[35] N. Malik, *Jak przestępcy i terroryści używają kryptowaluty: i jak to powstrzymać*, Forbes 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/, [dostęp: 16.05.2025].

[36] L. Lisiecki, K. Kucharski, *Źródła finasowania*…, op. cit., s. 290.

[37] *State sponsors of terrorism*, U.S. Department of State, https://www.state.gov/state-spon-sors-of-terrorism/, [dostęp: 16.05.2025].

[38] K. Liedel, P. Piasecka, T. Aleksandrowicz, *Bezpieczeństwo w XXI Wieku. Asymetryczny świat*, Difin, Warszawa 2011, s. 69

Ponadto, organizacje terrorystyczne często prowadzą własne działalności gospodarcze. Mogą to być zarówno małe przedsiębiorstwa, jak i duże firmy działające na skalę międzynarodową.

Firmy, które wydają się całkowicie legalne – komisy samochodowe, firmy zajmujące się nieruchomościami, organizacje charytatywne, a nawet banki – czasami służą jako legalna twarz organizacji terrorystycznych i stanowią istotny składnik aparatu pieniężnego, centralny kanał prania ogromnych sum, które organizacje terrorystyczne zarabiają na działalności przestępczej[39]. Legalne przedsięwzięcia biznesowe generują dochody, które są następnie wykorzystywane do finansowania działań terrorystycznych.

Ten system sieci służący transferowaniu pieniędzy dla Hamasu zakłada istnienie pracowników sektora finansowego czy nawet całych banków, które pośredniczą w przekazywaniu pieniędzy terrorystom. Na przykład w 2020 roku Sąd okręgowy wschodniego okręgu USA w Nowym Jorku orzekł, że mający siedzibę w Stambule bank Kuveyt Türk Katilim Bankasi m.in. prowadził konta klientów powiązanych z Hamasem, wiedząc, że pomaga transferować pieniądze[40].

Tymi klientami w bankach najczęściej są organizacje non-profit, czy firmy i korporacje działające w państwach Bliskiego Wschodu, w których Hamas posiada ukryte aktywa. Najczęściej są to firmy z sektora nieruchomości z Turcji, Arabii Saudyjskiej, Algierii, a nawet Sudanu.

Jak już wspomniano organizacje terrorystyczne korzystają również z pieniędzy pochodzących z legalnych źródeł, w tym ze wsparcia finansowego prywatnych darczyńców i organizacji charytatywnych. Organizacje charytatywne mogą być wykorzystywane przez ugrupowania terrorystyczne na trzy sposoby:

- organizacja charytatywna prowadzi działalność statutową, ale część pozyskiwanych środków przekazuje terrorystom,
- organizacja charytatywna jest jedynie kamuflażem, całość zaś pozyskiwanych przez nią środków przekazywana jest na działania ugrupowań terrorystycznych,

[39] *Najbogatsze organizacje terrorystyczne na świecie*, https://forbes.co.il/rankings/2021terrororganizations/intro/, [dostęp: 16.05.2025].

[40] *Terroryści z milionami na koncie. Skąd Hamas ma pieniądze na wojnę?*, https://geekweek.interia.pl/militaria/news-terrorysci-z-milionami-na-koncie-skad-hamas-ma-pieniadze-na-,nId,7085873#google_vignette, [dostęp: 16.05.2025].

- organizacja prowadzi działalność charytatywną, jednak pomoc udzielana jest przez punkty kontrolowane przez członków ugrupowania terrorystycznego, dzięki czemu beneficjenci mają wrażenie, że otrzymują ją od ugrupowania terrorystycznego, co przynosi wymierne efekty propagandowe[41].

Kontrola nad surowcami naturalnymi stanowi dodatkowe źródło finansowania. Niektóre grupy terrorystyczne przejmują kontrolę nad złożami ropy naftowej, diamentów, drewna czy innych surowców, które następnie sprzedają na czarnym rynku, generując znaczne zyski. Przykładem może być działalność ISIS, która finansowała się z handlu ropą naftową z kontrolowanych przez siebie terenów.

Poniżej w tabeli przedstawiono klasyfikacje grup terrorystycznych z uwzględnieniem źródeł finansowania.

Tabela 2. Klasyfikacja grup terrorystycznych z uwzględnieniem źródeł finansowania

Typy grup lub scenariuszy (działań)	Źródła finansowania
Terroryzm wewnętrzny	
• antykolonialne (nacjonalistyczne); • mniejszości etniczne, religijne i kulturowe; • mniejszości ideologiczne, lewicowe; • mniejszości ideologiczne, prawicowe; • grupy sponsorowane przez rząd; • partyzantka miejska, tj. grupy wystarczająco; duże, by miały szansę na obalenie rządu.	• sponsorowanie przez państwo, donacje; • donacje, uprowadzenia, działalność kryminalna; • rabowanie banków; • indywidualni sponsorzy; • rządowi „pracodawcy"; • donacje, podatek rewolucyjny.
Terroryzm międzynarodowy	
• emigracyjne; • wspierając emigrację; • internacjonalistyczne; • Odgrywające rolę parawanu dla innych; • kontrrewolucyjne; • Islamskie grupy fundamentalistyczne; • niezorganizowani naśladowcy.	• rabowanie banków i donacje. • finansowane przez „emigrantów"; • Starające się korzystać z tzw. war chest (skrzyń wojennych); • sponsorowane przez państwo; • sponsorowane przez państwo, również przez bogate osoby prywatne; • wiernych, osoby prywatne; • finansowani przez wszystkich, rzeczywiście nie-zorganizowani, ale wielu wyszkoliło się w Afganistanie w oszustwach z użyciem kart kredytowych i upodabniają się w małej skali do przestępców w „białych kołnierzykach".

Źródło: funding of terrorist groups compared, https://moneyjihad.wordpress.com/2013/01/21/funding-of-terrorist-groups-compared/.

[41] P. Pomianowski, E. Maćkowiak, *Zwalczanie finansowania terroryzmu w świetle prawa obowiązującego w Polsce i we Francji*, Przegląd Bezpieczeństwa Wewnętrznego, 4(6), 2012, s. 75.

Rzeczywiście, większość najtragiczniejszych zamachów ostatnich lat nie miało tak skomplikowanych planów jak ataki na Nowy Jork, a więc mogły mieć znacznie szczuplejsze budżety. ONZ szacuje, że zorganizowanie zamachu bombowego na turystów na Bali kosztowało około 50 tysięcy dolarów. Zginęło ponad 200 osób. Na bomby użyte do zamachów w Madrycie terroryści wydali między 10 a 15 tysięcy dolarów. 191 ofiar śmiertelnych.

Zorganizowanie zamachów w londyńskim metrze w 2005 r. kosztowało około dwóch tysięcy dolarów. „Zwrot z inwestycji" był imponujący: na każdego wydanego dolara przypadło 1,27 mln dolarów strat. Bomby, które wybuchły w godzinach szczytu w metrze i autobusie zabiły ponad 50 osób. Profesor Lomborg szacuje, że materiały wybuchowe zamachowiec-samobójca może kupić za 150 dolarów. Siła wybuchu takiego ładunku może zabić 12 osób[42]. W tabeli 3 przedstawiono przykłady kosztów zamachów terrorystycznych.

Tabela 3. Koszty ataków terrorystycznych

Atak	Szacowany koszt
Atak w Nicei w 2016 roku	2 000 dolarów
Zamachy w Paryżu w listopadzie 2015 roku	30 000 euro
Atak w Bamako w 2015 roku	10 000 dolarów
Zamach w Mumbaju w 2008 roku	50 000 dolarów
Londyn 7 lipca 2005 roku	8 000 funtów
Madryt 11 marca 2004 roku	10 000 dolarów
Stambuł 15 i 20 listopada 2003 roku	40 000 dolarów
Dżakarta 5 sierpnia 2003 roku	30 000 dolarów
Bali 12 października 2002 roku	50 000 dolarów
USS Cole 12 października 2000 roku	10 000 dolarów

Źródło: opracowane na podstawie: Raport Financial Action Task Force, Terrorist Financing, Raport EMCDDA, Raport Europol.

Główne zagrożenia terrorystyczne pochodzą od osób inspirowanych ideologią Al-Kaidy, ISIS lub krajowego brutalnego ekstremizmu, które pragną przeprowadzać śmiertelne ataki bez wskazówek ze strony obcej grupy. Zagrożenia w dalszym ciągu w dużej mierze finansują się ze środków własnych, co stwarza poważne wyzwania.

[42] *Zamachy w Paryżu. Zorganizowanie ataku kosztuje grosze*, https://www.money.pl/gospodarka/wiadomosci/artykul/zamachy-w-paryzu-zorganizowanie-ataku,187,0,1955003.html, [dostęp: 16.05.2025].

Znacznym problemem jest to, iż grupy terrorystyczne w USA nadal przebywają w USA i wspierają Al-Kaidę lub ISIS, którzy chcą wysyłać pieniądze za granicę lub finansują podróże osób fizycznych, w dużej mierze wykorzystując sprawdzone metody, takie jak rejestracja i niezarejestrowanie MSB, gotówka, a w niektórych przypadkach aktywa wirtualne. Dodatkowo irańskie grupy zastępcze, takie jak Hamas i Hezbollah mogą wyszukać luki we wdrażaniu sankcji, aby wykorzystać formalny system finansowy. Hamas również do tego przyłącza zwolenników na całym świecie i wykorzystuje różnorodne wyrafinowane metody w celu gromadzenia funduszy na swoją sprawę[43].

Finansowanie terroryzmu jest złożonym i wielowymiarowym procesem, który obejmuje szeroki wachlarz źródeł i metod uzyskiwania funduszy przez organizacje terrorystyczne. Kluczowe źródła finansowania obejmują przestępczość zorganizowaną, handel narkotykami, przemyt ropy naftowej, porwania dla okupu oraz różnorodne przestępstwa finansowe, takie jak pranie pieniędzy i oszustwa. Organizacje terrorystyczne również korzystają z darowizn i datków, często zbieranych za pośrednictwem fałszywych organizacji charytatywnych, oraz z handlu zasobami naturalnymi, takimi jak diamenty i złoto. W ostatnich latach rosnącą rolę odgrywa cyberprzestępczość, w tym ataki ransomware, phishing oraz wykorzystanie kryptowalut do ukrywania i transferu środków. W tabeli 4 przedstawiono ranking najbogatszych organizacji terrorystycznych na świecie.

Tabela 4. Ranking najbogatszych organizacji terrorystycznych na świecie

Organizacja	Budżet
Hezbollah	1.1 miliarda dolarów
Talibowie	800 milionów dolarów
Hamas	700 milionów dolarów
Al-Kaida	300 milionów dolarów
ISIS	200 milionów dolarów
PKK – Partia Pracujących Kurdystanu	180 milionów dolarów
Kata'ib Hezbollah	150 milionów dolarów
Palestyński Islamski Dżichad	100 milionów dolarów
Lashkar-e-Taiba	75 milionów dolarów

[43] *2024 National Strategy for Combating Terrorist and Other Illicit Financing*, Department of the Treasury, 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf, [dostęp: 16.05.2025].

Organizacja	Budżet
Prawdziwa IRA	50 milionów dolarów

Źródło: The Richest Terror Organizations in the World, Forbes International, https://www.forbes.com/sites/forbesinternational/2018/01/24/the-richest-terror-organizations-in-the-world/, [16.05.2025].

Z analizy źródeł finansowania wynika, że organizacje terrorystyczne są niezwykle elastyczne i innowacyjne w swoich metodach pozyskiwania funduszy. Wykorzystują legalnie dostępne informacje w Internecie do planowania i realizacji działań przestępczych, co czyni ich operacje trudnymi do wykrycia i śledzenia. Anonimowość zapewniana przez kryptowaluty oraz globalny zasięg cyberprzestępczości dodatkowo utrudniają działania organom ścigania.

W związku z powyższym, kluczowe jest wprowadzenie i utrzymanie zintegrowanych działań na poziomie międzynarodowym, które obejmują współpracę między rządami, organami ścigania, sektorem prywatnym oraz organizacjami międzynarodowymi. Istotne jest również wprowadzenie bardziej rygorystycznych regulacji dotyczących przejrzystości finansowej oraz monitorowania transakcji, zwłaszcza tych związanych z kryptowalutami. Ponadto, zwiększenie świadomości społecznej na temat zagrożeń związanych z udostępnianiem wrażliwych informacji w Internecie może przyczynić się do ograniczenia możliwości wykorzystywania tych danych przez organizacje terrorystyczne.

Przeciwdziałanie finasowaniu terroryzmu

Momentem przełomowym w walce z terroryzmem były wydarzenia z 11 września 2001 r. Niezwykle istotne było oświadczenie przewodniczącego Parlamentu, szefów i rządów państw Unii Europejskiej, mówiące, że atak na Stany Zjednoczone był atakiem przeciwko wszystkim państwom Wspólnoty. W oświadczeniu tym wezwano również do globalnej walki z terroryzmem oraz przyjęcia planu działania przeciw terroryzmowi[44].

Termin „zwalczanie finansowania terroryzmu" odnosi się w szczególności do wszystkich zbiorów zasad i aktów prawnych, które zmuszają instytucje finansowe do aktywnego monitorowania swoich klientów w celu zapobiegania

[44] K. Bartosz, *Prawne aspekty walski z terroryzmem*, Security, Economy & Law, Nr 1(XVIII), 2018, s. 23.

finansowaniu terroryzmu[45]. Długoterminowym, strategicznym celem zwalczania finansowania terroryzmu jest odcięcie terrorystów od ich źródeł funduszy oraz przerwanie kanałów dystrybucji środków. Jest to jednak cel, którego pełne osiągnięcie nie wydaje się możliwe[46].

Przeciwdziałanie finansowaniu terroryzmu jest kluczowym elementem globalnej strategii zwalczania terroryzmu. Efektywne działania wymagają skoordynowanych wysiłków na wielu frontach, w tym legislacji, technologii, międzynarodowej współpracy i edukacji.

Wprowadzenie i egzekwowanie rygorystycznych przepisów prawnych jest fundamentalne w walce z finansowaniem terroryzmu. Rządy na całym świecie wdrażają przepisy dotyczące przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT), które wymagają od instytucji finansowych, firm i organizacji pozarządowych ścisłego monitorowania i raportowania podejrzanych transakcji. Organizacje międzynarodowe, takie jak Financial Action Task Force (FATF), opracowują i promują globalne standardy w tej dziedzinie.

Terroryzm jest problemem transnarodowym, dlatego międzynarodowa współpraca jest niezbędna. Kraje współpracują poprzez wymianę informacji wywiadowczych, wspólne operacje policyjne i wspieranie międzynarodowych sankcji finansowych wobec organizacji terrorystycznych i ich sympatyków. Organizacje międzynarodowe, takie jak ONZ i Interpol, odgrywają kluczową rolę w koordynowaniu tych działań.

Zaawansowane technologie analityczne i systemy monitoringu transakcji finansowych pomagają wykrywać podejrzane operacje finansowe. Instytucje finansowe wykorzystują systemy do monitorowania przepływów pieniędzy, które mogą być związane z finansowaniem terroryzmu, a także raportują nietypowe transakcje do odpowiednich władz. Wykorzystanie sztucznej inteligencji i analizy big data zwiększają skuteczność tych narzędzi.

Kryptowaluty, ze względu na swoją anonimowość, stanowią wyzwanie dla tradycyjnych metod monitorowania finansowania terroryzmu. Wiele krajów i organizacji międzynarodowych wprowadza regulacje dotyczące giełd kryptowalut i portfeli cyfrowych, aby zapewnić większą przejrzystość

[45] *Zwalczanie finansowania terroryzmu*, https://help.revolut.com/pl-PL/business/help/more/security-and-personal-data/what-is-terrorism-financing/, [dostęp: 16.05.2025].

[46] C. Sońta, G. Szczuciński, *Wybrane zagadnienia przeciwdziałania Terroryzmu w Polsce*, Studia Bezpieczeństwa Narodowego, nr 1, 2011, s. 51.

i możliwość śledzenia transakcji. Firmy specjalizujące się w analizie blockchain, takie jak Chainalysis, odgrywają kluczową rolę w identyfikowaniu podejrzanych działań.

Wielu terrorystów korzysta z luk prawnych i słabości ekonomicznych w niektórych krajach. Wsparcie międzynarodowe dla państw o słabszych systemach prawnych i finansowych może pomóc w budowaniu ich zdolności do przeciwdziałania finansowaniu terroryzmu. Inwestycje w rozwój infrastruktury prawnej, szkolenia dla służb oraz wsparcie technologiczne są kluczowe.

Wprowadzanie sankcji finansowych i zamrażanie aktywów osób i organizacji powiązanych z terroryzmem to skuteczne narzędzia przeciwdziałania. Międzynarodowe listy sankcyjne, takie jak te prowadzone przez ONZ i różne państwa, pomagają w identyfikowaniu i blokowaniu zasobów finansowych terrorystów. Zaangażowanie sektora prywatnego, zwłaszcza instytucji finansowych i firm technologicznych, jest kluczowe. Banki, firmy technologiczne i giełdy kryptowalutowe muszą aktywnie uczestniczyć w wykrywaniu i zgłaszaniu podejrzanych transakcji. Publiczno-prywatne partnerstwa mogą znacząco zwiększyć skuteczność działań prewencyjnych.

Walka Unii Europejskiej (UE) z praniem pieniędzy i finansowaniem terroryzmu jest priorytetem w polityce bezpieczeństwa i gospodarczej. UE stosuje złożony system regulacji, nadzoru i współpracy międzynarodowej w celu przeciwdziałania tym zagrożeniom. Unia Europejska wprowadziła szereg dyrektyw dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT). Najważniejsze z nich to:

- Czwarta Dyrektywa AML (2015): Wprowadziła wymogi dotyczące identyfikacji klientów, zgłaszania podejrzanych transakcji i prowadzenia rejestrów beneficjentów rzeczywistych. Ustanowiła centralne rejestry beneficjentów rzeczywistych w państwach członkowskich[47].
- Piąta Dyrektywa AML (2018): Zwiększyła przejrzystość poprzez publiczny dostęp do rejestrów beneficjentów rzeczywistych. Nałożyła nowe obowiązki na giełdy kryptowalut i portfele cyfrowe w zakresie

[47] Dyrektywa 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.

AML. Zwiększyła wymogi dotyczące współpracy i wymiany informacji między państwami członkowskimi[48].

- Szósta Dyrektywa AML: Obecnie trwające prace dotyczą regulacji będących częścią tzw. Pakietu AML, w skład, którego wchodzą trzy rozporządzenia (w tym AMLAR i AMLR) oraz tzw. 6 Dyrektywa. Celem 6 Dyrektywy AML ma być przede wszystkim ujednolicenie praktyk państw członkowskich Unii[49].

Jeśli chodzi o normatywne aspekty przeciwdziałania tytułowemu procederowi, należy wskazać, że na polski system prawny wpływ wywarło wiele aktów prawnych o charakterze międzynarodowym[50].

Jednym z pierwszych aktów prawnych, który zobowiązywał Polskę do wprowadzenia penalizacji finansowania terroryzmu, była Międzynarodowa Konwencja o Zwalczaniu Finansowania Terroryzmu[51]. Na podstawie niniejszego aktu prawnego każde Państwo-Strona zobowiązało się do uznania w prawie wewnętrznym finansowania terroryzmu za czyn karalny.

Drugim w tym zakresie aktem prawnym jest także Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu[52].

Kształt polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu wyznaczają przede wszystkim przepisy prawne, zarówno krajowe, jak i Unii Europejskiej (UE). Podstawowym aktem prawnym w tym obszarze jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu

[48] Dyrektywa 2018/843 zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

[49] *Jakie zmiany wprowadzi 6 Dyrektywa AML*, https://www.prawo.pl/podatki/co-zmieni-6-dyrektywa-aml,527059.html, [dostęp: 16.05.2025].

[50] W. Goleński, *Proceder prania pieniędzy – zarys problematyki*, Kontrola Państwowa, nr 4, 2023, s. 107.

[51] Międzynarodowa Konwencja o Zwalczaniu Finansowania Terroryzmu przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r. (Dz. U. z 2004 r. Nr 263, poz. 2620), która to została ratyfikowana za zgodą wyrażoną w Ustawie z dnia 9 stycznia 2003 r. o ratyfikacji Międzynarodowej Konwencji o zwalczaniu finansowania terroryzmu, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych w dniu 9 grudnia 1999 r. (Dz. U. z 2003 r. Nr 44, poz. 374).

[52] Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie dnia 16 maja 2005 r. (Dz. U. z 2008 r. Nr 165, poz. 1028), ratyfikowana za zgodą wyrażoną w ustawie z dnia 27 października 2006 r.

praniu pieniędzy oraz finansowaniu terroryzmu. Ustawa określa zasady i tryb przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu[53]. 13 grudnia 2023 r. Rada i Parlament uzgadniały wspólnie powołanie nowego urzędu ds. przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AMLA). To kluczowe osiągnięcie pakietu dotyczącego przeciwdziałania praniu pieniędzy przedstawionego przez Komisję Europejską w lipcu 2021 r. Nowe przepisy mają chronić obywateli UE i unijny system finansowy przed praniem pieniędzy i finansowaniem terroryzmu. AMLA będzie miał bezpośrednie i pośrednie kompetencje w zakresie nadzoru nad podmiotami zobowiązanymi stwarzającymi największe ryzyko w sektorze finansowym[54].

Doskonały przykład działania w tej materii stanowi realizowana przez ONZ Globalna Strategia Zwalczania Terroryzmu (A/RES/60/288): jest to unikatowy światowy instrument, który umacnia krajowe, regionalne i międzynarodowe wysiłki na rzecz zwalczania terroryzmu. Poprzez jej przyjęcie w drodze konsensusu w 2006 r. wszystkie państwa członkowskie ONZ zgodziły się na wspólne podejście strategiczne i operacyjne do walki z terroryzmem. Globalna Strategia Zwalczania Terroryzmu ONZ składa się z 4 filarów. Są to:

- eliminowanie okoliczności sprzyjających rozprzestrzenianiu się terroryzmu,
- środki na rzecz zapobiegania terroryzmowi i jego zwalczania,
- środki mające na celu zwiększanie skuteczności państw w zapobieganiu terroryzmowi i jego zwalczaniu oraz wzmocnienie roli systemu ONZ w tym zakresie,
- środki mające na celu zapewnienie poszanowania praw człowieka wszystkich osób oraz praworządności jako podstawy walki z terroryzmem.

Przeciwdziałanie finansowaniu terroryzmu wymaga kompleksowych działań. Monitorowanie przepływów finansowych, zamrażanie aktywów podejrzanych podmiotów, a także wdrażanie regulacji przeciwdziałających praniu pieniędzy są kluczowymi elementami w walce z finansowaniem terroryzmu. Skuteczna walka z tym zjawiskiem jest niezbędna dla zapewnienia globalnego bezpieczeństwa i stabilności.

[53] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, (Dz. U. z 2018 r. poz. 723), art. 1.

[54] *Walka UE z praniem pieniędzy i finansowaniem terroryzmu*, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/fight-against-terrorist-financing/timeline/, [dostęp: 16.05.2025].

Walka z praniem pieniędzy i finansowaniem terroryzmu wymaga również ciągłej adaptacji i współpracy na poziomie krajowym, regionalnym i międzynarodowym. Unia Europejska podejmuje liczne kroki w celu wzmocnienia regulacji, nadzoru i współpracy, aby skutecznie przeciwdziałać tym zagrożeniom. Inicjatywy takie jak centralne rejestry beneficjentów rzeczywistych, regulacje dotyczące kryptowalut oraz utworzenie Europejskiego Urzędu ds. Zwalczania Prania Pieniędzy stanowią kluczowe elementy tej strategii. Jednak skuteczność tych działań zależy od konsekwentnego wdrażania i egzekwowania przepisów w państwach członkowskich oraz od zdolności do szybkiej adaptacji do nowych zagrożeń.

Podsumowanie

Współczesny terroryzm to zjawisko złożone, dynamiczne i trudne do jednoznacznego zdefiniowania, zarówno pod względem form działania, jak i mechanizmów finansowania. Organizacje terrorystyczne wykazują się dużą elastycznością i zdolnością adaptacji do zmieniających się warunków geopolitycznych, technologicznych i społecznych. Wykorzystują zarówno konwencjonalne formy przemocy, jak i nowoczesne narzędzia, takie jak cyberataki, propaganda internetowa czy transakcje kryptowalutowe, co znacznie utrudnia skuteczne przeciwdziałanie ich działalności. Zróżnicowanie źródeł finansowania – od przestępczości zorganizowanej po legalne podmioty gospodarcze – powoduje, że konieczne staje się tworzenie coraz bardziej kompleksowych i interdyscyplinarnych mechanizmów kontroli oraz współpracy między państwami i instytucjami międzynarodowymi. Skuteczna walka z terroryzmem wymaga integracji działań służb wywiadowczych, instytucji finansowych, podmiotów prywatnych i społeczeństwa obywatelskiego. Wnioski płynące z przeprowadzonej analizy jasno wskazują, że tylko całościowe, skoordynowane podejście – łączące działania prewencyjne, edukacyjne, legislacyjne i technologiczne – może skutecznie ograniczyć potencjał organizacji terrorystycznych oraz minimalizować ryzyko kolejnych zamachów.

Literatura

1. Bąk T., *Oblicza terroryzmu*, Wyd. Konsorcjum Akademickie, Kraków-Rzeszów-Zamość 2011.
2. Bartosz K., *Prawne aspekty walski z terroryzmem*, Security, Economy & Law, Nr 1(XVIII), 2018.
3. Bolechów B., *Terroryzm w świecie podwubiegunowym*, Wydawnictwo Adam Marszałek, Toruń 2003.
4. Conway M., *Terrorist 'Use' of the Internet and Fighting Back*, Information & Security. An International Journal, vol.19, 2006.
5. Dyrektywa 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE.
6. Dyrektywa 2018/843 zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.
7. Don B. W. et al., *Network Technologies for Networked Terrorists. Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, RAND Technical Report, 2007.
8. Goleński W., *Proceder prania pieniędzy – zarys problematyki*, Kontrola Państwowa, nr 4, 2023.
9. Hennig R., *Cyberterroryzm miękki. Cz. 1, Internet jako źródło informacji i funduszy*, Przegląd Naukowo-Metodyczny, Edukacja dla bezpieczeństwa, Rok IX, nr 4(29), 2015.
10. Horgan J., *Psychologia terroryzmu*, Wydawnictwo Naukowe PWN, Warszawa 2015.
11. Izak K., Kluczyński M., *Handel Narkotykami jako źródło finansowania terroryzmu*, Przegląd Bezpieczeństwa Wewnętrznego, nr 10, 2014.
12. Karolczak K., *Terroryzm XXI wieku – wybrane aspekty*, Terroryzm – Studia, Analizy, Prewencja 2022, Nr 1(1), 2022.
13. Krupa Ł., *Przeciwdziałanie finansowaniu terroryzmu*, Cybersecurity and Law nr 7, 2022.
14. Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie dnia 16 maja 2005 r. (Dz.U. 2008 nr 165 poz. 1028), ratyfikowana za zgodą wyrażoną w ustawie z dnia 27 października 2006 r.
15. Liedel K., Piasecka P., Aleksandrowicz T., B*ezpieczeństwo w XXI Wieku. Asymetryczny świat*, Wydawnictwo Difin, Warszawa 2011.
16. Lisiecki L., Kucharski K., *Źródła finasowania Al-Kaidy*, Studia bezpieczeństwa narodowego, vol. 4, nr 1, 2013.
17. Lubiewski P., *Reguły i metody działania współczesnych organizacji terrorystycznych*, Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy, Nr 29(4), 2018.

18. Międzynarodowa Konwencja o Zwalczaniu Finansowania Terroryzmu przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1999 r. (Dz.U. 2004 nr 263 poz. 2620), która to została ratyfikowana za zgodą wyrażoną w Ustawie z dnia 9 stycznia 2003 r. o ratyfikacji Międzynarodowej Konwencji o zwalczaniu finansowania terroryzmu, przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych w dniu 9 grudnia 1999 r. (Dz.U. 2003 nr 44 poz. 374).
19. Nowacki G., *Zagrożenia terrorystyczne na świecie*, Nierówności Społeczne a Wzrost Gospodarczy, Nr 44, 2015.
20. Nowak P., *Bioterroryzm i chemoterroryzm jako formy współczesnego terroryzmu. Zapobieganie atakom w Rzeczypospolitej Polskiej*, „Kultura Bezpieczeństwa", Nr 36, 2019.
21. Pomianowski P., Maćkowiak E., *Zwalczanie finansowania terroryzmu w świetle prawa obowiązującego w Polsce i we Francji*, Przegląd Bezpieczeństwa Wewnętrznego, nr 6, 2012.
22. Ranstorp M., *The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation,* [w:] J. Eriksson, G. Giacomello (red.), International Relations and Security in the Digital Age, Routledge, London 2007.
23. Sońta C., Szczuciński G., *Wybrane zagadnienia przeciwdziałania finansowaniu terroryzmu w Polsce*, „Studia Bezpieczeństwa Narodowego", nr 1, vol, 1, 2011.
24. Thelesklaf D., Gercke M., *Terrorist Use of the Internet and Legal Response*, F3 – Freedom From Fear Magazine, Issue 7, July 2010.
25. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2018 poz. 723.
26. Wójcik J. W., *Przeciwdziałanie finasowaniu terroryzmu*, Wolters Kluwer, Warszawa 2007.

Netografia

1. *Cyberarmia kalifatu*, https://polska-zbrojna.pl/Mobile/ArticleShow/30080
2. *Globalny atak ransomware WannaCry może być powiązane z grupą cyberprzestępczą Lazarus – komentarz Kaspersky Lab*, https://itreseller.com.pl/globalny-atak-ransomware-wannacry-moze-byc-powiazane-z-grupa-cyberprzestepcza-lazarus-komentarz-kaspersky-lab/
3. *Jakie zmiany wprowadzi 6 Dyrektywa AML*, https://www.prawo.pl/podatki/co-zmieni-6-dyrektywa-aml,527059.html
4. Malik N., *Jak przestępcy i terroryści używają kryptowaluty: i jak to powstrzymać*, Forbes 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/
5. *Najbogatsze organizacje terrorystyczne na świecie*, https://forbes.co.il/rankings/2021terrororganizations/intro/
6. *Prezydent odznaczył zabitego przez talibów geologa*, https://www.prezydent.pl/kancelaria/archiwum/archiwum-bronislawa-komorowskiego/aktualnosci/ordery-i-odznaczenia/prezydent-odznaczyl-zabitego-przez-talibow-geologa,18399
7. *Przeciwdziałanie praniu pieniędzy: Podstawy*, https://www.pibr.org.pl/static/items/publishing/AML_cz.8_Trendy%20w%20przest-opczoCcci.pdf

8. *State sponsors of terrorism*, U.S. Department of State, https://www.state.gov/state-spon-sors-of-terrorism/
9. *Terroryści z milionami na koncie. Skąd Hamas ma pieniądze na wojnę?* https://geekweek.interia.pl/militaria/news-terrorysci-z-milionami-na-koncie-skad-hamas-ma-pieniadze-na-,nId,7085873#google_vignette
10. *The Richest Terror Organizations in the World*, Forbes International, https://www.forbes.com/sites/forbesinternational/2018/01/24/the-richest-terror-organizations-in-the-world/
11. *Walka UE z praniem pieniędzy i finansowaniem terroryzmu*, https://www.consilium.europa.eu/pl/policies/fight-against-terrorism/fight-against-terrorist-financing/timeline/
12. *Zamachy w Paryżu. Zorganizowanie ataku kosztuje grosze*, https://www.money.pl/gospodarka/wiadomosci/artykul/zamachy-w-paryzu-zorganizowanie-ataku,187,0,1955003.html
13. *Zwalczanie finansowania terroryzmu*, https://help.revolut.com/pl-PL/business/help/more/security-and-personal-data/what-is-terrorism-financing/
14. *2024 National Strategy for Combating Terrorist and Other Illicit Financing*, Department of the Treasury, 2024, https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf

dr Zbigniew Piskor
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID 0000-0002-4456-1104

https://doi.org/10.29316/9788368103205_15

ANALIZA INFORMACJI W ZARZĄDZANIU BEZPIECZEŃSTWEM LOTNISKA

ANALYSIS OF INFORMATION IN AIRPORT SAFETY MANAGEMENT

Streszczenie

Analiza informacji w zarządzaniu bezpieczeństwem stała się głównym wyzwaniem dla branży lotniczej. Wiele z obecnych procesów związanych z kontrolą bezpieczeństwa czy kontrolą paszportową będzie odbywało się automatycznie i bez udziału obsługi lotniska, minimalizując czas potrzebny na odprawę przedlotową. Powstają nowe stanowiska do których potrzeba specjalistów z dziedziny IT, którzy będą budować markę portu lotniczego, linii lotniczej nie tylko w kraju, ale w globalnym świecie. Analiza zagrożeń jakie mogą wystąpić ma wpływ na poziom bezpieczeństwa na lotnisku. Stosownie do przyjętego celu, sformułowano główny problem badawczy: Jak analiza informacji wpływa na poziom bezpieczeństwa lotniczego dla personelu, pasażerów oraz samego portu lotniczego, lotniska? Uzyskanie odpowiedzi na powyższe pytanie wymagało zastosowania metod badawczych w tym dokonania krytycznej analizy aktów

Summary

Information analysis in safety management has become a major challenge for the aviation industry. Many of the current processes related to security control or passport control will take place automatically and without the participation of airport staff, minimizing the time needed for pre-flight check-in. New positions are being created for which IT specjalists are needed, will build the brand of an airport, of an airport, an airline not only in the country but in the country but in the global world.

Analysis of the threats that may occur has an impact on the level of safety at the airport. In, accordance with the adopted goal, the main research problem was formulated: How does information analysis affect the level of aviation safety for staff, passengers, and the airport itself? Obtaining an answer to the above question required the use of research methods, including a critical analysis of legal acts and selected items of the subject literature.

prawnych i wybranych pozycji literatury przedmiotu. Analiza powyższych obszarów wskazuje, aby poprawić działalność lotniczą, należy rozważyć wprowadzenie odpowiednich środków zapobiegawczych, prewencyjnych, profilaktycznych oraz przyjąć wyznaczone kierunki zmian wskazane w wytycznych czy też dyrektywach.

Słowa kluczowe: zagrożenia, lotnictwo, bezpieczeństwo, ochrona, ryzyko

Analysis of the above areas indicates that in order to improve aviation activity, it is necessary to consider introducing appropriate preventive, preventive and prophylactic measures and adopt the designated directions of changes indicated in the guidelines or directives.

Keywords: threats, aviation, safety, aircraft, protection, risk

Wstęp

Transport lotniczy to najszybciej rozwijająca się gałąź transportu w globalnym systemie przewozu pasażerów i ładunków. Ma znaczący wpływ na światową gospodarkę, tworząc nowe miejsca pracy, rozwijając handel i pobudzając turystykę. Prędkość z jaką przemieszczają się statki powietrzne pokazuje, że samoloty są bezkonkurencyjne. Rozwój gospodarczy oprócz wpływu na zatrudnienie ma wpływ na szereg kluczowych wskaźników branży lotniczej, w tym na łączność i przystępność cenową. Trwają prace nad samolotami autonomicznymi. W przyszłości czekają nas orbitalne loty pasażerskie. Od dawna potwierdzana jest teza, że jedynie dobra organizacja jest w stanie dać dobre produkty, usługi. Hybrydowe modele biznesowe, które mają nie tylko sprzedaż wyłącznie biletów, ale całe pakiety usług lotniczych. Linie lotnicze w ten sposób finansują swoją działalność operacyjną. Kupno biletu i odprawę można załatwić kliknięciami w smartfonie.

Dlatego powstała konieczność wypracowania i stosowania działań w analizie informacji do budowania strategii i bezpieczeństwa w sektorze przemysłu lotniczego. Zgodnie ze standardami, zaleceniami Międzynarodowej Organizacji Lotnictwa Cywilnego (ICAO) w lotnictwie cywilnym wprowadzane są programy dotyczące zarządzania bezpieczeństwem lotniczym na poziomie krajowym i krajowych organizacji lotniczych poprzez Krajowy Program Ochrony Lotnictwa Cywilnego[1]. Zalecane normy i metody Postępowania Rozdziału III Załącznika 19 „Odpowiedzialność Państwa za zarządzanie

[1] Rozporządzenie Ministra Infrastruktury z dnia 2 grudnia 2020 r. w sprawie Krajowego Programu Ochrony Lotnictwa Cywilnego (Dz. U. z 2023 r. poz. 774).

Bezpieczeństwem", Rozdziału II Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 „Zarządzanie Bezpieczeństwem Lotniczym" zobowiązuje każde państwo do konsultacji z odpowiednimi stronami i ustanowiło Krajowy program bezpieczeństwa w celu zarządzania bezpieczeństwem lotnictwa cywilnego i wchodzącą w zakres jego odpowiedzialności[2]. Polityka rozwoju lotnictwa cywilnego w Polsce została opracowana i zatwierdzona przez Radę Ministrów uchwałą nr 228/2023 w sprawie przyjęcia „Polityki rozwoju lotnictwa cywilnego w Polsce do 2030 roku z perspektywą do 2040 roku", ustanawia formalne kontakty ze wszystkimi podmiotami zainteresowanymi mającymi wpływ na bezpieczeństwo, jak też ze służbami, w tym żeglugi powietrznej. Zarządzanie bezpieczeństwem musi być oparte na zadeklarowanej polityce bezpieczeństwa w organizacji lotniczej w sposób sformalizowany, wyraźnie określony i proaktywny.

Na podstawie przepisów ustawy Prawo Lotnicze, zarządzający lotniskami są zobowiązani do koordynowania prac lotniskowego zespołu do spraw bezpieczeństwa lotniskowego. Wymagania dotyczące wdrożenia zostały określone w załączniku VII Rozporządzenia (UE) nr 139/2014 oraz ADR, OR.D.005 w Podczęści D, załącznika III do w/w Rozporządzenia. Organizacje świadczące obsługę naziemną na lotniskach (*Ground Handling Service Providers*) nie mają obowiązku wdrożenia i posiadania systemu SMS, co z kolei dyktuje, że nie jest zwolniony z zarządzania bezpieczeństwem i musi podlegać w swoich działaniach do obowiązującego lotniskowego SMS-a i zgłaszania zdarzeń w ramach systemu w celu przyczyniania się do stałej poprawy bezpieczeństwa. Wynika to z konieczności współpracy z zarządzającym lotniskiem i stosowania się do Instrukcji Operacyjnej Lotniska (INOP). Kolejną istotną kwestią jest promowanie bezpieczeństwa poprzez podnoszenie świadomości, upowszechnianie doświadczeń i analizie informacji, jak również aktywne zachęcanie personelu do proponowania rozwiązań mających na celu identyfikowanie zagrożeń, co w konsekwencji będzie skutkowało poprawą bezpieczeństwa.

[2] *Krajowy Program Bezpieczeństwa w Lotnictwie Cywilnym 2024*, Ministerstwo Infrastruktury, ULC, KPBwLC_2024.pdf, s. 4.

Rola analizy informacji w zarządzaniu bezpieczeństwem lotniska

Infrastruktura lotniskowa to nie tylko port, ale urządzenia lotniskowe radionawigacyjne, wieże do kierowania lotami. To wszystko dzisiaj szybko się zmienia. Stare systemy wypierane są przez systemy satelitarne o wiele bardziej dokładne. Dlatego systemy teleinformacyjne są standardami dla wzrostu bezpieczeństwa, pozwalają obsługiwać dużo większy ruch i w sposób dużo bardziej płynny. Dzisiaj fotel pasażera nie jest zwykłym siedziskiem, lecz urządzeniem z wbudowanymi urządzeniami jak Wi-Fi, monitorem w fotelu sąsiada, stolikiem do posiłku. Globalny świat zmobilizował lotnictwo do ekonomii i ekologii mającymi na celu zminimalizowanie wpływu działalności na środowisko naturalne oraz poszukiwanie rozwiązań. W kontekście zmian klimatycznych i obaw związanych z zanieczyszczeniem środowiska, podejście ekologiczne staje się w lotnictwie coraz bardziej istotne w kluczowych aspektach jak:

- Zrównoważone paliwa lotnicze (SAF)[3] – dążenie do 2050 r. do wprowadzenia 50/50, badania nad biopaliwami i innymi alternatywnymi źródłami energii mają na celu zmniejszenie emisji związanych z tradycyjnymi paliwami lotniczymi (elektryczność, wodór).
- Emisja gazów cieplarnianych – wprowadzane regulacje mają na celu ograniczenie emisji, a także na rozwijanie technologii pozwalających na bardziej efektywne spalanie paliw. Lotnictwo jest w znacznym stopniu odpowiedzialne za część globalnych emisji CO2.
- Efektywność – nowoczesne statki powietrzne są projektowane z myślą o większej efektywności paliwowej. Ulepszone silniki przyczyniają się do obniżenia zużycia paliwa.
- Hałas lotniczy – jest problemem, który dotyka społeczności żyjące w pobliżu lotniska. Wprowadza się technologie mające na celu redukcję poprzez cichsze silniki czy trasy dolotowe i odlotowe według standardów radionawigacyjnych opartych na GPSie.
- Edukacja i świadomość ekologiczna – wśród pracowników i pasażerów sprzyja podejmowaniu bardziej świadomych decyzji i wyborów dotyczących podróży.

[3] SAF – Sustainable Aviation Fuels, zrównoważone paliwa lotnicze.

- Zarządzanie odpadami i zanieczyszczeniami – na lotniskach służby starają się zmniejszyć ilość odpadów poprzez redukcję jednorazowych opakowań, czy wprowadzenie recyklingu na lotniskach.
- Inicjatywy rządowe i międzynarodowe – ICAO, EASA, rządy poszczególnych krajów wprowadzają strategię oraz regulacje dotyczące emisji zrównoważonego rozwoju. Wymaga współpracy między różnymi interesariuszami, przemysłem, organizacjami non-profit, aby zmniejszyć negatywne skutki działalności lotniczej.

Systemy Zarządzania Bezpieczeństwem (*Safety Management System*, SMS) w organizacjach lotniczych mają za zadanie zwrócić uwagę osób zarządzających w nich odpowiednimi zasobami, takimi jak personel, czas, środki finansowe, na zdarzenia niepożądane, które mogą mieć miejsce w danym środowisku aktualnie i w przyszłości oraz nakłonić do podjęcia działań wyprzedzających, zapobiegawczych tworzących podejście proaktywne[4].

Analiza informacji w zarządzaniu bezpieczeństwem stała się głównym wyzwaniem dla branży lotniczej. Lotniska, porty lotnicze oraz przewoźnicy muszą dążyć do zmiany sposobu oferowania usług przy planowaniu podróży oraz na pokładach samolotów. Wiele z obecnych procesów związanych z kontrolą bezpieczeństwa czy kontrolą paszportową będzie odbywało się automatycznie i bez udziału obsługi lotniska, minimalizując czas potrzebny na odprawę przedlotową. Powstają nowe stanowiska, do których potrzeba specjalistów z dziedziny IT. Specjaliści IT będą budować markę portu lotniczego, linii lotniczej nie tylko w kraju, ale w globalnym świecie. Potrzeby informacyjne branży lotniczej i służącej jej celom i realizacji polityki rosną wraz z dostępnością zasobów informacyjnych. Sam dostęp do coraz większej ilości informacji nie jest wystarczającym argumentem na rzecz możliwości efektywnego wykorzystania nowych szans oferowanych przez rozwój technologiczny oraz przejście w epokę społeczeństwa sieciowego[5].

Dzielenie się informacjami o zagrożeniach i najlepszych praktykach może wpłynąć na poprawę ogólnego poziomu bezpieczeństwa. Dane są jednym z najcenniejszych zasobów, jakimi może dysponować każda organizacja. Zarządzający lotniskami muszą wdrażać różne strategie zarządzania

[4] Z. Ciekanowski. Z. Piskor, *System kontroli bezpieczeństwa w transporcie lotniczym w Polsce w latach 2015-2022*, MANS, Warszawa 2024, s. 17.

[5] K. Liedl, P. Piasecka, T. Aleksandrowicz, *Analiza informacji w zarządzaniu bezpieczeństwem*, Difin, Warszawa 2013, s. 41.

bezpieczeństwem poprzez analizę informacji z audytów, szkoleń personelu czy implementacji nowoczesnych technologii jak skanery, systemy monitorowania. Analiza informacji w zarządzaniu bezpieczeństwem lotniska odgrywa kluczową rolę wpływając na różne aspekty operacyjne i strategiczne poprzez:
Identyfikację zagrożeń w zarządzaniu bezpieczeństwem portu lotniczego, zarówno wewnętrznych jak i zewnętrznych, dzięki analizie informacji poprzez zbieranie i ocenę danych dotyczących działalności operacyjnej oraz informacji wywiadowczych pozwala na interwencję, przeciwdziałanie czy przygotowanie się na możliwe ataki. Instalacja zapór oraz systemów wykrywania i zapobiegania włamaniom w celu ochrony i monitorowania sieci jak też oprogramowania w najnowszych wersjach. Wprowadzając ograniczenie dostępu do krytycznych systemów i informacji dla uprawnionych osób. Informacja jest kluczowym elementem zapewnienia bezpieczeństwa pasażerów, personelu oraz infrastruktury w eliminacji zagrożeń:

- zagrożenie terrorystyczne poprzez ataki bombowe za pomocą ładunków umieszczonych w bagażu czy na pokładzie samolotu, katastrofa nad Szkocją, Lockerbie[6] – PAN AM 103, Boeing 747 lecący z Londynu do Nowego Jorku eksplodował w powietrzu w dniu 21.12.1988, (bomba, zbudowana z bezwonnego plastikowego materiału wybuchowego Semtex, była ukryta w odtwarzaczu kasetowym, który był przechowywany w walizce), WTC[7] porwanie samolotu, strzelanina w terminalu lotniska,
- zagrożenia przestępcze jak, przemycanie nielegalnych towarów, rzeczy (broń, narkotyki, skóry, waluta), kradzież bagażu czy dokumentów, włamania do obiektów,
- zagrożenia naturalne związane z zjawiskami pogodowymi, które mogą zakłócić operacje lotnicze (opady śniegu, burze, popiół wulkaniczny), czy katastrofy naturalne (pożary, trzęsienia ziemi),
- zagrożenia zdrowotne poprzez wprowadzenie chorób zakaźnych (epidemia COVID 19[8], błonica, cholera, ameba), czy też niezadowolenie pasażerów z powodu zarażeń w porcie lotniczym,
- zagrożenia związane z pasażerami poprzez agresywne, podejrzane zachowanie (alkohol, narkotyki), czy użycie niebezpiecznych przedmiotów

[6] *Lockerbie. 35 lat od katastrofy lotu Pan Am 103*, Podróże, [dostęp: 31.03.2025].
[7] Dlaczego po zamachach z 11 września wieże WTC runęły? To ten czynnik był decydujący – Wielka Historia, [dostęp: 07.04.2025]
[8] COVID-19 – Główny Inspektorat Sanitarny – Portal Gov.pl, [dostęp: 05.04.2025].

(substancji chemicznych, noży, powerbanki[9]), powstała lista najbardziej uciążliwych pasażerów linii lotniczych. Jakie zachowania są niedopuszczalne w czasie rejsu? Jakie kary grożą?[10]

- zagrożenia związane z transportem publicznym, które mogą wpłynąć na dojazd podróżnych do terminala, wypadki komunikacyjne do i z lotniska,
- zagrożenia wewnętrzne spowodowane poprzez niewłaściwe, nieprawidłowe działania, w tym niezastosowanie się do procedur lub wykonywanie niewłaściwych procedur operacyjnych,
- zagrożenia związane z infrastrukturą, w tym krytyczną związaną z energetyką (lotnisko Heathrow otrzymało ostrzeżenia o awariach zasilania[11]), uszkodzenie pasa startowego, terminali portu lotniczego, problemy z mobilnością, awarie pojazdów lotniskowych.

Ocena ryzyka, związanego z różnymi rodzajami zagrożeń umożliwia poprzez analizę informacji przy pomocy narzędzi analitycznych w określaniu prawdopodobieństwa wystąpienia zdarzenia lotniczego oraz potencjalnych skutków. Pozwala to w prioryteryzacji działań bezpieczeństwa lotniczego.

Decyzje operacyjne dotyczące bezpieczeństwa czy też w planowaniu działań sytuacji kryzysowych stanowią w oparciu o analizę danych informacji na szybką decyzję. Pozwala to na podjęcie odpowiednich działań w zaistnieniu sytuacji kryzysowej.

Monitorowanie i ocena, pozwala na szybką reakcję w zmieniających się okolicznościach w dostosowaniu strategii bezpieczeństwa do aktualnych potrzeb. Regularna analiza informacji pozwala na bieżąco monitorować sytuację w porcie lotniczym czy na lotnisku. Opracowanie i wdrożenie planu reagowania na incydenty z określeniem kroków do podjęcia w przypadku wystąpienia naruszenia, jak również analizowanie logów w celu wczesnego wykrywania nietypowych aktywności.

Współpracę między organizacjami, dzielenie się informacjami umożliwia lepszą współpracę między służbami i agencjami zarówno na poziomie krajowym, jak i międzynarodowym w zakresie wymiany informacji na temat zagrożeń. Dostosowanie działań do międzynarodowych standardów i regulacji

[9] *Ograniczenia w samolotach po wielkim pożarze. Trzeba uważać na powerbanki – Podróże Wprost*, [dostęp: 04.05.2025].

[10] *Czarna lista uciążliwych pasażerów. Nowa inicjatywa KLM i Transavii,* INNPoland.pl, [dostęp: 15.04.2025].

[11] *Lotnisko Heathrow otrzymało ostrzeżenia o awariach zasilani*a, [dostęp: 01.04.2025].

(ICAO, EASA). Szkolenie i edukacja personelu w organizacjach, komórkach, działach, musi być cyklicznie prowadzona. Zrozumienie trendów i wzorców przez personel, który ma odpowiedzialne zadania operacyjne, a do których musi być przeszkolony teoretycznie i praktycznie w celu radzenia sobie z zagrożeniami, a co zwiększa efektywność działań proaktywnych. Regularne szkolenia z zagrożeń cybernetycznych, rozpoznawania phishingu oraz bezpiecznych praktyk w użytku IT.

Technologię i innowację poprzez wykorzystanie nowoczesnych urządzeń do prowadzenia działań operacyjnych w kontroli, nadzorowaniu czy monitorowaniu sytuacji w czasie rzeczywistym, identyfikacji zagrożeń, podejmowaniu decyzji operacyjnych. Co przekłada się na bardziej zaawansowany i efektywny zbiór informacji przekładający się na sprawniejsze, lepsze zarządzanie bezpieczeństwem. Wykorzystanie technologii AI do analizy zbiorów danych w celu identyfikacji potencjalnych zagrożeń.

Wpływ szkolenia personelu na kształtowanie świadomości sytuacyjnej

Lotnictwo jest tą dziedziną działalności człowieka, w której stawia się szczególnie wysokie wymagania przed osobami zaangażowanymi w proces przygotowania i realizacji zadań. Nauka o bezpieczeństwie oparta jest o dyscypliny naukowe, jak: medycyna pracy, cybernetyka, ergonomia, socjologia, psychologia, diagnostyka, teoria niezawodności, teoria systemów, teoria ekonomiczna, teoria eksploatacji. Bezpieczeństwo lotów[12] badane jest jako jedna z dziedzin bezpieczeństwa pracy. W praktyce rozumie się je jako całokształt właściwości zapobiegających sytuacjom awaryjnym oraz zmniejszania skutków możliwości wystąpienia sytuacji poprzez zastosowanie odpowiednich systemów chroniących życie i zdrowie pasażerów i załogi na pokładach samolotów.

Od konstruktorów po pilotów, określanych mianem ostatniego ogniwa w łańcuchu bezpieczeństwa lotniczego. Istotną rolę odgrywa personel techniczny i kontrolerzy ruchu lotniczego, obsługa naziemna. W dzisiejszych czasach szczególnie dużą wagę przywiązuje się do pożądanego stanu tzw. świadomości sytuacyjnej (*Situational Awareness*, SA) poprzez odpowiednie

[12] E. Klich, *Bezpieczeństwo lotów*, Wydawnictwo Naukowe Instytutu Technologii Eksploatacji – PIB, Radom 2011, s. 31.

szkolenia teoretyczne i praktyczne. Niezależnie od rodzaju lotnictwa branego pod uwagę (linie lotnicze, lotnictwo ogólne, bussinesowe, czy też państwowe - lotnictwo policji, lotnictwo straży granicznej, HEMS, lotnictwo sił zbrojnych) utrzymanie pożądanego stanu personelu jest jednym z zasadniczych elementów decydujących o poziomie bezpieczeństwa w realizacji zadań lotniczych. Analiza informacji skupiać się ma wokół tematu oceny i oszacowania znaczenia błędów i zagrożeń i ich wpływu na bezpieczeństwo lotów. Uczy, jak szybko rozpoznać elementy łańcucha błędów oraz zrozumienia wagi podejmowania takich działań, które zmierzają do przerwania tegoż łańcucha.

Dział bezpieczeństwa w każdej organizacji lotniczej zajmuje się także uzmysłowieniem pracownikom faktu, że błąd ludzki nie równa się błędowi pilota. Wypadki są wynikiem ciągu zdarzeń powiązanych ze sobą, są procesem składającym się z kilku albo nawet kilkunastu ogniw. Są rezultatem sekwencji zdarzeń, które kumulują się, prowadząc do wypadku.

Bezpieczeństwo w lotnictwie w całości zależy od profesjonalizmu każdego pracownika, absolutnie bez znaczenia, czy pracuje on w powietrzu, czy na ziemi. Od wiedzy, umiejętności, zdolności zależy spełnienie wymogów bezpieczeństwa, a zatem życia pasażerów, spokoju na pokładzie. Zarządzanie ryzykiem oraz obszary błędów zidentyfikowanych na podstawie zaistniałych zdarzeń, katastrof w lotnictwie komercyjnym wskazują na ich analizę i wnioski, które stanowią materiał do przemyślenia. Nowe technologie i innowacje jak sztuczna inteligencja, uczenie maszynowe i robotyka procesów mają swój potencjał w analizie informacji danej organizacji, poprawiając szybkość, dokładność, efektywność w obszarze zarządzania bezpieczeństwem.

Podniesienie poziomu świadomości dotyczącej wagi czynnika ludzkiego i jego wpływu na operacje lotnicze bez wskazywania palcem winnych. Trening nie może opierać się tylko na nauce teorii, musi dążyć do wytworzenia świadomości potencjalnych zagrożeń i opierać się na aktywnym działaniu mającym na celu podniesienie efektywności działań, w tym analizy informacji w zarządzaniu bezpieczeństwem portu lotniczego, lotniska. Promuje także świadomość zachowań ludzkich, poprawia komunikację i relacje interpersonalne osób zaangażowanych w operacje lotnicze (piloci, stewardessy/stewardzi, pracownicy wieży kontroli lotów, obsługa naziemna, mechanicy).

Pozwala zobaczyć szerszą perspektywę związaną z natężeniem operacji powietrznych, planowaniem załóg na lot, planowaniem szkoleń. Uświadamia także ogromną wagę odpowiedniej współpracy z firmami oraz osobami

niezatrudnionym bezpośrednio przez operatora, takimi jak straż graniczna, straż pożarna, inżynierowie, mechanicy, agenci handlingowi, obsługa check in, inspektorzy CAA (*Civil Aviation Authority*), pracownicy cateringu, osoby odpowiedzialne za tankowanie samolotu i wiele innych. Identyfikacja z organizacją wykazywana jest w postawie, lojalności, satysfakcji i przynależności do branży. Wprowadzani powinni być w środowisko poprzez odpowiednio przygotowanych, przeszkolonych współpracowników celem adaptacji do osiągnięcia pełnego profesjonalizmu.

Organizacja wyróżniająca się wysokim poziomem kompetencji charakteryzuje się wysokim profesjonalizmem w zakresie motywowania całej załogi. Ponadto: budowaniem pozytywnego podejścia do realizacji zadań, zapewnieniem odpowiedniego wpływu na wykonywaną pracę, traktowaniem każdego w indywidualny sposób, zaangażowaniem w karierę, bieżącym ocenianiem według jasno sprecyzowanych kryteriów dla wszystkich pracowników. Funkcjonowanie społeczne człowieka odbywa się w relacjach z innymi ludźmi.
Osiągnięcie sukcesu zawodowego i osobistego jest uzależnione od umiejętnego zarządzania emocjami, w tym posiadania wysokich kompetencji, przez co osoby te są cenionymi pracownikami, mają dobre kontakty z ludźmi, pracują efektywnie. Osiągnięta, a następnie pogłębiana wiedza teoretyczna, począwszy od edukacji szkolnej, poprzez umiejętności panowania nad sobą, pragnienie rozwijania własnej kariery, zdolności przystosowania się, polubownego rozwijania konfliktów, przyczyniają się do umiejętnego panowania w sytuacjach, w których mają miejsce bezpośrednie kontakty interpersonalne, wymagające asertywności.
Wprowadzenie i rozwój szkoleń doprowadziło do potwierdzenia faktu, że bezpieczeństwo i wydajność lotu może zostać uzyskana jedynie poprzez pracę zespołową załogi.

Bardzo ważną umiejętnością, jaką powinien mieć każdy członek załogi, jest umiejętność pracy zespołowej. Przy doborze pracowników do organizacji szczególną uwagę zwraca się na kandydatów posiadających umiejętności pracy w zespole, nie tylko na poziom współpracy i komunikacji z członkami zespołu, ale także z wszystkimi pracownikami organizacji, dzielenie się wiedzą i doświadczeniem. Dzięki współpracy i uzupełnianiu się członkowie zespołu mogą osiągać więcej[13]. Według J.R. Katzenbach i D.R. Smith to mała grupa

[13] W. Bańka, *Zarządzanie potencjałem społecznym w nowoczesnej organizacji*, Wydawnictwo NOVUM, Płock 2005, s. 352.

ludzi posiadająca komplementarne umiejętności, wspólne podejście do pracy, zaangażowanych w działania do osiągnięcia celu, za który wszyscy czują się odpowiedzialni[14].

Dla przykładu szkolenie CRM obejmuje następujące główne tematy:

- błędy spowodowane przez czynnik ludzki, łańcuch pomyłek i podejmowanie działań, przerywających ten łańcuch,
- polityka bezpieczeństwa przewoźnika, standardowe procedury operacyjne, organizacja pracy i podział obowiązków w załodze,
- stres, panowanie nad stresem, zmęczenie i czujność,
- przyswajanie zdobytych informacji oraz ich przetwarzanie, świadomość sytuacyjna, kierowanie obciążającymi zadaniami,
- podejmowanie decyzji,
- skuteczne porozumiewanie się i koordynacja pomiędzy członkami załogi lotniczej oraz z personelem pokładowym,
- przywództwo i zachowanie się załogi w przypadku utraty informacji lub kierownictwa,
- wpływ automatyzacji na CRM,
- wpływ różnic w osobowości na wzajemne relacje członków załogi,
- statystyki i przykłady wypadków lotniczych, spowodowanych przez czynnik ludzki.

Współpraca zespołowa to odpowiedzialność, która skupia się na skutecznym i umiejętnym kierowaniu daną grupą. Budowanie relacji z innymi jest zadaniem trudnym i złożonym, a realizacja zależy od predyspozycji cech osobowościowych, jak i od ukształtowanych umiejętności w procesie socjalizacji jednostki, od czynników wrodzonych, jak np. inteligencja płynna czy skrystalizowana, cech temperamentnych i osobowościowych, doświadczeń wyniesionych z interakcji społecznych, pozyskiwanie zaufania i poparcia oraz udzielanie wsparcia[15]. Dla członka załogi lotniczej, który jest specjalistą od budowania dobrych relacji, priorytetem jest wdrażanie wartości wspierających

[14] J.R. Katzenbach, D.K. Smith, *Siła zespołów*, Wyd. Oficyna Ekonomiczna i Dom Wydawniczy ABC, Kraków 2001, s. 55; W. Bańka*, Zarządzanie potencjałem społecznym w nowoczesnej organizacji*, Wydawnictwo NOVUM, Płock 2005, s. 353.

[15] A. Matczak, *Temperament a kompetencje społeczne,* [w:] *Psychologia różnic indywidualnych: wybrane badania inspirowane Regulacyjną Teorią Temperamentu Profesora Jana Strelaua*, red. W. Ciarkowska, A. Matczak, Wydawnictwo Uniwersytet Warszawski, Interdyscyplinarne Centrum Genetyki Zachowania, Warszawa 2001, s. 53-69.

budowanie relacji wzajemnego wsparcia i zaufania. Jest to postawa propagowana w całej organizacji, branży lotniczej, a także społeczności, w której dana osobowość funkcjonuje.

Christine Negroni w swej książce *Na tropie niewyjaśnionych katastrof lotniczych* przekonuje, jak niewiele trzeba, by narazić życie osób na pokładzie. Bo do coraz częstszych przyczyn zdarzeń należy wymienić problemy w komunikacji, błędy w projektowaniu samolotów, silników, zbytnie zaufanie do technologii, błędy popełniane przez załogę w kokpicie, mechaników. Dlatego opanowanie sztuki rozwiązywania konfliktów jest też elementem kształtowania wizerunku osobistego. Osobiste umiejętności w tym zakresie stanowią to, co warto opanować, budując pozytywny wizerunek.

Analiza danych w celu podejmowania decyzji w zarządzaniu bezpieczeństwem lotniska

System bezpieczeństwa w lotnictwie to kompleksowe podejście do zapewnienia bezpieczeństwa we wszelkich operacjach związanych z lotniczą działalnością. Obejmuje różne aspekty, od zapewnienia bezpieczeństwa pasażerom, załodze, personelowi lotniskowemu oraz ochrona przed terroryzmem, cyberterroryzmem, minimalizacja ryzyka wypadków i awarii.

Globalne i europejskie wymagania nakazały potrzebę rozwijania procesowych systemów zarządzania adekwatnych dla aktywności firm w sektorze lotniczym, do których należą:

- SMS – Safety Management System – System Zarządzania Bezpieczeństwem,
- MMS – Maintenance Management System – System Zarządzania Utrzymaniem,
- QMS – Quality Management System – System Zarządzania Jakością,
- RSM – Risk Management System – System Zarządzania Ryzykiem.

Analiza informacji w zarządzaniu bezpieczeństwem lotniska, portu lotniczego jest konieczna poprzez zastosowanie zaawansowanych technologii, systemów monitorowania. Najbliższe kilka lub kilkanaście lat to okres dalszego poszerzania kręgu osób związanych z lotnictwem, do których będą adresowane omawiane szkolenia i w których udział będzie obowiązkowy. Szkolenia w niedalekiej przyszłości będą zapewne prowadzone nie tylko w obrębie jednej organizacji, ale też będą łączone dla różnych grup, przedstawicieli kilku firm

w celu polepszenia współpracy między jednostkami i dalszej minimalizacji zdarzeń lotniczych w zapobieganiu atakom cybernetycznym, ochronie portów lotniczych, w zapewnianiu bezpieczeństwa podróżnych oraz ochrony infrastruktury lotniczej. Dobrze zorganizowany system analizy informacji wspiera oprócz wszelkich działań bezpieczeństwa, komfort podróży, co jest kluczowe w branży lotniczej. Niezależnie od systemów funkcjonowania, zarządzania, modyfikacji wewnętrznych struktur, wymaga to zaplanowania i przygotowania odpowiednich rozwiązań, które pozwolą na utrzymanie dotychczasowego bezpieczeństwa w organizacji lotniczej. Należy zwracać uwagę na możliwe niedociągnięcia mogące stanowić barierę w komunikacji, nieprofesjonalne zarządzanie zainteresowanymi stronami, jak również stosowane metody i narzędzia w zarządzaniu zmianą poprzez upraszczanie problemów oraz braku monitorowania postępów. Na bieżąco powinna być aktualizowana lista zidentyfikowanych zagrożeń z analizą informacji i przypisanego ryzyka. Dobór odpowiednich działań naprawczych powinien uwzględniać specyfikę podmiotu lotniczego, by nie powodować zagrożeń. Implementacja działań naprawczych powiązana jest z monitorowaniem postępu eliminacji zagrożeń oraz związanego z nimi ryzyka. W przypadku braku poprawy założonych rezultatów cykl bezpieczeństwa należy powtórzyć.

ICAO w swych rekomendacjach wyróżnia następujące etapy cyklu zarządzania bezpieczeństwem:

- zbiór danych,
- analiza danych,
- hierarchizacja warunków niebezpiecznych,
- wypracowanie strategii działania,
- zaakceptowanie strategii działania,
- przyporządkowanie odpowiedzialności oraz implementacja strategii,
- ocena ponowna sytuacji bezpieczeństwa,
- zbiór dodatkowych danych.

Analiza informacji pozwala na określenie zagrożeń mogących stanowić ryzyko dla bezpieczeństwa, prawdopodobieństwo oraz potencjalne skutki wystąpienia poprzez wnioski z analizy jakościowej i ilościowej. Poszukiwanie odpowiedzi na pytania: co i kiedy może się wydarzyć, w jaki sposób? Hierarchizacja warunków niebezpiecznych prowadzona jest w celu określenia, które zagrożenia stanowią największy problem dla bezpieczeństwa i wymagają stosownych działań naprawczych. Wypracowanie koncepcji działania umożliwia

stworzenie strategii w celu całkowitego wyeliminowania ryzyka, czy też ograniczenia go bądź zaakceptowania.

Trendy i najlepsze praktyki w zakresie transformacji cyfrowej w analizie informacji

Organizacja lotnicza realizując politykę bezpieczeństwa, alokuje posiadane zasoby, definiuje standardy bezpieczeństwa lotniczego w organizacji, jak również zachowuje ciągłość realizacji przedsięwzięć, zasad oraz monitorowania w osiąganiu celów i przestrzeganiu przyjętych standardów w formalnym systemie nadzoru nad bezpieczeństwem transportu lotniczego i ochronie w lotnictwie. Musimy zauważyć, że obejmuje coraz bardziej zaawansowaną technologię zabezpieczeń. Należą do nich przede wszystkim:

- opakowania, kontenery odporne na tzw. nieuprawnioną ingerencję,
- systemy wykrywania materiałów wybuchowych,
- biometryczne poświadczenia identyfikacji każdego pracownika oraz przyznanych kontroli dostępu.

Transformacja cyfrowa w zarządzaniu bezpieczeństwem lotnisk to kluczowy obszar, który zyskuje na znaczeniu z powodu rosnących oczekiwań dotyczących bezpieczeństwa, w tym wydajności operacyjnej personelu, łącząc innowacje technologiczne z odpowiedzialnością za komfort i bezpieczeństwo pasażerów. Dostarcza informacji niezbędnych do podejmowania decyzji dotyczących zarządzania ryzykiem, w tym wyboru odpowiednich środków ochrony, które można wdrożyć w celu minimalizacji zagrożeń poprzez najlepsze praktyki związane z tą dziedziną:

- zaawansowana Analiza Danych i integracja danych poprzez wykorzystanie algorytmów do analizy danych wykorzystując: monitoring, wideo, dane operacyjne w celu przewidywania zagrożeń i optymalizacji procesów oraz do uzyskania pełnego obrazu sytuacji,
- Internet rzeczy, Internet of Things, systemy GPS i techniki mobilne, automatyzacja, robotyzacja, co pozwalana na lepsze planowanie operacji i zasobów,
- zarządzanie bezpieczeństwem, cyberbezpieczeństwo, bardziej dokładne kontrole poprzez rozpoznawanie twarzy, analiza ruchu, na lotniskach są wykorzystywane do poprawy wizerunku i przewidywania potencjalnych zagrożeń,

- współpraca i integracja, można stworzyć bardziej spersonalizowane informacje dla pasażerów o lotach, promocjach, oferty oparte na preferencjach podróżnych użytkowników aplikacji mobilnych na platformach,
- rozwiązania chmurowe, wykorzystanie nowoczesnych technologii pozwala na zbieraniu dużej ilości danych w czasie rzeczywistym. Informacje dotyczą warunków pogodowych, sytuacji na drogach startowych i kołowania, ruchu i ilości pasażerów,
- zrównoważony rozwój, lotniska, operatorzy dzięki ścisłemu śledzeniu zużycia paliw, energii, emisji CO2 mogą wdrażać działania pomagające w osiąganiu celów.

Technologia, która nie tylko poprawia bezpieczeństwo, ale także zmniejsza ilość zanieczyszczeń w środowisku. Ciągły postęp cyfryzacji poprzez narzędzia IT w każdej płaszczyźnie funkcjonowania i prowadzenia działalności lotniczej wprowadził zmiany i modyfikacje w zapewnieniu bezpieczeństwa transportu lotniczego. W przyszłości można oczekiwać dalszego rozwoju tych technologii oraz ich integracji w codzienne operacje lotniskowe od portu lotniczego do statków powietrznych włącznie.

Podsumowanie

Transport lotniczy składa się z wielu współzależnych systemów powiązanych współpracą przez kraje i kontynenty. Według prognoz (IATA) Międzynarodowego Zrzeszenia Przewoźników Powietrznych kreuje i przyspiesza procesy globalizacji. Dane jakie są gromadzone na potrzeby analiz w różnych formatach są najcenniejszymi zasobami w dyspozycji organizacji lotniczej. Nowe technologie wiążą się z koniecznością zabezpieczenia przed cyberatakami. Piloci w swej pracy wykorzystują iPady zamiast tradycyjnej dokumentacji papierowej. Lotniska, porty lotnicze oraz przewoźnicy muszą dążyć do zmiany sposobu oferowania usług przy planowaniu podróży oraz na pokładach samolotów. Wiele z obecnych procesów związanych z kontrolą bezpieczeństwa czy kontrolą paszportową będzie odbywało się automatycznie i bez udziału obsługi lotniska, minimalizując czas potrzebny na odprawę przedlotową.

Analiza informacji w zarządzaniu bezpieczeństwem lotniska jest fundamentem skutecznego i efektywnego zarządzania bezpieczeństwem lotniska, pomagając w identyfikacji zagrożeń, ocenie ryzyka, podejmowaniu decyzji operacyjnych oraz w monitorowaniu sytuacji. Walka z lukami w przepisach

oraz z cyberprzestępczością poprzez Dyrektywę NIS2 nakłada nowe obowiązki na branżę lotniczą jako kluczowy ważny podmiot i musi spełniać szczególne kryteria. Dążąc do osiągnięcia pełnej harmonizacji w prowadzonej działalności lotniczej w branży, należy poszczególne kwestie rozwiązywać na poziomie organizacji lotniczej bądź państwa odnoszących się do systemu lotniczego danego kraju w ramach konsultacji z odpowiednimi zainteresowanymi stronami. Analiza informacji przez podmioty lotnicze podejmując starania w kierunku wdrożenia odpowiednich narzędzi w tym wskaźników SPIs i planowania działań zapobiegawczo – naprawczych i analizy ryzyka.

Obecnie powstająca koncepcja wprowadzania tzw.: „Zintegrowanych Systemów Zarządzania Bezpieczeństwem[16]", co doprowadzi w niedalekiej przyszłości poprzez analizę informacji, gdy zostaną wypracowane odpowiednie rozwiązania i wprowadzone do Załącznika 19 Konwencji Chicagowskiej.

Dlatego ciągłe doskonalenie poprzez regularne przeprowadzenie audytów w ewaluacji i testowaniu w celu oceny skuteczności stosowanych rozwiązań ułatwia aktualizowanie strategii i procedur w celu lepszego dostosowania do zmieniającego się katalogu zagrożeń cybernetycznych. Pozwala na lepsze zarządzanie ryzykiem i ochronę zarówno informacji, jak też infrastruktury krytycznej.

Literatura

1. Ciekanowski Z., Piskor Z., *System kontroli bezpieczeństwa w transporcie lotniczym w Polsce w latach 2015-2022*, MANS Warszawa 2024,
2. Liedl K., Piasecka P., Aleksandrowicz T., *Analiza informacji w zarządzaniu bezpieczeństwem*, DIFIN, Warszawa 2013,
3. Klich E., *Bezpieczeństwo lotów,* Instytut Technologii Eksploatacji – PIB, Radom 2011.
4. Klich E., *Bezpieczeństwo lotów – wybrane zagadnienia*, AON, Warszawa 1999.
5. Klich E., *Bezpieczeństwo lotów. Wypadki, przyczyny, profilaktyka*, Zakład Poligraficzny WISŁA, Puławy 1998.
6. IKKU – *Seminarium szkoleniowe, Systemy zarządzania bezpieczeństwem w lotnictwie (SMS)*, Warszawa 2011.
7. Krystek R, *Zintegrowany system bezpieczeństwa transportu*. T.I. Diagnoza bezpieczeństwa transportu w Polsce,
8. Zając G., *Wspólna polityka lotnicza Unii Europejskiej*, Państwowa Wyższa Szkoła Wschodnioeuropejska w Przemyślu Przemyśl 2009.

[16] iSMS – Integrated Safety Management System, Zintegrowanych Systemów Zarządzania Bezpieczeństwem, KPBwLC_2024, s. 14.

9. Żylicz M., *Prawo lotnicze międzynarodowe, europejskie i krajowe*, Wydawnictwo Prawnicze LexisNexis TM, Warszawa 2002.
10. EASA, Annual Safety Review 2023.

Netografia

1. COVID-19 – Główny Inspektorat Sanitarny – Portal Gov.pl, https://www.gov.pl/web/gis/covid-19.
2. Czarna lista uciążliwych pasażerów. Nowa inicjatywa KLM i Transavii, https://innpoland.pl/185248,czarna-lista-pasazerow-lotniczych.
3. Dlaczego po zamachach z 11 września wieże WTC runęły? To ten czynnik był decydujący - WielkaHistoria, https://wielkahistoria.pl/dlaczego-po-zamachach-z-11-wrzesnia-wieze-wtc-runely-to-ten-czynnik-byl-decydujacy/.
4. Lockerbie. 35 lat od katastrofy lotu Pan Am 103 – Podróże, https://podroze.onet.pl/ciekawe/lockerbie-35-lat-od-katastrofy-lotu-pan-am-103/ytczj1z.
5. Ograniczenia w samolotach po wielkim pożarze. Trzeba uważać na powerbanki – Podróże Wprost, https://podroze.wprost.pl/turystyka/11932911/ograniczenia-w-samolotach-po-wielkim-pozarze-trzeba-uwazac-na-powerbanki.html.

dr Marcin Sztobryn
Lotnicza Akademia Wojskowa w Dęblinie
ORCID: 0009-0004-4981-7713

https://doi.org/10.29316/9788368103205_16

FUNKCJE, CELE ORAZ CZYNNIKI DETERMINUJĄCE SZKOLENIE PERSONELU SŁUŻBY INŻYNIERYJNO-LOTNICZEJ

FUNCTIONS, OBJECTIVES AND FACTORS DETERMINING THE TRAINING OF AIRCRAFT MAINTENANCE PERSONNEL

Streszczenie

Rozwój pracowników jest jednym z istotnych aspektów dla organizacji działających w sektorze lotniczym. Wynika to z konieczności opracowania bardziej ukierunkowanego i spójnego podejścia do rozwoju pracowników w obliczu szybkich zmian w organizacjach. Kierownictwo musi zrozumieć i docenić znaczenie zapewnienia szkoleń pracownikom, uznając, że szkolenie jest kluczowym elementem skuteczności organizacji. W branżach opartych na technologii, takich jak organizacje obsługi samolotów, szkolenie dla personelu technicznego ma szczególne znaczenie. Z tego powodu kierownictwo musi precyzyjnie zdefiniować wymagane programy szkoleniowe, skupiając się na osiąganiu konkretnych rezultatów,

Summary

Employee development is one of the important aspects for organizations operating in the aviation sector. This is due to the need to develop a more focused and coherent approach to employee development in the face of rapid changes in organizations. Management must understand and appreciate the importance of providing training to employees, recognizing that training is a key element of organizational effectiveness. In technology-based industries such as aircraft maintenance organizations, training for technical staff is particularly important. For this reason, management must precisely define required training programs, focusing on achieving specific results, and develop methods to measure the effectiveness of training.

a także opracować metody pomiaru skuteczności szkoleń. Konieczne jest poważne rozważenie czynników wpływających na efektywność szkolenia, aby inwestycja w szkolenie przyniosła oczekiwane korzyści. Celem rozdziału jest identyfikacja determinantów działalności szkoleniowej ukierunkowanych na personel inżynieryjno-lotniczy. Badania przeprowadzono w bazie szkolenia lotniczego. Podkreślono istotne zagadnienia związane ze szkoleniami i rozwojem personelu SIL. Nie można zignorować znaczenia szkoleń w dostarczaniu niezbędnej wiedzy i umiejętności. W związku z tym, szkolenie powinno być wystarczająco efektywne, aby osiągnąć te cele.

Słowa kluczowe: szkolenie specjalistyczne, personel służby inżynieryjno-lotniczej, samolot M-346, bezpieczeństwo lotów

It is necessary to seriously consider the factors affecting the effectiveness of training so that the investment in training brings the expected benefits. The purpose of this material is to identify the determinants of training activities targeted at maintenance staff. The research was conducted at an aviation training base. Important issues related to the training and development of maintenance staff were highlighted. The importance of training in providing the necessary knowledge and skills cannot be ignored. Therefore, training should be effective enough to achieve these goals.

Keywords: specialized training, maintenance staff, M-346 aircraft, flight safety

Wstęp

Organizacje uświadomiły sobie istotę szkoleń oraz kluczową rolę, jaką pełnią w poprawie efektywności pracy i wydajności pracowników. Nie ma znaczenia rodzaj organizacji czy też charakter prowadzonej działalności. Szkolenia i ich efektywność są obecnie przedmiotem szczególnej uwagi i troski. Szkolenia stanowią doskonałe narzędzie do przygotowania pracowników do konkretnych działań lub umożliwienia im uzupełnienia ewentualnych braków w umiejętnościach.

Ze względu na zróżnicowanie organizacji pod względem wielkości, celów, funkcji, złożoności, struktury oraz fizycznego charakteru produktu, szkolenia powinny być dostosowane do specyficznych potrzeb każdej z nich. Również ich atrakcyjność jako pracodawców i wkład w szkolenia mogą się różnić, co podkreśla znaczenie indywidualnego podejścia do planowania i realizacji procesów szkoleniowych. Jednak głównym celem szkoleń jest „zapewnienie, że organizacja będzie stale odpowiednio zabezpieczona pracownikami posiadającymi umiejętności odpowiadające potrzebom…". Oznacza to utrzymanie optymalnej liczby pracowników, bez nadmiaru ani niedoboru. Przy

rozpatrzeniu zarówno ogólnej liczby, jak i w zakresie personelu w dowolnej specjalności czy na różnych poziomach stanowisk pracy[1].

Celem rozdziału jest identyfikacja determinantów działalności szkoleniowej ukierunkowanych na personel inżynieryjno-lotniczy. Skuteczność, w tym kontekście, odnosi się do osiągnięcia lub nieosiągnięcia założonych celów. Dodatkowo, istotne jest zwrócenie uwagi na fakt, że efektywność zwykle koreluje z motywacją pracowników do osiągania lepszych wyników w pracy, co stanowi bezpośredni cel szkolenia.

Przedmiotem analizy stała się działalność szkoleniowa personelu SIL w bazie lotniczej. Natomiast problem badawczy, jaki przyjęto, został wyrażony pytaniem: Jakie funkcje, cele oraz czynniki determinują działalność szkoleniową personelu SIL w bazie lotniczej? Do głównych metod badawczych stosowanych w tych dociekaniach naukowych zaliczono: kwerendę literatury, indukcję i dedukcję oraz sondaż diagnostyczny. Bazą do analizy były pozycje zwarte oraz artykuły.

Rozdział został podzielony na trzy merytoryczne części. Pierwsza ma charakter wprowadzający i dotyczy funkcji i celów działalności szkoleniowej jako szczególnego zasobu organizacji. Druga część skupia się na czynnikach determinujących efektywność szkoleń. W ostatniej części uwagę skierowano na przedstawienie wyników badań zrealizowanych w procesie obsługi samolotów w bazie lotniczej. Całość wieńczy podsumowanie. Ze względu na pojemność tematu podjęte studium należy traktować jako zarys problemu.

Funkcje i cele działalności szkoleniowej

Szkolenia stanowią jedno z narzędzi rozwoju pracowników. W literaturze przedmiotu można znaleźć różne definicje tego terminu, ale praktycznie wszystkie opisują go jako proces mający na celu rozwijanie umiejętności i kompetencji pracowników.

Specyficznym rodzajem szkolenia jest proces przygotowania personelu lotniczego wykonywania zadań w jednostkach sił zbrojnych. Według prof. Dariusza Bogusza, który zajmuje się treningiem pilotów wojskowych, szkolenie lotnicze ma na celu przekazanie teoretycznej wiedzy oraz praktycznych umiejętności niezbędnych do obsługi samolotów i zapewnienia bezpiecznych

[1] L. Morton, *Integrated and integative talent management: A strategic HR framework*., The Conference Board, New York 2004, s. 21.

lotów. Szkolenia lotnicze są realizowane przez szkoły lotnicze, które są upoważnione i certyfikowane do prowadzenia tego rodzaju szkoleń. Szkolenie skupia się na nauce konkretnych umiejętności lub zwiększaniu wiedzy w określonym obszarze zawodowym. Prowadzone jest przez specjalistów z danej dziedziny, którzy posiadają praktyczne doświadczenie w danym obszarze.[2]

Ponadto wyposażenie i dobrze wyszkolony i mobilny personel są ważnymi elementami funkcjonowania każdej organizacji, co jest szczególnie widoczne w Siłach Powietrznych, jak i Sił Zbrojnych RP. Badania oparte na krytycznej analizie literatury przedmiotu wskazują na wydajne struktury i kadrę wojskową jako ważny aspekt funkcjonowania każdej organizacji. Uwidacznia to organizacja poszczególnych rodzajów Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP), których struktury organizacyjne ciągle ewoluują. Tworzenie nowych jednostek, sformowanie, rozformowanie, zmiany dyslokacji oraz podporządkowania różnych instytucji militarnych i ich dowództw to codzienność funkcjonowania SZ[3]. Nawet najnowocześniejszy sprzęt bez profesjonalnych operatorów nic nie znaczy. Odpowiednie struktury, wyszkolona kadra i wystarczające środki techniczne są podstawą do osiągnięcia celu i wypełnienia powierzonych zadań[4]. Problematyka szkolenia lotniczego i jego efektywności jest istotna ze względu na jego koszty. W najbogatszych krajach, czego przykładem może być Wielka Brytania, szuka się oszczędności w dziedzinie szkolenia personelu lotniczego i pilotów wojskowych[5].

W niniejszym rozdziale założono, że szkolenia to kompleksowe, systematyczne działania podejmowane przez organizacje, mające na celu rozszerzenie wiedzy, rozwój umiejętności i kształtowanie pożądanych postaw pracowników. Ich celem jest poprawa efektywności pracy oraz umożliwienie osiągania obecnych i przyszłych celów zarówno dla organizacji, jak i szkolonych pracowników.

Kompleksowe, systematyczne działania oznaczają, że szkolenia winny być przeprowadzane permanentnie, rozpatrując zmiany zachodzące zarówno

[2] D. Bogusz, *Kształcenie i szkolenie lotnicze pilotów wojskowych. Problemy definicyjne*, Journal of Modern Science 1/55/2024, s. 136. doi.org/10.13166/jms/184336.

[3] D. Bogusz, *Siły Powietrzne i Lotnictwo Sił Zbrojnych Rzeczypospolitej Polskiej*, Wydawnictwo LAW, Dęblin 2021, s. 13.

[4] D. Bogusz, *Polish Air Force*, Warsaw Management University, Warsaw 2024, s. 5.

[5] D. Bogusz, *Selekcja i szkolenie lotnicze pilotów wojskowych w Wielkiej Brytanii*, Lotnicza Akademia Wojskowa, Dęblin 2020, s. 11.

w otoczeniu, jak i wewnętrznej strukturze organizacji. Ponadto należy uwzględnić ewentualne modyfikacje kompetencji pracownika, które mogą wynikać z uczestnictwa we wcześniejszych szkoleniach i zdobytych doświadczeń zawodowych. Szkolenia powinny dotyczyć tych elementów kapitału ludzkiego, które są podatne na zmiany i związane są z wykonywanymi zadaniami. Z tego powodu należy skoncentrować się na rozwijaniu wiedzy, umiejętności i postaw pracowników. Wartościowym elementem zawartym w tym opisie jest również uwzględnienie potrzeb pracowników, ponieważ stworzenie możliwości rozwoju w obszarach pożądanych przyczynia się do wzrostu ich potencjału, co skutkować będzie korzystnymi implikacjami w przyszłości[6]. Aktywne uczestnictwo pracowników w procesie szkoleniowym dodatkowo generuje wzrost motywacji do pracy, co z kolei pozytywnie wpływa na ogólną efektywność.

Odnosząc się do tak określonych szkoleń, można wskazać na ich funkcje i cele w organizacji. W przeważającej liczbie przypadków głównym determinantem działań szkoleniowych jest podniesienie poziomu wiedzy i umiejętności pracowników. Generalnym celem pozostaje rozwój zawodowy, skoncentrowany na kształtowaniu kapitału ludzkiego w taki sposób, aby nałożone na pracowników obowiązki były realizowane na coraz wyższym poziomie. Paralelnie, w takim przypadku, działalność szkoleniowa jest silnie powiązana z rozwojem organizacji[7]. Takowy cel umożliwia realizację funkcji rozwojowej szkoleń. Jednakże, podniesienie poziomu wiedzy i umiejętności nie jest jedynym warunkiem, który uzasadnia podejmowanie działań w tym obszarze.

Znaczenie szkoleń w organizacji nadal rośnie, co wynika z różnych czynników, takich jak wymogi motywowania pracowników, wspieranie zaangażowania, rozwijanie współpracy zespołowej, rosnące oczekiwania odbiorców, a także postępujący rozwój koncepcji zarządzania zatrudnionymi, które uwzględniają aspekty związane z karierą zawodową, zapewnieniem przyszłości i bezpieczeństwem własnym oraz rodziny[8]. W obliczu tych wszystkich wyzwań, szkolenie pracowników ewoluuje w kierunku kluczowego obszaru

[6] U. Pauli, *Rola szkoleń pracowników w rozwoju małych i średnich przedsiębiorstw*, Uniwersytet Ekonomiczny, Kraków 2012, s. 123-124.

[7] M. Fryczyńska, M. Jabłońska-Wołoszyn, *Praktyczny przewodnik rozwoju zawodowego pracowników*, Placet, Warszawa 2008, s. 11-12.

[8] J. Urbański, *Rozwój i szkolenie w firmach, teoria i rzeczywistość*, Wydawnictwo Naukowe NOVUM, Płock 2004, s. 14.

działań, a związane z nim znaczne nakłady finansowe będą wzrastać w kolejnych latach[9].

Aldona Andrzejczak, badając przyczyny prowadzenia działań szkoleniowych w organizacjach, identyfikuje cztery główne funkcje szkoleń:

- adaptacyjną – oznacza dostosowanie wiedzy i umiejętności pracownika do wymagań danego stanowiska pracy,
- modernizacyjną – dotyczy konieczności aktualizacji kwalifikacji, które w wyniku postępu w nauce i technologii stają się przestarzałe lub wymagają odświeżenia z powodu rutyny,
- innowacyjną – oznacza tworzenie warunków sprzyjających postępowi oraz implementacji nowych rozwiązań,
- społeczną – obejmuje wzmacnianie więzi między ludźmi i rozwijanie umiejętności współpracy[10].

Warto zwrócić uwagę na dwa główne cele związane z działalnością szkoleniową. Pierwszym z tych celów jest dopasowanie kompetencji pracowników do potrzeb organizacji, natomiast drugim jest wspieranie działań innowacyjnych. Zaprezentowane wcześniej funkcje nie obejmują jednak w całości wszystkich powodów, dla których organizacje angażują się w działalność szkoleniową. Rozsądne jest rozszerzenie rozpatrywanych funkcji o dodatkowe, co pozwoli na przedstawienie pełnego zakresu oczekiwanych rezultatów z działalności szkoleniowej. Wśród zasadniczych funkcji uwzględnić należy:

- rozwojową,
- integracyjną,
- społeczną,
- motywacyjną,
- informacyjną,
- innowacyjną,
- wizerunkową[11].

Zazwyczaj funkcje i cele realizowane w ramach działalności szkoleniowej są ze sobą wzajemnie powiązane. Przykładowo, organizacja może łączyć funkcję rozwojową i integracyjną szkoleń, aby wprowadzić jednolite metody,

[9] W. Cascio, J. Boudreau, *Inwestowanie w ludzi, wpływ inicjatyw z zakresu ZZL na wyniki finansowe przedsiębiorstwa*, Oficyna Ekonomiczna Wolters Kluwer, Warszawa 2011, s. 351-352.

[10] A. Andrzejczak, *Projektowanie i realizacja szkoleń*, PWE, Warszawa 2010, s. 87-88.

[11] U. Pauli, *Rola szkoleń pracowników …*, op. cit., s. 125.

które będą stosowane w całej organizacji. Wskazanie funkcji i ustalenie głównych celów zwiększa skuteczność przeprowadzanych szkoleń, umożliwiając dokładniejsze dopasowanie zarówno do grupy szkoleniowej, jak i stosowanych metod i technik.

Realizacja szkoleń, które mają na celu osiągnięcie zamierzonych rezultatów w zakresie ustalonych funkcji, umożliwia dokładniejsze określenie, że taka działalność jest rozwojowa i przyniesie oczekiwane korzyści. Korzyści związane z wymienionymi wcześniej funkcjami obejmują:

- Zwiększenie wydajności i jakości pracy pracowników, zespołu lub organizacji (f. rozwojowa).
- Atrakcyjność dla wybitnych specjalistów poprzez dostarczenie im szansy na naukę i rozwój, poszerzenie ich zakresu kompetencji i umiejętności (f. wizerunkowa).
- Poprawa zdolności operacyjnej poprzez poszerzenie umiejętności pracowników (f. innowacyjna).
- Podniesienie poziomu zaangażowania i lojalności pracowników poprzez zachęcanie ich do przyjęcia misji organizacji oraz identyfikowania osobistych celów z celami przedsiębiorstwa (f. integracyjna).
- Wzmocnienie więzi pracowników z organizacją poprzez stworzenie możliwości dla ich samorealizacji i rozwoju (f. motywacyjna).
- Pomoc w implementacji zmian poprzez uświadomienie pracownikom powodów tych zmian oraz dostarczenie im niezbędnej wiedzy i umiejętności do skutecznego dostosowania się do nowych warunków (f. informacyjna).
- Pomoc w tworzeniu pożądanej kultury organizacyjnej, na przykład zorientowanej na nieustanne doskonalenie (f. społeczna).
- Zredukowanie wydatków związanych z procesem nauki i szkolenia [12].

W tym kontekście niezbędne jest opracowanie adekwatnego modelu organizacyjnego, według którego prowadzone będą szkolenia. Model taki powinien obejmować cele, podmioty oraz procesy, a także wskazywać na istniejące między nimi związki.

[12] M. Amstrong, *Zarządzanie zasobami ludzkimi*, Oficyna Ekonomiczna Wolters Kluwer, Kraków 2005, s. 498-499.

Czynniki determinujące efektywność szkoleń

Przyjęcie perspektywy procesowej stanowi jedno z podejść umożliwiających rozpoznanie czynników wpływających na skuteczność szkoleń prowadzonych w danej organizacji. Przeanalizowanie składników występujących na etapie wejściowym, w trakcie realizacji oraz na etapie wyjściowym szkoleń umożliwia dokładne określenie czynników determinujących skuteczność tego procesu.

Kierując się strategicznymi założeniami rozwoju pracowników, analizując modele i funkcje tego procesu, warto zwrócić uwagę na istotną rolę kształtowania odpowiedniego środowiska sprzyjającego uczeniu się w ramach organizacji, co staje się kluczowym czynnikiem wpływającym na skuteczność szkoleń. Klimat ten musi opierać się na przekonaniu, że rozwój jest kluczowym elementem osiągnięcia sukcesu organizacyjnego.

Zatrudnieni powinni zdawać sobie sprawę, że doskonalenie swoich kompetencji lub inwestowanie w swój rozwój zawodowy to stały element ich aktywności zawodowej. Dodatkowo, zrozumienie tego powinno wynikać z wewnętrznego przekonania pracowników o konieczności rozwoju, a nie być wynikiem narzucanych odgórnie nakazów i procedur.

Wypracowanie w organizacji modelu rozwoju pracowników, który integruje cele organizacji z indywidualnymi celami pracowników, stanowi kluczowy czynnik wpływający na efektywność szkoleń. Ten model nie powinien ograniczać się jedynie do rozwiązywania aktualnych problemów w funkcjonowaniu organizacji lub pracowników na ich stanowiskach. Raczej powinien stworzyć możliwość budowania potencjału na przyszłość.

Podsumowując, na początkowym etapie ważne jest, aby organizacja podejmowała działania wspierające proces uczenia się, które uwzględniać mogą:

- motywacyjne inicjatywy, akcentujące znaczenie kompetencji i stałego procesu nauki,
- konsultacyjne działania, skierowane na ukierunkowanie działań rozwojowych pracowników i wspieranie inicjatyw zgodnych z kierunkiem rozwoju organizacji[13].

[13] A. Andrzejczak, *Od szkolenia do organizacyjnego uczenia się*, [w:] *Zarządzanie zasobami ludzkimi w warunkach nowej gospodarki*, red. A. Pocztowski, Z.Wiśniewski, Oficyna Ekonomiczna, Kraków 2004, s. 182-183.

W trakcie realizacji działań szkoleniowych niezwykle istotne staje się precyzyjne i profesjonalne prowadzenie następujących etapów tego procesu zgodnie ze standardami i dostępną wiedzą. Wśród kluczowych komponentów, które będą miały wpływ na skuteczność, zalicza się: prawidłowe zrealizowanie analizy i identyfikacji potrzeb szkoleniowych, precyzyjne sformułowanie celów szkoleniowych, idealnie w formie spodziewanych rezultatów dotyczących rozszerzania wiedzy, rozwinięcia umiejętności i ewolucji postaw, przystosowanie metod i technik szkoleniowych do założonych celów, właściwa selekcja uczestniczących w szkoleniu, zagwarantowanie odpowiednich instruktorów prowadzących szkolenie, zaplanowanie oraz zrealizowanie ewaluacji skuteczności szkoleń. Ocena skuteczności szkoleń jest kluczowa z perspektywy planowania przyszłych szkoleń, umożliwiając także zrozumienie, jakie postępy zanotowali pracownicy i jakich kompetencji można od nich oczekiwać[14].

W kontekście podejścia procesowego, istotnym elementem na ostatnim etapie jest umożliwienie uczestnikom szkoleń praktycznego zastosowania pozyskanej wiedzy i umiejętności w miejscu pracy, a także ułatwianie adaptacji do zmienionych standardów działania.

Istotną funkcję pełni w tym kontekście bezpośrednio nadzorujący, który regularnie monitoruje postępy i zmiany w zachowaniu pracownika. Wsparciem dla praktycznego zastosowania pozyskanej wiedzy na stanowisku pracy może być związanie systemu premiowania i wynagradzania z poprawą skuteczności lub wdrożenie modelu zarządzania przez cele. Dzięki temu pracownik uczestniczący w szkoleniu będzie bardziej skłonny dostrzec pozytywną zmianę w swoich wynikach[15].

Podjęcie inicjatyw mających na celu wyeliminowanie potencjalnie szkodliwego wpływu zidentyfikowanych czynników jest kluczowe dla zapewnienia skuteczności szkoleń. W oparciu o wyniki przeprowadzonych badań wśród europejskich organizacji odnaleziono szczególnie często występujące przeszkody w zakresie przeprowadzania szkoleń. Obejmują one:

- ograniczenia czasowe (54%),
- niedostateczne środki finansowe (30%),
- niedostatek właściwych szkoleń (13%),
- brak skonkretyzowanych planów i harmonogramów (18%),

[14] U. Pauli, *Rola szkoleń pracowników …*, op. cit., s. 129.

[15] Ibidem.

- niedostateczne zaangażowanie kierownictwa (13%),
- zaniechanie szkoleń (8%),
- niewłaściwa motywacja szkolonych (8%),
- brak świadomości dotyczącej dostępnych opcji i rodzajów szkoleń (7%),
- brak odpowiednich szkoleń w bliskiej okolicy (7%),
- niewystarczająca pomoc oraz kierowanie w tych działaniach (4%)[16].

Z połowy wymienionych czynników wynikać może konieczność działań ze strony zarządzających, szczególnie na etapie tworzenia modelu rozwoju zatrudnionych i kształtowania właściwej atmosfery wspomagającej proces uczenia się.

Wśród czynników, które wpływają na skuteczność szkoleń, zidentyfikowanych w kolejnym etapie, można uwzględnić brak skonkretyzowanych planów i harmonogramów, niedostatek właściwych szkoleń oraz zaniechanie szkoleń. Wskazuje to na nieodpowiednio zrealizowany proces identyfikacji potencjalnych obszarów rozwojowych oraz braki w uwzględnianiu tych obszarów w założeniach szkoleniowych.

W odniesieniu do końcowego etapu można zasygnalizować: niedostateczne zaangażowanie kierownictwa oraz niewystarczającą pomoc oraz kierowanie w tych działaniach. Przytaczanie takich przekonań przez zarządzających nie sprzyja zaangażowaniu personelu w rozwijanie swoich kompetencji oraz wprowadzanie zmian w utrwalonych praktykach w miejscu pracy[17].

Powodami, dla których organizacje nie angażują się w tak dużym stopniu w opracowanie i realizowanie szkoleń dla pracowników mogą być:

- niewystarczające środki na szkolenie,
- brak sprecyzowania długofalowej ścieżki kariery pracowników, co wynika często z małej liczby poziomów zarządzania,
- obawy przed problemami w operacyjnej działalności organizacji, w sytuacji, wysłania pracownika (pracowników) na szkolenia,
- niechęć do inwestowania w pracowników ze względu na dużą rotację i obawę, że uczestnik szkolenia może w każdej chwili przejść do konkurencji[18].

[16] I. Isusi, *Competence development in SMEs – report*, Observatory of European SMEs no 1 2003, European commision, 2003, s. 35.

[17] U. Pauli, *Rola szkoleń pracowników ...*, op. cit., s. 130.

[18] M. Szczepaniec, T. Jurkiewicz, *Kapitał ludzki i jego akumulacja w MŚP*, Polityka Społeczna, nr 8, 2009, s. 19.

Czynniki te, choć obiektywne, nie oddają w pełni istoty problemu. Wydaje się bowiem, że głównym powodem zbyt niskiego zaangażowania organizacji w działalność szkoleniową jest, wspomniane wcześniej, niedostrzeganie pozytywnej zależności między szkoleniami, a efektywnością organizacji[19].

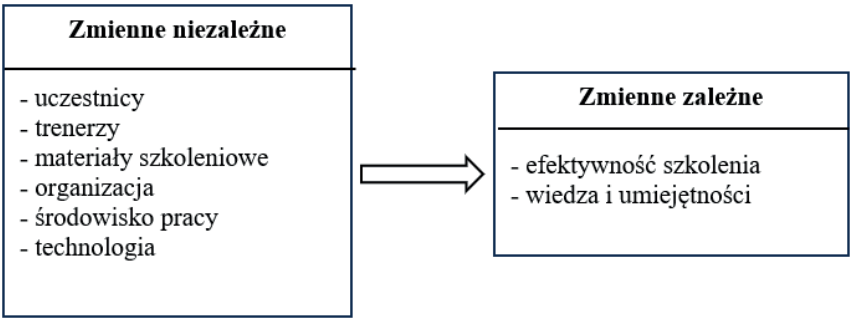
Badania sondażowe

W trakcie badania zastosowano podejście ilościowe, które obejmowało rozpowszechnienie kwestionariuszy wśród uczestników, a także przeprowadzenie wywiadów z wybranymi osobami (ekspertami), takimi jak personel kierujący obsługami samolotów. Dobór uczestników opierał się na ich zdolności do udzielania odpowiedzi i oceniania pytań postawionych przez badacza. Zadaniem tego podejścia jest dodatkowe wsparcie oraz weryfikacja danych uzyskanych z kwestionariusza.

Efektywność i osiągnięcia przeszkolonego personelu zostały ocenione na podstawie danych zebranych od personelu SIL bazy szkolenia lotniczego. Na potrzeby badania kwestionariusze ankiety rozdano personelowi SIL obsługującemu samoloty M-346. Badanie trwało około miesiąca. Respondenci mieli wystarczająco dużo czasu na udzielenie odpowiedzi na pytania zawarte w ankiecie.

Ramy badania przedstawiono na rysunku 1. Ilustruje on związek pomiędzy zmiennymi niezależnymi a zmiennymi zależnymi. W związku z tym, efektywność szkolenia oraz wiedza i umiejętności są zmiennymi zależnymi. Zmiennymi niezależnymi są uczestnicy, trenerzy, materiały treningowe, organizacja, środowisko pracy, technologie. Zmienne niezależne, decydujące o sukcesie szkolenia, to czynniki, które mają wpływ na efektywność treningu. Zebrane dane stanowią podstawę analizy różnych poziomów efektywności szkolenia.

[19] U. Pauli, *Rola szkoleń pracowników …*, op. cit., s. 131.



Rysunek 1. Ramy przeprowadzonego badania
Źródło: opracowanie własne.

Realizacja obsług i kierowanie personelem to newralgiczne obszary zadań. Personel SIL samolotów szkolno-treningowych ma gwarantować jakość wykonywanych obsług oraz ponosić za nie pełną odpowiedzialność[20]. Aspekt ten był poruszany przez personel o różnym doświadczeniu. Respondenci udzielili odpowiedzi na pytanie o elementy, które wpływają na przygotowanie do realizowania czynności obsługowych samolotów.

Opinie respondentów dotyczące małego zainteresowania personelu problematyką odbywania szkolenia były podzielone. Jednak większość ankietowanych wskazała, że personel jest zainteresowany tematyką szkolenia (tabela 1). Personel SIL, w przedziale wieku 11-20 lat, w zdecydowanej większości nie traktuje tego czynnika jako zagrażającemu efektywności szkolenia.

Tabela 1. Małe zainteresowanie personelu problematyką odbywanego szkolenia

	W bardzo małym stopniu	W małym stopniu	W średnim stopniu	W dużym stopniu	W bardzo dużym stopniu
Poniżej 5 lat	6,3%	6,3%	6,3%	3,9%	0,8%
5-10 lat	1,6%	7,9%	5,5%	3,1%	0,8%
11-20 lat	7,1%	11,0%	22,0%	6,3%	1,6%
Powyżej 20 lat	0,0%	3,1%	3,9%	2,4%	0,0%

Źródło: opracowanie własne.

[20] Zob. M. Sztobryn, *Realizacja procesu eksploatacji samolotów w bazie szkolenia lotniczego. Wybrane aspekty bezpieczeństwa*, LAW, Dęblin, 2024.

Okazuje się również, że ponad 30% badanych zauważa problem złej organizacji szkolenia. To oznacza, że część najbardziej doświadczonego personelu odczuwa wpływ organizacji szkolenia na jego skuteczność. Takowe postępowanie może prowadzić do nieświadomego łamania obowiązujących procedur w czasie pracy na sprzęcie lotniczym (tabela 2).

Tabela 2. Zła organizacja szkolenia

	W bardzo małym stopniu	W małym stopniu	W średnim stopniu	W dużym stopniu	W bardzo dużym stopniu
Poniżej 5 lat	5,6%	4,8%	7,1%	4,0%	2,4%
5-10 lat	0,0%	4,8%	10,3%	2,4%	1,6%
11-20 lat	1,6%	11,9%	15,9%	13,5%	4,0%
Powyżej 20 lat	0,0%	1,6%	3,2%	4,0%	1,6%

Źródło: opracowanie własne.

W przeprowadzonych badaniach respondenci mieli możliwość oceny wpływu trafności implementowanych treści na efektywność szkolenia (tabela 3). Analiza pozwoliła na dostrzeżenie pewnych prawidłowości. Część personelu (ok. 30%) zauważa problem z przekazywanymi treściami w czasie szkolenia. Należy przy tym zauważyć, że konieczność realizacji programu związanego z częścią teoretyczną nie zawsze jest wykorzystywana w praktycznym procesie obsługi samolotów M-346[21].

Tabela 3. Mała przydatność poszczególnych treści szkolenia w przyszłej pracy

	W bardzo małym stopniu	W małym stopniu	W średnim stopniu	W dużym stopniu	W bardzo dużym stopniu
Poniżej 5 lat	4,7%	2,4%	10,2%	4,7%	1,6%
5-10 lat	0,0%	2,4%	13,4%	1,6%	1,6%
11-20 lat	3,9%	10,2%	15,0%	16,5%	1,6%
Powyżej 20 lat	0,0%	3,1%	3,9%	1,6%	1,6%

Źródło: opracowanie własne.

Tabela 4 przedstawia skalę występowania negatywnego wpływu braku odpowiednich materiałów szkoleniowych w trakcie realizowanego szkolenia,

[21] Zob. M. Sztobryn, An*aliza przygotowania personelu SIL do obsługi samolotów M-346. Wybrane aspekty bezpieczeństwa,* Scientific Journal of Safety and Logistics, Warszawa 2023.

w opinii personelu o różnym stażu zatrudnienia. Jak zauważono, największy odsetek personelu SIL waha się w opiniach (ok. 40%). Odsetek najmłodszego personelu zauważa ten problem (7,9%). Warto podkreślić, że wymagane jest stosowanie odpowiednich materiałów szkoleniowych, umożliwiających stosowanie wyszukanych i nowatorskich rozwiązań dydaktycznych, które pozwolą na optymalne przygotowanie słuchaczy.

Tabela 4. Brak odpowiednich materiałów szkoleniowych

	W bardzo małym stopniu	**W małym stopniu**	**W średnim stopniu**	**W dużym stopniu**	**W bardzo dużym stopniu**
Poniżej 5 lat	4,8%	3,2%	7,9%	7,1%	0,8%
5-10 lat	0,0%	3,2%	11,1%	4,0%	0,8%
11-20 lat	3,2%	4,0%	19,0%	13,5%	7,1%
Powyżej 20 lat	0,0%	1,6%	2,4%	4,8%	1,6%

Źródło: opracowanie własne.

Badani również oceniali potencjalny wpływ zbyt pobieżnego traktowania problematyki szkolenia przez kadrę dydaktyczną na efektywność szkolenia (tabela 5). Z deklaracji badanych wynika, że takowy dystraktor może występować w trakcie szkolenia. Odsetek badanych, o średnim stażu zauważa ten problem (19,5%). Zwrócono uwagę na fakt, że kadra dydaktyczna bezwzględnie musi mieć autorytet i merytoryczne i metodyczne przygotowanie, gwarantujące osiągnięcie zamierzonych celów szkolenia. Instruktor musi pełnić rolę koordynatora, z uwagi na ponadprzeciętny zasób wiedzy, umiejętności i doświadczenia. Powinien posiadać również dobre przygotowanie pedagogiczne i psychologiczne. Z innej strony, cechy charakterystyczne szkoleniowców będą miały wpływ na efektywność szkolenia. Przeprowadzone badanie wykazuje, że pełnią kluczową rolę w tworzeniu i przeprowadzeniu interesujących zajęć. Wszystko to wynika z faktu, że kultura szkoleniowa wciąż wymaga, aby trener aktywnie wspierał środowisko szkoleniowe, w przeciwnym razie szkolenie nie będzie przynosić oczekiwanych rezultatów

Tabela 5. Zbyt pobieżne traktowanie problematyki szkolenia przez kadrę dydaktyczną

	W bardzo małym stopniu	W małym stopniu	W średnim stopniu	W dużym stopniu	W bardzo dużym stopniu
Poniżej 5 lat	5,5%	6,3%	6,3%	4,7%	0,8%
5-10 lat	0,0%	6,3%	7,8%	3,9%	1,6%
11-20 lat	3,1%	11,7%	12,5%	17,2%	2,3%
Powyżej 20 lat	0,8%	2,3%	3,9%	1,6%	1,6%

Źródło: opracowanie własne.

Jak można zauważyć, oceny badanych na temat zbyt obszernego i niedostosowanego do poziomu słuchaczy programu szkolenia różnią się od siebie w zależności od doświadczenia zawodowego personelu (tabela 6). Największy odsetek badanych waha się w ocenie (ok. 40%).

Tabela 6. Zbyt obszerny i niedostosowany do poziomu słuchaczy program szkolenia

	W bardzo małym stopniu	W małym stopniu	W średnim stopniu	W dużym stopniu	W bardzo dużym stopniu
Poniżej 5 lat	2,3%	2,3%	8,5%	7,8%	2,3%
5-10 lat	0,8%	5,4%	10,9%	0,8%	1,6%
11-20 lat	3,9%	6,2%	21,7%	11,6%	3,9%
Powyżej 20 lat	1,6%	2,3%	2,3%	3,1%	0,8%

Źródło: opracowanie własne.

Powyższe wyniki wykazały, że nie wszystkie czynniki wskazane w tym badaniu mają tożsamy wpływ na skuteczność treningu. Warto zaznaczyć, że w trakcie szkolenia wszyscy uczestnicy są zobowiązani do realizacji jednolitego programu szkoleniowego, co może ograniczać zdolność do krytycznego myślenia, szczególnie istotnego w obszarze obsługi nowej floty samolotów szkolno-treningowych. Można wysunąć tezę, że obecna struktura szkolenia w SIL skoncentrowana jest na ogólnych korzyściach, co prowadzi do pominięcia indywidualnych predyspozycji każdego szkolonego uczestnika. Jednocześnie eksperci zauważają, że w szkoleniu widoczne są pewne braki, również w przypadku istotnych specjalności. Kluczowy wpływ na ocenę gotowości personelu do samodzielnego wykonywania zadań obsługowych mają dowódcy w poszczególnych specjalnościach. Absolwentom Szkoły Podoficerskiej Sił

Powietrznych (SPSP) oferuje się stanowiska początkowe, a zdobycie pożądanego doświadczenia zajmuje kilka lat praktyki.

Podsumowanie

Skuteczność procesu szkoleniowego jest uzależniona od odpowiedniego scalenia wszystkich podejmowanych działań, z uwagi na zróżnicowane funkcje i różnorodność celów przypisanych tej działalności. Z tego powodu tak istotne jest, by działania szkoleniowe realizowane były w sposób profesjonalny, gdyż wówczas możliwe będzie osiąganie założonych celów.

Reasumując, przedstawione wyniki badań wykazały, że najmniejszy wpływ na efektywność szkolenia personelu SIL ma motywacja personelu, podczas gdy największe, to braki w materiałach szkoleniowych i praktycznym zastosowaniu teorii. Badani zaznaczyli, że najbardziej niekorzystny wpływ mają niewielkie ilości zajęć praktycznych realizowanych na samolocie i ograniczona użyteczność narzuconych treści programowych. Wskazano także brak dostępu do odpowiednich środków szkoleniowych, które umożliwiłyby rozwijanie kompetencji w obszarze konstrukcji i obsługi samolotów. Elementy ocenione jako średnio problematyczne to organizacja szkolenia, pobieżne podejście kadry dydaktycznej oraz zbyt obszerny program szkoleniowy. Z tego wynika, że warto zwrócić uwagę na czynniki zewnętrzne w procesie szkolenia, a nie tylko wewnętrzną motywację personelu technicznego. Jednocześnie wyniki tego badania wykazały, że wszystkie omówione czynniki mają wpływ na rezultaty szkoleń i ich efektywność. Ogólny wynik jest pozytywny, co oznacza, że te czynniki są niezwykle ważne dla skuteczności szkolenia. Zapewnia również odpowiedź dla kierownictwa organizacji, aby upewnić się, że wszystkie czynniki zostały uwzględnione, aby można było przygotować odpowiedni plan działań podjętych w celu poprawy efektywności szkolenia.

Tym samym można stwierdzić, że cel tego rozdziału został spełniony. Udało się zidentyfikować funkcje, cele i czynniki determinujące działalność szkoleniową, które są konieczne do realizacji zadań związanych z obsługą nowoczesnych samolotów. Wyniki badań pozwalają na stwierdzenie, że sukces bazy lotniczej w znacznym stopniu zależy od skutecznych działań szkoleniowych dedykowanych personelowi SIL. Pragnę równocześnie zaznaczyć, że zagadnienie to ma tak duże znaczenie, że warto monitorować postępy w tej dziedzinie.

Literatura

1. Amstrong M., *Zarządzanie zasobami ludzkimi*, Oficyna ekonomiczna a Wolters Kluwer, Kraków 2005.
2. Andrzejczak A., *Od szkolenia do organizacyjnego uczenia się*, [w:] A. Pocztowski, Z. Wiśniewski (red.), Zarządzanie zasobami ludzkimi w warunkach nowej gospodarki, Oficyna Ekonomiczna, Kraków 2004.
3. Andrzejczak A., *Projektowanie i realizacja szkoleń*, PWE, Warszawa 2010.
4. Bogusz, D. A., *Aviation education and training. Definition problems*. Journal of Modern Science, 55(1), 118-137, 2024. https://doi.org/10.13166/jms/184336
5. Bogusz D., *Polish Air Force*, Warsaw Management University, Warsaw 2024.
6. Bogusz D., *Selekcja i szkolenie lotnicze pilotów wojskowych w Wielkiej Brytanii*, Lotnicza Akademia Wojskowa, Dęblin 2020.
7. Bogusz D., *Siły Powietrzne i Lotnictwo Sił Zbrojnych Rzeczypospolitej Polskiej*, Wydawnictwo Lotniczej Akademii Wojskowej, Dęblin 2021.
8. Cascio W., Boudreau J., *Inwestowanie w ludzi, wpływ inicjatyw z zakresu ZZL na wyniki finansowe przedsiębiorstwa*, Oficyna a Wolter Kluwer Business, Warszawa 2011.
9. Fryczyńska M., Jabłońska-Wołoszyn M., *Praktyczny przewodnik rozwoju zawodowego pracowników*, Placet, Warszawa 2008.
10. Isusi I., *Competence development in SMEs – report*, Observatory of European SMEs no 1 2003, European commision, 2003.
11. Morton L., *Integrated and integative talent management: A strategic HR framework*., The Conference Board, New York 2004.
12. Pauli U., *Rola szkoleń pracowników w rozwoju małych i średnich przedsiębiorstw*, Uniwersytet Ekonomiczny, Kraków 2012.
13. Szczepaniec M., T. Jurkiewicz, *Kapitał ludzki i jego akumulacja w MŚP*, Polityka Społeczna nr 8, 2009.
14. Sztobryn M., An*aliza przygotowania personelu SIL do obsługi samolotów M-346. Wybrane aspekty bezpieczeństwa,* Scientific Journal of Safety and Logistics, Warszawa 2023.
15. Sztobryn M., *Realizacja procesu eksploatacji samolotów w bazie szkolenia lotniczego*. *Wybrane aspekty bezpieczeństwa*, LAW, Dęblin, 2024.
16. Urbański J., *Rozwój i szkolenie w firmach, teoria i rzeczywistość*, Wydawnictwo Naukowe NOVUM, Płock 2004.

mgr Stanisław Brzozowski
Wojskowa Akademia Techniczna
ORCID: 0009-0002-3320-9903

mgr Emanuel Sosnowski
Wojskowa Akademia Techniczna
ORCID: 0009-0009-4141-9493

mgr Wojciech Bobak
ORCID: 0009-0002-1125-0948

mgr Zuzanna Jordan
ORCID: 0009-0009-2636-8501

https://doi.org/10.29316/9788368103205_17

DRONY W SYSTEMIE BEZPIECZEŃSTWA

DRONES IN THE SECURITY SYSTEM

Streszczenie

Głównym celem rozdziału jest wskazanie funkcjonalności dronów przydatnych w zachowaniu prawidłowego poziomu bezpieczeństwa państwa, zwłaszcza w kontekście rosnących zagrożeń, jakie niesie ze sobą wojna w Ukrainie i dynamicznie zmieniające się środowisko bezpieczeństwa międzynarodowego. Współczesne systemy bezpieczeństwa wymagają szybkiej adaptacji do nowych wyzwań, a ciągła modernizacja bezzałogowych statków powietrznych oraz dostosowywanie ich funkcjonalności do aktualnych zagrożeń powinny być jednym z priorytetów polityki bezpieczeństwa. Drony, dzięki swojej konstrukcji i wszechstronności,

Summary

The main objective of the chapter is to indicate the functionality of drones useful in maintaining the correct level of national security, especially in the context of the growing threats posed by the war in Ukraine and the dynamically changing international security environment. Modern safety systems require quick adaptation to new challenges, and continuous modernization of unmanned aerial vehicles and adapting their functionality to current threats should be one of the priorities of security policy. Drones, thanks to their design and versatility, can play a key role in the implementation of tasks in the field of monitoring, prevention,

mogą odgrywać kluczową rolę w realizacji zadań z zakresu monitoringu, prewencji oraz reagowania na zagrożenia. Ich obecność w przestrzeni operacyjnej pozwala na bardziej efektywne wykorzystanie zasobów, lepsze rozpoznanie sytuacyjne oraz zwiększenie zasięgu i precyzji działań zarówno w czasie pokoju, jak i w sytuacjach kryzysowych. W kontekście powyższego postawiono problem badawczy: w jakim zakresie bezzałogowe statki powietrzne zwiększają efektywność funkcjonowania systemu bezpieczeństwa państwa? Przyjęta hipoteza badawcza zakłada, że wykorzystanie dronów znacząco zwiększa skuteczność działań podejmowanych w ramach systemu bezpieczeństwa poprzez poprawę zdolności do wykrywania, monitorowania i neutralizacji zagrożeń. W ramach opracowania zastosowano metody teoretyczne, takie jak analiza literatury przedmiotu, analiza funkcjonalna oraz podejście systemowe. W rozdziale odniesiono się także do wybranych przypadków operacyjnego wykorzystania dronów w działaniach wojskowych i cywilnych, co pozwoliło na weryfikację hipotezy w kontekście realnych zastosowań.

Słowa kluczowe: bezzałogowe statki powietrzne, system bezpieczeństwa państwa, drony, monitorowanie zagrożeń, bezpieczeństwo narodowe

and response to threats. Their presence in the operational space allows for more efficient use of resources, better situational reconnaissance, and increased range and precision of operations both in peacetime and in crisis situations. In the context of the above, a research problem was posed: to what extent do unmanned aerial vehicles increase the effectiveness of the functioning of the state security system? The adopted research hypothesis assumes that the use of drones significantly increases the effectiveness of activities undertaken as part of the security system by improving the ability to detect, monitor and neutralize threats. The study used theoretical methods such as literature analysis, functional analysis, and a systems approach. The paper also refers to selected cases of operational use of drones in military and civilian operations, which allowed to verify the hypothesis in the context of real applications.

Keywords: unmanned aerial vehicles, state security system, drones, threat monitoring, national security

Wstęp

W obliczu dynamicznie zmieniających się zagrożeń drony pełnią różne funkcje i zadania, zarówno w sferze cywilnej, jak i militarnej. Ich coraz częstsze użycie spowodowane jest zmianą zagrożeń, które są niezwykle niebezpieczne dla całości społeczeństwa. Samo ich użycie spowodowane jest dużymi możliwościami rozpoznawczymi i monitorującymi. Drony coraz częściej wyposażone są w specjalistyczne kamery lub inne elementy służące np. do dokonywania zrzutów lub transportu. Systemy bezzałogowe stają się potęgą nie tylko na polu walki

czy w trakcie realizacji określonej akcji poszukiwawczej, lecz również na rynku cywilnym w czynnościach takich jak: fotografia, pomiary lub inspekcje. Technika pilotowania bezzałogowym statkiem powietrznym (BSP) nie jest trudna, a z pewnością jest łatwiejsza niż np. samolotem czy śmigłowcem. Brak wymaganych badań lekarskich wśród pilotów dronów powoduje również ich większą popularność i dostępność. Duże kompleksy leśne czy tereny bagniste są często utrudnieniem dla ludzi, którzy chcą w tym obszarze wykonać określone zadania.

Możliwość penetracji terenu przez drony daje ogromne możliwości wizualne. Właściwe zobrazowanie terenów niedostępnych pozwala na przewidywanie i określanie potrzeb sprzętów oraz ludzi. Dynamika prowadzenia akcji poszukiwawczych czy ratowniczych powoduje zmiany w podejmowaniu decyzji przez prowadzącego czy kierującego daną akcją – dowódcę. Wykonywanie lotów dronem w zasięgu wzroku lub poza zasięgiem wzroku pozwala na monitorowanie określonych obiektów czy zdarzeń i tym samym przekazywanie informacji do określonego stanowiska dowodzenia. Warto zaznaczyć, że jednocześnie w powietrzu może latać kilka dronów, które mogą być kompatybilne. Często drony wykorzystywane są prewencyjnie przez instytucje i służą jako atrapa kamery, której zadaniem jest odstraszanie potencjalnego przestępcy czy napastnika. Służby oraz instytucje państwowe wykorzystują drony do konkretnych celów. Coraz to lepsze parametry, takie jak długotrwałość lotu, prędkość czy odporność na określone warunki atmosferyczne podnosi ich atrakcyjność.

Drony na stałe umiejscowiły się już w strukturach służb i wzmacniają system bezpieczeństwa. Drony powinny być modyfikowane i zastępowane innymi technologiami, które są skuteczne do zwalczania realnych zagrożeń. Warto też wspomnieć o dronach, które są wykorzystywane przez grupy przestępcze i stanowią ogromne zagrożenie dla bezpieczeństwa.

Istota bezpieczeństwa

Współczesne i prognozowane zagrożenia uświadamiają wszystkim, że ważnym elementem jest współdziałanie. Dlatego służby i instytucje państwowe muszą współpracować i wzajemnie się wspomagać[1]. Jak uważa L. Elak wybuch konfliktu ukraińsko-rosyjskiego w 2014 r. uświadomił, że

[1] B. Kaczmarczyk, *Racjonalizacja procesów zarządzania kryzysowego Straży Granicznej*, Wyższa Szkoła Policji, Szczytno 2012, s. 73.

bezpieczeństwo zarówno Polski, jak i Unii Europejskiej, powinno być zwiększone[2]. Podobna sytuacja jest obecnie, kiedy to trwa konflikt zbrojny na terytorium Ukrainy. Bezpośrednie sąsiedztwo Polski z Ukrainą potęguje liczbę różnego rodzaju zagrożeń, które często występują w strefach nadgranicznych w różnych regionach i miejscach.

Same rozważania na temat bezpieczeństwa mają długą historię. Człowiek od zawsze ma swoje potrzeby i trapią go różnego rodzaju strachy wewnętrzne (psychologiczne) czy zewnętrzne. Społeczeństwo zawsze stawało w obliczu zagrożeń naturalnych i duchowych[3]. System bezpieczeństwa to całość sił i środków przeznaczonych przez państwa do realizacji zadań w obszarze bezpieczeństwa. Celem systemu bezpieczeństwa jest przeciwdziałanie wszelkiego rodzaju zagrożeniom państwa. Na system bezpieczeństwa składają się struktury i urządzenia oraz wydzieleni ludzie, odpowiedzialni za bezpieczeństwo[4]. Współczesna cywilizacja jest pełna zagrożeń. Człowiek intensywnie doświadcza nowych problemów przez otaczający świat. Poczucie bezpieczeństwa personalnego jest wartością, stanem najsilniej oczekiwanym, pożądanym, a jego znaczenie wzrasta w dynamicznie zmieniającym się społeczeństwie ponowoczesnym[5]. Jak twierdzi A. Szczepański bezpieczeństwo jest kategorią złożoną i wieloaspektową. Jest ono interpretowane jako stan związany z brakiem zagrożeń. Jednak bywa charakteryzowane w aspekcie pozytywnym (poczucia pewności, ochrony) lub negatywnym (niewystępowania niebezpieczeństw), a także w ujęciu obiektywnym (np. dotyczącym statusu materialnego jednostek) bądź subiektywnym (świadomościowym)[6].

Samo pojęcie bezpieczeństwa jest ważną kwestią wśród społeczeństwa. Każdy obywatel powinien czuć się bezpiecznie. Zachwianie pewnych elementów bezpieczeństwa powoduje lęk i obawy. Niestety często zagrożenie pojawiają się nagle i są całkowicie nowym doświadczeniem dla służb czy

---

[2] L. Elak, *Ochrona granicy państwowej. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2017, s. 8.

[3] A. Wawrzusiszyn, *Wybrane problemy transgranicznego bezpieczeństwa Polski*, Difin, Warszawa 2012, s. 14-15.

[4] A. Bilski, K. Kowalczyk, *Elementarz bezpieczeństwa pomorza zachodniego*, Nobilis Media, Szczecin 2016, s. 26.

[5] P. Wasilewski, J. Świniarski, M. Marcinkowski, *Bezpieczeństwo personalne w sytuacjach trudnych*, Akademia Wojsk Lądowych, Wrocław 2020, s. 153.

[6] A. Szczepański, *Pojęcie bezpieczeństwa i jego typologia - próba systematyzacji*, Zeszyty Naukowe Collegium Witelona, nr 48(3), 2023.

instytucji. Dlatego narzędzia oraz system szkolenia służb odpowiedzialnych za bezpieczeństwo powinien być modyfikowany i wdrażany z niezwykłą starannością. Zagrożenia militarne są niebezpieczne i towarzyszyły już nam od pokoleń. Wojna powoduje spustoszenia i zmusza państwa do podejmowania ciągłych decyzji, które stanowią często o ludzkim życiu. W chwili obecnej coraz częściej wykorzystuje się bezzałogowe statki powietrzne celem minimalizowania określonych zagrożeń.

W Strategii bezpieczeństwa narodowego RP z 2020 r. jest mowa o rozwoju nowych technologii – zarówno cywilnych, jak i wojskowych. Powyższe sprawia, że istotnie wzrasta wykorzystanie bezzałogowych i autonomicznych systemów, zautomatyzowanych i zrobotyzowanych platform uzbrojenia wykorzystujących sztuczną inteligencję, a także systemów broni precyzyjnego rażenia na dalekie odległości, w tym rakiet balistycznych i manewrujących[7]. Systemy bezzałogowe w dzisiejszej rzeczywistości wykorzystywane są do ataków nieprzyjaciela, monitoringu czy rozpoznania. Pełnią one funkcje rozpoznawania pola walki w różnych płaszczyznach. W czasie pokoju pełnią zupełnie inne zadania niż np. w czasie kryzysu czy podejmowania działań wojennych. Bardzo często wspomagają lotnictwo załogowe, które koncentruje się na bardziej skomplikowanych misjach.

Warto zaznaczyć w tym miejscu, że drony potrafią być również niebezpieczne i mogą służyć do działalności przestępczej. Dlatego należy uświadamiać społeczeństwo o pozytywnych i negatywnych cechach bezzałogowych statków powietrznych.

Systemy bezzałogowe

Historia bezzałogowych statków powietrznych sięga czasów I wojny światowej, gdzie pierwsi naukowcy próbowali testować różnego rodzaju konstrukcje BSP w postaci latawców, bomb czy innych obiektów latających, które nie posiadały pilota na pokładzie. Bezzałogowe statki powietrzne w bezpieczeństwie spełniają głównie role związane z ochroną i dozorem obiektów i miejsc, nadzorem nad ruchem drogowym, zabezpieczaniem imprez masowych, ochroną granic, wykrywaniem zagrożeń technicznych, chemicznych,

[7] Strategia Bezpieczeństwa Narodowego RP, Warszawa 2020.

środowiskowych, obroną i ofensywnym działaniem bojowym, wykrywaniem przestępstw i przestępców czy działaniami ratowniczymi[8].

Rozpatrując szczegółowo powyższe stwierdzenie w pierwszej kolejności można się skupić nad ochroną czy dozorem obiektów oraz ochroną imprez masowych. Drony ze względu na swoją manewrowość oraz niewielką wagę są w stanie dokonywać monitoringu różnych miejsc często trudnodostępnych. Obiekty kryte typu hale czy duże hangary również nie stanowią przeszkody dla lotnictwa bezzałogowego i mogą być przez nie monitorowane. Całość danej imprezy masowej np. koncert wymaga zaangażowania dużej ilości sił i środków. Często na tego typu imprezach dochodzi do różnych incydentów związanych np. z zasłabnięciem osoby czy nagłym wypadkiem. Drony mogą nie tylko monitorować, ale dostarczać na miejsce zdarzenia leki, bandaże czy inne medykamenty. Transport towarów przez drony staje się coraz bardziej popularny i jest stosunkowo tani szczególnie w obszarach miejskich. Czasami dostarczenie określonego towaru w mieście jest bardzo kosztowne i wymaga czasu ze względu chociażby na duże natężenie ruchu drogowego.

Transport przy pomocy BSP jest coraz bardziej popularny, szczególnie sprawdzają się w realizacji tzw. „last mile delivery", czyli dostaw na ostatnim odcinku trasy. Bezzałogowe statki powietrzne są w stanie szybko dostarczyć przesyłki do domów klientów, punktów odbioru czy biur, eliminując problemy związane z korkami i parkowaniem. Dzięki możliwości zawisu nad punktem czy zdolności do pionowego startu i lądowania drony są w stanie dotrzeć do trudnych sfer miejskich. Wraz z postępem technologicznym wzrasta długotrwałość wykonywanych lotów przez drony np. zwiększają się pojemności baterii oraz możliwości zastosowania sztucznej inteligencji. Przyszłość logistyki miejskiej może obejmować implementację dronów z tradycyjnymi pojazdami oraz autonomicznymi robotami dostawczymi, całość może tworzyć kompleksowe usługi transportowe[9]. Czyli drony mogą również sprawdzać się w systemie usług transportowych i wykonywać określone zadanie np. dostarczać daną paczkę w określone miejsce, gdzie jest możliwy bezpieczny zrzut towaru i możliwość podebrania go przez np. auto dostawcze lub robota autonomicznego. Podobne zadania do tej pory drony wykonują podczas akcji

[8] P. Wrzosek *Wykorzystanie dronów w zakresie bezpieczeństwa. Nowe rozwiązania z projektu FASTER*, Przegląd Policyjny, 145(1), 2022, s. 165-176.

[9] A. Kowalski, *Transport powietrzny a logistyka miejskiej dostawy dronami*, https://logistica.pl/transport-powietrzny-a-logistyka-miejskiej-dostawy-dronami/, [dostęp: 12.04.2025].

ratowniczych np. w czasie gaszenia pożaru. Drony strażackie potrafią przenosić ładunek w postaci wody i skierować ją pod dużym ciśnieniem w cel. Przekazywanie obrazu poprzez drona do jednostki gaśniczej jest również możliwe i jest niezwykle ważnym elementem. Pożar bardzo szybko się rozprzestrzenia tak, że decyzje muszą być podejmowane dynamicznie.

Bezzałogowe statki powietrzne są widoczne w armiach różnych państw. Zaczynają odgrywać coraz znaczniejszą rolę na współczesnym polu walki, w misjach zarówno rozpoznawczych, jak i uderzeniowych. BSP odnajdują się w artylerii, marynarce wojennej czy lotnictwie[10]. W Siłach Zbrojnych RP drony występują w większości jednostek wojskowych. Różne typy i modele BSP są przystosowane do odmiennych zadań. Przed zakupem drona każda służba czy instytucja państwowa powinna dokładnie przeanalizować zadania do jakich będzie on wykorzystywany.

Należy pamiętać, że każdy rodzaj drona będzie lżejszy od samolotu czy śmigłowca, co z pewnością wpłynie na jego zadaniowość. W dzisiejszej dobie drony są jednym z podstawowych narzędzi stosowanych na współczesnym polu walki. Lista zastosowań militarnych i niemilitarnych oraz możliwości misji taktycznych BSP jest bardzo obszerna. Zakres zastosowań użytkowych BSP zmienia się wraz z burzliwym rozwojem technologicznym[11]. Jak opisuje L. Cwojdziński systemy bezzałogowe mogą wykonywać zadania bojowe, takie jak: wsparcie ogniowe, rozpoznanie radiometryczne, umiejscawianie przeszkód czy wsparcie operacji specjalnych[12].

Zastosowanie bezzałogowych statków powietrznych w kontekście bezpieczeństwa jest bardzo obszerne. Samo zastosowanie dronów militarnych do potrzeb wojska realizowane jest w wielu obszarach. Wojska Obrony Terytorialnej wykonują zadania z użyciem BSP, zarówno w bezpośredniej ochronie granicy państwowej, jak i w wewnątrz kraju. Sytuacje kryzysowe w Polsce pokazały, jak drony się sprawdzają i w jaki sposób podejmują działania. Pandemia COVID-19 dużo nauczyła społeczeństwa i w pewien sposób zmobilizowała do podejmowania działań naprawczych w systemie bezpieczeństwa.

[10] P. Polkowski, *Bezzałogowe statki powietrzne*, Rocznik Bezpieczeństwa Międzynarodowego, 10(1), 2019, s. 237-248.

[11] W. Leśnikowski, *Drony, bezzałogowe aparaty latające. Od starożytności do współczesności*, Wydawnictwo Adam Marszałek, Toruń 2016, s. 105-110.

[12] L. Cwojdziński, *Przyszłość dla systemów bezzałogowych?* Przegląd Sił Powietrznych, nr 1(061), 2013, s. 11-13.

Wynikało to z ogromnego chaosu jaki zapanował wśród społeczeństwa. Nieprzestrzeganie procedur przez społeczeństwo powodowało tylko zwiększanie zagrożenia. W tym wypadku zagrożeniem był wirus czy choroba, która bardzo szybko się rozprzestrzeniała. Wprowadzone przez aparat państwa procedury bezpieczeństwa miały na celu zminimalizowanie ryzyka zagrożenia. Pandemia była wszechobecna – dotknęła cały świat. Obserwując działania zaradcze niektórych państw, w tym Polski, można stwierdzić, że drony w pewnym stopniu przyczyniły się do zwalczania pewnych zagrożeń, w tym wypadku związanych z pandemią. Czynności takie jak: informowanie, odkażanie, transportowanie czy dokonywanie inspekcji obiektów, były realizowane w tamtym czasie przez drony. System bezzałogowy w czasie pandemii wykonywał szereg zadań, które miały na celu m.in. zachowanie prawidłowego bezpieczeństwa wewnętrznego.

W chwili obecnej w trakcie toczącej się wojny w Ukrainie lotnictwo bezzałogowe pełni rolę militarną. Jak słusznie opisuje A. Kwiatkowski bezpieczeństwo Polski z uwagi na sytuację w Ukrainie jest mocno zagrożone. Należy spodziewać się rozprzestrzenienia się konfliktu zbrojnego. Rosja realizuje agresywną politykę, wykorzystując siłę militarną w celu wywierania presji. Autor uważa, że Polska podjęła wysiłki na rzecz wzmacniania potencjału wojskowego. Sukcesywne zwiększanie nakładów na polską armię poprawia bezpieczeństwo Polski i jej sojuszników, zwiększając ich ochronę przed agresją Rosji[13].

Polska w dalszym ciągu musi rozwijać swoje wojska bezpośrednio przy granicy polsko-białoruskiej. Siły Zbrojne RP powinny w dalszym ciągu wspomagać działalność Straży Granicznej. Wspólne patrole, jak i wspólne szkolenia pomiędzy Siłami Zbrojnymi a Strażą Graniczną, powinny być kontynuowane. Warto zauważyć, że w chwili obecnej monitoring granicy państwowej odbywa się przy pomocy bezzałogowych statków powietrznych.

Maciej Konieczny stwierdza, że utrzymanie bezpieczeństwa na odpowiednim poziomie w państwie jest jedną z najważniejszych wartości, do której dążą władze każdego państwa. Każde państwo posiada swoje wyspecjalizowane jednostki do wykrywania i prewencji zagrożeń[14]. Tymi jednostkami oczywiście są służby i instytucje, ale muszą one posiadać sprzęt i wykwalifikowaną

[13] A. Kwiatkowski, *Bezpieczeństwo Polski w świetle działań wojennych Rosji na Ukrainie*, De Securitate Et Defensione. O Bezpieczeństwie I Obronności, 9(1), 2023, s. 32-47.

[14] M. Konieczny, *Status, rola i zadania Straży Granicznej w Polsce*, Security, Economy & Law, Nr 2(XXIX), 2021, s. 28.

kadrę, która będzie w stanie przeciwstawić się danemu zagrożeniu. Jednym z narzędzi są drony, bez których ciężko sobie wyobrazić w dzisiejszych czasach efektywne prowadzenie działań.

Jak słusznie zauważają M. Adamski oraz J. Rajchel wraz z postępem technologicznym wzrastają wyzwania. Bezzałogowe statki powietrzne cały czas należy udoskonalać i unowocześniać m.in. w zakresie głowic optycznych, przesyłania obrazu z możliwością natychmiastowego jego przetwarzania oraz zdolności do precyzyjnego i wiarygodnego określania celu. Ważnym elementem jest też ciągłe rozwijanie źródeł zasilania BSP oraz zmniejszenie jego energochłonności[15].

W Strategii Bezpieczeństwa Narodowego RP z 2020 r. mowa jest o budowaniu narodowego, zintegrowanego systemu świadomości sytuacyjnej, opartego na różnych rodzajach środków rozpoznania, łączności, dowodzenia, w tym krajowych systemach satelitarnej obserwacji Ziemi i systemach bezzałogowych statków powietrznych działających w strukturach sieciocentrycznych, przy zachowaniu pełnego bezpieczeństwa kryptograficznego[16]. W samej strategii jest mowa o systemach bezzałogowych, co podkreśla tylko ich niezawodność i skuteczność działania.

W wielu wewnętrznych aktach prawnych poszczególnych służb czy instytucji państwowych można spotkać obszar BSP. W tym miejscu należy również wspomnieć o niebezpieczeństwach jakie mogą stwarzać drony. Te latające obiekty są w stanie przemycać substancje narkotyczne, papierosy czy inne niedozwolone substancje. Częste przypadki przestępstw z użyciem BSP widoczne są na polsko – ukraińskiej granicy państwowej. Dlatego zadaniem służb jest również właściwa weryfikacja i kontrolowanie pilotów BSP, którzy wykonują operacje lotnicze. Oprócz przepisów krajowych w Polsce obowiązują również przepisy unijne, które nakazują określone czynności w stosunku do wykonywanych lotów BSP.

Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych[17], określa kategorie wykonywania lotów BSP. Loty

[15] M. Adamski, J. Rajchel, *Bezzałogowe statki powietrzne, Część I. Charakterystyka i wykorzystanie*, Wydawnictwo Wyższej Szkoły Oficerskiej Sił Powietrznych Dęblin 2013, s. 60-72.

[16] Strategia Bezpieczeństwa Narodowego RP z 2020 roku, Warszawa 2020.

[17] Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. – w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz.

dronami podyktowane są analizą ryzyka. Pilot BSP zmuszony jest do przestrzegania odległości np. od osób czy wysokości. Ponadto zobowiązany jest do informowania innych użytkowników przestrzeni powietrznej o danym locie i jego zakończeniu. W Polsce wykonywanie lotów dronami w niektórych miejscach jest całkowicie zabronione lub ograniczone. Dlatego poprzez specjalnie dedykowaną aplikację piloci BSP są w stanie określić przestrzeń powietrzną oraz podać swoją identyfikację.

W dobie zagrożeń należy ciągle rozwijać system bezzałogowy i opracowywać metody skutecznego zwalczania dronów będących w użyciu np. grup przestępczych czy nieprzyjaciela. Funkcjonalności BSP pozwalają na ich skuteczną implementację z lotnictwem załogowym. Mogą służyć one jako głowica bojowa, która ma za zadanie zniszczyć określony cel. Jednak w wielu przypadkach używane są do monitoringu, naprowadzania lub rozpoznania. Armie większości państwa europejskich dążą do zakupu nowych rozwiązań BSP. W Polsce drony są popularne zarówno w sektorze z militarnym, jak i cywilnym. Należy w dalszym ciągu prowadzić badania naukowe i rozpowszechniać użycie BSP zarówno w czasie pokoju, sytuacji kryzysowej, jak i działań militarnych.

Podsumowanie

Bezzałogowe statki powietrzne, popularnie zwane dronami, stały się integralnym elementem współczesnych systemów bezpieczeństwa państwa. Ich zastosowanie obejmuje zarówno działania wojskowe, jak i cywilne, od rozpoznania, monitoringu, transportu, aż po działania prewencyjne i interwencyjne. Rozdział ukazuje, jak dynamiczny rozwój technologiczny BSP – wsparty między innymi postępem w dziedzinie sztucznej inteligencji oraz miniaturyzacji systemów optycznych i energetycznych – zwiększa ich użyteczność w obszarze bezpieczeństwa. W dobie pandemii COVID-19 drony wykorzystywano do informowania społeczeństwa, dekontaminacji czy dostarczania środków ochrony, natomiast w czasie wojny w Ukrainie pełnią one istotną funkcję bojową i rozpoznawczą.

Jednocześnie podkreślono konieczność dalszego rozwoju systemów przeciwdziałania zagrożeniom związanym z wykorzystywaniem dronów do

U. UE L 152/45).

celów przestępczych, jak przemyt czy działania sabotażowe. Autorzy wskazują, że skuteczne wdrażanie BSP w struktury bezpieczeństwa państwowego wymaga nie tylko zaawansowanego sprzętu, ale także odpowiednich regulacji prawnych, kontroli przestrzeni powietrznej oraz systemów szkoleniowych dla operatorów.

Wnioski zawarte w rozdziale prowadzą do konkluzji, że bezzałogowe statki powietrzne są nieodzownym komponentem współczesnych działań bezpieczeństwa – zarówno na poziomie operacyjnym, jak i strategicznym. Ich dalsza integracja z tradycyjnymi systemami bezpieczeństwa, rozwój technologiczny i prawidłowe zarządzanie ryzykiem związanym z ich użytkowaniem, stanowią wyzwanie, które powinno być priorytetem dla struktur odpowiedzialnych za bezpieczeństwo narodowe.

Literatura

1. Adamski M., Rajchel J., B*ezzałogowe statki powietrzne, Część I. Charakterystyka i wykorzystanie*, Wyd. Wyższa Szkoła Oficerska Sił Powietrznych, Dęblin 2013.
2. Bilski A., Kowalczyk K., *Elementarz bezpieczeństwa pomorza zachodniego*, Nobilis Media, Szczecin 2016.
3. Cwojdziński L., *Przyszłość dla systemów bezzałogowych?* Przegląd Sił Powietrznych, nr 1(061), 2013.
4. Elak L., *Ochrona granicy państwowej. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2017.
5. Kaczmarczyk B., *Racjonalizacja procesów zarządzania kryzysowego Straży Granicznej*, Wyższa Szkoła Policji, Szczytno 2012.
6. Kowalski A., *Transport powietrzny a logistyka miejskiej dostawy dronami*, https://logistica.pl/transport-powietrzny-a-logistyka-miejskiej-dostawy-dronami/
7. Konieczny M., *Status, rola i zadania Straży Granicznej w Polsce*, Security, Economy & Law, Nr 2/2021 (XXIX), 2021.
8. Kwiatkowski A., *Bezpieczeństwo Polski w świetle działań wojennych Rosji na Ukrainie*, De Securitate Et Defensione. O Bezpieczeństwie I Obronności, 9(1), 2023.
9. Leśnikowski W., *Drony, bezzałogowe aparaty latające. Od starożytności do współczesności*, Wyd. Adam Marszałek, Toruń 2016.
10. Polkowski P., *Bezzałogowe statki powietrzne*, Rocznik Bezpieczeństwa Międzynarodowego, 10(1), 2019.
11. Rozporządzenie wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. - w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dz. U. UE L 152/45).
12. Szczepański A., *Pojęcie bezpieczeństwa i jego typologia - próba systematyzacji*, Zeszyty Naukowe Collegium Witelona, nr 48(3), 2023.
13. Strategia Bezpieczeństwa Narodowego RP, Warszawa 2020.

14. Wawrzusiszyn A., *Wybrane problemy transgranicznego bezpieczeństwa Polski*, Wydawnictwo Difin, Warszawa 2012.
15. Wasilewski P., Świniarski J., Marcinkowski M., *Bezpieczeństwo personalne w sytuacjach trudnych*, Akademia Wojsk Lądowych, Wrocław 2020.
16. Wrzosek P., *Wykorzystanie dronów w zakresie bezpieczeństwa. Nowe rozwiązania z projektu FASTER*, Przegląd Policyjny, 145(1), 2022.

mgr Malwina Olbrych
ORCID: 0009-0004-2613-2842

https://doi.org/10.29316/9788368103205_18

OSOBA ZARZĄDZAJĄCA TRANSPORTEM JAKO GWARANT BEZPIECZEŃSTWA W KOMUNIKACJI

TRANSPORT MANAGER AS A GUARANTOR OF SAFETY IN TRANSPORT

Streszczenie

Celem rozdziału jest ocena, czy i w jakim zakresie funkcja zarządzającego transportem – jako osoby odpowiedzialnej za dopuszczenie pojazdu i kierowcy do udziału w ruchu – ma realne znaczenie dla zapewnienia bezpieczeństwa komunikacyjnego. W pierwszej części rozdziału opisano ogólny stan bezpieczeństwa na polskich drogach oraz strukturę zagrożeń, zwracając uwagę na niedostateczne uwzględnianie technicznych aspektów pojazdów, jako źródeł wypadków. Następnie przedstawiono definicję oraz obowiązki zarządzającego transportem w świetle prawa unijnego i krajowego, uwzględniając zakres jego odpowiedzialności. W kolejnej części zaprezentowano przesłanki oceny niesprawności technicznej pojazdu w kontekście ryzyka dla uczestników ruchu. Rozdział kończy się analizą zbiegu przepisów karnych i wykroczeniowych (art. 179 k.k. i art. 96 k.w.) oraz postuluje precyzyjniejsze

Summary

The aim of the chapter is to assess whether and to what extent the function of the transport manager – as a person responsible for allowing the vehicle and the driver to participate in traffic – is of real importance for ensuring traffic safety. The first part of the chapter describes the general state of safety on Polish roads and the structure of hazards, paying attention to the insufficient consideration of technical aspects of vehicles as sources of accidents. Next, the definition and obligations of the transport manager in the light of EU and national law are presented, taking into account the scope of their responsibility. The next part presents the premises for assessing the technical malfunction of a vehicle in the context of the risk to road users. The chapter concludes with an analysis of the concurrence of criminal and misdemeanor provisions (Article 179 of the Penal Code and Article 96 of the Penal Code) and

określenie obowiązków zarządzającego w przepisach prawa. Problem badawczy sformułowano w pytaniu: Jak funkcja zarządzającego transportem wpływa na poziom bezpieczeństwa w komunikacji? Hipoteza badawcza zakłada, że zarządzający transportem ma istotne znaczenie dla stanu bezpieczeństwa w transporcie drogowym, a jego zaniechania mogą skutkować odpowiedzialnością karną na podstawie art. 179 k.k. Zastosowano metody badawcze, takie jak analizę aktów prawnych krajowych i unijnych, orzecznictwa sądowego, literatury naukowej oraz interpretacji doktrynalnej przepisów karnych i wykroczeniowych.

Słowa kluczowe: bezpieczeństwo ruchu drogowego, transport drogowy, zarządzający transportem, stan techniczny pojazdu

postulates a more precise definition of the manager's obligations in the provisions of law. The research problem was formulated in the question: How does the function of the transport manager affect the level of safety in communication? The research hypothesis assumes that the transport manager is of significant importance for the state of safety in road transport, and his omissions may result in criminal liability under Article 179 of the Penal Code.

Keywords: road safety, road transport, transport manager, technical condition of the vehicle

Wstęp

Historia ludzkości jest ściśle powiązana z przemieszczaniem się zarówno ludzi, jak i towarów. Konieczność zapewnienia coraz to nowszych dóbr, szczególnie w dobie konsumpcjonizmu, wymaga translokowania produktów użytkowych z miejsca wydobycia surowców do zakładu przetwarzającego je w wyrób i dalej do odbiorcy czy konsumenta. Również osobista działalność człowieka w sferze zawodowej i społecznej, związana jest z koniecznością ciągłego przemieszczania się. Potrzeby przemieszczania się, stały się inspiracją do tworzenia środków umożliwiających komunikację i poruszanie się w coraz efektywniejszy sposób, co w XXI wieku ma odzwierciedlenie szczególnie we wzmożonym ruchu drogowym, w którym poruszają się różni jego uczestnicy, użytkujący różnorodne, niekiedy bardzo nowoczesne pojazdy. Wyzwaniem w obecnych czasach jest zapewnienie właściwego bezpieczeństwa w ruchu drogowym dla wszystkich jego użytkowników.

Wśród czynników mających decydujący wpływ na bezpieczeństwo ruchu drogowego (człowiek – droga – pojazd, jako czynnik sprawczy wypadków), na pierwsze miejsce zdecydowanie wysuwa się człowiek. To właśnie zachowanie się poszczególnych grup użytkowników dróg generalnie wpływa

na powstawanie wypadków drogowych[1]. Czynnik technicznego stanu pojazdu najczęściej jest jedynie składową częścią przyczyny zdarzenia drogowego. Inne czynniki, w tym przede wszystkim związane ze stanem dróg, stanowią ostatni z elementów.

Truizmem jest, że nie da się całkowicie wyeliminować wypadków drogowych czy innych niebezpiecznych zdarzeń drogowych. W ruchu drogowym będą one towarzyszyły człowiekowi zawsze i będą nieodłącznie towarzyszyć rozwojowi motoryzacji. Należy jednak dążyć do zmniejszenia rozmiarów tego zjawiska, podejmując działania profilaktyczne oraz stosować środki karno-represyjne.

Stan bezpieczeństwa ruchu drogowego w Polsce

W związku z ewaluującym procesem rozwoju zagadnienia transportu drogowego powstają również problemy związane z zagrożeniem bezpieczeństwa ruchu drogowego oraz straty społeczne ponoszone w wyniku wypadków drogowych. Problem wypadków drogowych stał się jednym z najważniejszych problemów społecznych XXI wieku.

Obecnie, jak wynika z analizy dostępnych danych statystycznych, większość wypadków jest wynikiem błędów w zachowaniu człowieka, a w niewielkim stopniu jest spowodowanych złym stanem technicznym pojazdów lub warunkami drogowymi. Interpretując zjawisko wypadków drogowych w różnych krajach, można stwierdzić, że ich dynamika nie jest ściśle związana z natężeniem ruchu drogowego, a krzywe wypadków są odmienne, dlatego dokonując porównań należy zachować ostrożność, aby nie doprowadzić do błędnych wniosków. Wobec powyższego nie można ujednolicić stanowisk co do przyczyn wypadków.

Każdy kraj dysponuje środkami profilaktycznymi. W Polsce rozwinęły się multidyscyplinarne programy poprawy bezpieczeństwa w ruchu drogowym, które skupiają się wokół Krajowego Programu Bezpieczeństwa Ruchu Drogowego, wdrażanego od 2005 r[2].

Wspomniana polska doktryna poprawy bezpieczeństwa w ruchu drogowym – znana jako program „Gambit" – opiera się na analizie czynników

[1] Raport KGP „Wypadki drogowe w Polsce w 2023 roku".

[2] Krajowa Rada Bezpieczeństwa Ruchu Drogowego „Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2023".

ruchu drogowego mających istotny wpływ na stan bezpieczeństwa. Program ten opiera się na przekonaniu, że doszukując się genezy zdarzenia drogowego należy przyjąć, że dochodzi do niego wskutek zaburzenia jednego lub wielu elementów składających się na system ruchu drogowego lub relacje pomiędzy tymi elementami.

Winno się zaznaczyć, że każde zdarzenie drogowe najczęściej jest zbiegiem kilku czynników. Jednakże praktyka dochodzeniowa skupia się głównie na ocenie zachowania kierującego, bez pogłębionej analizy związków przyczynowo-skutkowych z innymi elementami zdarzenia drogowego. Problem ten zauważył już w latach 80. XX wieku A. Gaberle. Według niego fikcja bardzo dobrego stanu technicznego pojazdów w Polsce wynika z tego, że o wiele łatwiej jest ustalić, że kierowca nie przestrzegał obowiązujących przepisów, niż to, że pojazd był niesprawny przed wypadkiem lub że niewłaściwe zachowanie kierującego zostało wywołane lub wzmocnione przez niesprawność pojazdu[3]. Problem ten jest aktualny po dziś dzień, bowiem w tym kontekście zwraca uwagę bardzo duży udział procentowy nieustalonych przyczyn wypadków w grupie innych przyczyn wypadków. W Polsce organy procesowe nie prowadzą pogłębionej analizy zdarzeń drogowych, poza procedurami prawnymi ukierunkowanymi na poznanie wszelkich istotnych dla zdarzenia drogowego czynników[4]. Powoduje to znikomy procent spraw karnych związanych z niedopełnieniem obowiązków przez osoby odpowiedzialne za stan techniczny pojazdów czy też infrastruktury drogowej.

A przecież rozwój motoryzacji, jak również postęp techniczny w zakresie wszystkich elementów bezpieczeństwa ruchu drogowego, oprócz wymogów norm technicznych, powoduje, że ruch drogowy wymaga wprowadzenia odpowiednich środków kontroli bezpieczeństwa oraz ustanowienia sankcji za naruszanie reguł bezpieczeństwa przez użytkowników. Wraz z rozwojem norm prawnych regulujących zasady ruchu drogowego sfera ta nie mogła pozostać pominięta przez prawo karne.

[3] A. Gaberle, *Wypadki drogowe – aspekty kryminologiczne*, Wydawnictwo Prawnicze, Warszawa 1986, s. 182

[4] Ibidem. s. 24-34.

Analiza pojęcia „zarządzający transportem”

Definicję zarządzającego transportem zawiera art. 2 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1071/2009 z dnia 21 października 2009 r. ustanawiające wspólne zasady dotyczące warunków wykonywania zawodu przewoźnika drogowego i uchylające dyrektywę Rady Unii Europejskiej 96/26/WE z dnia 29 kwietnia 1996 r. Zgodnie z definicją zawartą w Rozporządzeniu, pojęcie zarządzającego transportem: „oznacza osoba fizyczna zatrudniona przez przedsiębiorcę lub jeżeli przedsiębiorca jest osobą fizyczną, tę osobę fizyczną lub w razie potrzeby, inną osobę fizyczną wyznaczoną przez tego przedsiębiorcę na podstawie umowy, zarządzającą w sposób rzeczywisty i ciągły operacjami transportowymi przedsiębiorcy”[5].

W polskim prawie odwołanie do zarządzającego transportem znaleźć można w Ustawie z dnia 6 września 2001 r. o transporcie drogowym[6]. Ustawa ta jednak nie zawiera legalnej definicji zarządzającego transportem. W art. 1 ust. 2 pkt 2 lit. C ustawy wskazane jest jedynie, że ustawa określa odpowiedzialność za naruszenie obowiązków lub warunków przewozu drogowego w stosunku m.in. do osób zarządzających transportem. Natomiast art. 5 ustawy zawiera bezpośrednie odesłanie do wskazanego wyżej rozporządzenia, podkreślając, że: „Podjęcie i wykonywanie transportu drogowego, z zastrzeżeniem art. 5b ust. 1 i 2, wymaga uzyskania zezwolenia na wykonywanie zawodu przewoźnika drogowego, na zasadach określonych w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1071/2009 z dnia 21 października 2009 r. ustanawiającym wspólne zasady dotyczące warunków wykonywania zawodu przewoźnika drogowego i uchylającym dyrektywę Rady 96/26/WE, zwanym dalej „rozporządzeniem (WE) nr 1071/2009”[7]. Zatem chcąc zdefiniować zarządzającego transportem, należy sięgnąć do definicji oraz przepisów zawartych w przywoływanym rozporządzeniu.

Zgodnie z definicją zawartą w powyżej powoływanym rozporządzeniu zarządzającym transportem może być jedynie osoba fizyczna. Oznacza to, że funkcję tę winien pełnić sam właściciel przedsiębiorstwa, członek władz

[5] Art. 2 pkt 5 Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1071/2009 z dnia 21 października 2009 r. (Dz.U.UE.L.2009.300.51).

[6] Art. 5 ust. 1 i 5a ust. 1 Ustawy z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2019 r. poz. 2140).

[7] Art. 5 ust. 2 pkt 1 Ustawy z dnia 6 września 2001 r. o transporcie drogowym.

spółki (zarządu) lub inny pracownik wyznaczony przez właściciela lub władze spółki. Ustawodawca dopuszcza również (w przypadku braku osób spełniających kryteria kompetencji zawodowych przez pracownika) możliwość zawarcia z osobą z zewnątrz, posiadającą odpowiednie kompetencje, umowy cywilno – prawnej, w której zostanie ściśle określony zakres praw i obowiązków w związku z pełnioną funkcją zarządzającego transportem[8]. Aktualne regulacje nie dopuszczają natomiast, aby funkcję tę pełnił organ kolegialny lub osoba prawna.

Obowiązki zarządzającego transportem

Zgodnie z przepisami powoływanego rozporządzenia osoba, która pełni obowiązki zarządzającego transportem, jest zobowiązana do rzeczywistego i ciągłego zajmowania się wszystkimi operacjami transportowymi w przedsiębiorstwie.

Obowiązki zarządzającego transportem wynikać mogą z:

- tytułu pełnienia określonej funkcji,
- przepisów prawa,
- tytułu obowiązku dbałości o stan techniczny pojazdów, ich konserwację,
- umowy, w tym umowy o pracę,
- dobrowolnego podjęcia się określonej czynności.

Wydaje się, że z punktu widzenia przedsiębiorcy powierzającemu innej osobie funkcję zarządzającego transportem koniecznym jest zawarcie umowy cywilnoprawnej lub umowy o pracę. Obowiązek taki wynika wprost z powoływanych powyżej przepisów rozporządzenia, które obligują przedsiębiorcę będącego osobą fizyczną, w razie braku właściwych kompetencji przedsiębiorcy, do zawarcia umowy z osobą fizyczną, która ma objąć rzeczywisty zarząd operacjami transportowymi przedsiębiorstwa. W umowie takiej należy precyzyjnie określić zadania oraz obowiązki zarządzającego transportem. Przede wszystkim do zakresu obowiązków takiej osoby należy: utrzymanie i konserwacja pojazdów, sprawdzanie umów i dokumentów przewozowych, podstawowa księgowość, przydzielanie ładunków lub usług kierowcom i pojazdom, sprawdzanie procedur związanych z bezpieczeństwem, kontrola stanu technicznego pojazdów, kontrola stanu psychofizycznego pracowników – kierowców.

[8] Art. 4 ust. 2 Rozporządzenia 1071/2009 z dnia 21 października 2009 r.

W ramach nadzorowania stanu technicznego pojazdów zarządzający obowiązany jest do nadzorowania regularnego wykonywania przeglądów pojazdów wynikających z instrukcji eksploatacyjnej oraz przepisów dotyczących obowiązkowych przeglądów technicznych. Ponadto osoba taka w związku z pełnioną funkcją zobowiązana jest do kontroli stanu pojazdów pod kątem spełniania wymagań określonych w rozporządzeniu z dnia 31 grudnia 2002 r., w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia[9]. O ile w przypadku małych firm i przedsiębiorców sprawowanie nadzoru nad stanem technicznym pojazdów i kontroli tego stanu nie wydaje się trudne, to w przypadku dużych przedsiębiorstw transportowych pojawia się problem z możliwością posiadania przez zarządzającego wiedzy o występujących bieżących usterkach pojazdów. Wydaje się zatem, że w takich przypadkach osoba zarządzająca transportem jest obowiązana w ramach swych obowiązków stworzyć odpowiednie procedury zgłaszania usterek przez kierowców.

Do zakresu obowiązków osoby zarządzającej transportem należy także nadzór nad stanem psychofizycznym kierowców. Realizacja tego obowiązku polega na kontrolowaniu stanu sprawności kierowcy, w tym przede wszystkim na sprawdzeniu stanu trzeźwości pracownika – kierowcy. Zwrócić należy jednak uwagę, że obowiązujące przepisy nie dopuszczają możliwości sprawdzenia trzeźwości bez zgody pracownika – kierowcy[10]. Możliwe jest wykonanie takiego badania bez zgody pracownika jedynie przez policję. Pojawia się zatem konieczność wprowadzenia zapisu dotyczącego takiej zgody do m.in. umów zawieranych z pracownikami, regulaminów pracy. Brak takich procedur i zapisów może być potraktowany jako zaniechanie przez zarządzającego transportem wykonania obowiązków związanych z bezpieczeństwem ruchu drogowego, które to zaniechanie wyczerpuje znamiona typu czynu zabronionego[11].

Osoba zarządzająca wykonuje określone zadania, zawsze działa wyłącznie w interesie przedsiębiorcy, który ją zatrudnia i sprawuje swe obowiązki

[9] Rozporządzenie Ministra Infrastruktury z dnia 31 grudnia 2002 r. w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia (Dz. U. z 2016 r. poz. 2022).

[10] Art. 17 ust. 3 Ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. z 2016 r. poz. 487 ze zm.)

[11] G. Bogdan, Art. 179, [w:] *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117-211a*, red. W. Wróbel, Wolters Kluwer, Warszawa 2017.

niezależnie od wpływów jakichkolwiek osób trzecich np. kontrahentów, spedytorów. Jednakże zakres kompetencji zarządzającego obejmuje przypadki korzystania z pojazdów wynajmowanych oraz osób niezatrudnionych przez przedsiębiorcę, lecz osobiście wykonujących przewozy drogowe na jego rzecz. W tym miejscu wskazać należy, że mając na względzie źródła oraz zakres obowiązków osoby zarządzającej transportem, należy dokonać dokładnej analizy, czy w świetle powyższych rozważań zarządzającemu transportem można przypisać odpowiedzialność z art. 179 k.k.

Odpowiedzialność karna zarządzającego transportem

Polskie prawo karne w art. 179 Ustawy z dnia 6 czerwca 1997 r. Kodeks karny (zwany dalej k.k.) przewiduje odpowiedzialność karną m.in. wobec osoby zarządzającej transportem, która wbrew szczególnemu obowiązkowi dopuszcza do ruchu pojazd mechaniczny albo inny pojazd w stanie bezpośrednio zagrażającym bezpieczeństwu w ruchu lądowym, wodnym lub powietrznym, lub dopuszcza do prowadzenia pojazdu mechanicznego albo innego pojazdu na drodze publicznej, w strefie zamieszkania lub w strefie ruchu przez osobę znajdującą się w stanie nietrzeźwości, będącą pod wpływem środka odurzającego lub osobę nieposiadającą wymaganych uprawnień.

Przestępstwo stypizowane w art. 179 k.k. ma charakter indywidualny właściwy. Jego sprawcą może być jedynie osoba, na której ciąży szczególny obowiązek pieczy nad bezpieczeństwem w komunikacji. Obowiązek ten może wynikać z ustawy, ze specyfiki zawodu lub pełnionej funkcji, jak również z umownego przyjęcia na siebie takiego obowiązku. Obejmuje on z jednej strony kontrolowanie stanu technicznego pojazdów uczestniczących w ruchu lądowym, wodnym lub powietrznym, a z drugiej – badanie osób prowadzących takie pojazdy pod kątem trzeźwości, braku odurzenia lub posiadania wymaganych uprawnień.

W doktrynie wskazuje się, że źródłem tego szczególnego obowiązku może być ustawa lub inny akt normatywny, stanowisko lub funkcja, umowa o pracę, a także dobrowolne podjęcie się określonej czynności. Podnosi się nadto, że obowiązek niedopuszczenia do ruchu niesprawnego pojazdu

lub niebezpiecznego kierowcy nie musi być podstawowym czy wyłącznym obowiązkiem zarządzającego transportem, a może być obowiązkiem dodatkowym[12].

Występek z art. 179 k.k. jest przestępstwem umyślnym. Może być popełniony w zamiarze bezpośrednim (świadomość złego stanu technicznego pojazdu, świadomość stanu odurzenia lub nietrzeźwości osoby kierującej) lub ewentualnym (godzenie się na usterkę pojazdu, która może ewentualnie spowodować zagrożenie w ruchu drogowym).

Czynność sprawcza może polegać zarówno na działaniu, jak i zaniechaniu. Poprzez działanie można rozumieć: wystawienie zlecenia na dokonanie przewozu niesprawnym pojazdem – pomimo posiadania wiedzy o jego stanie technicznym, wręczenie kluczyków nietrzeźwemu kierowcy bądź otwarcie bramy wyjazdowej. Popełnienie przestępstwa z art. 179 k.k. przez zaniechanie może polegać na niezapobieżeniu włączenia się do ruchu pojazdu, przez np. niedopełnienie obowiązków w zakresie diagnostyki bądź niepowstrzymaniu od uczestnictwa w ruchu prowadzącego pojazd przez np. zbagatelizowanie braku odpowiednich uprawnień kierowcy.

Występek z art. 179 k.k. jest przestępstwem formalnym, stanowi jedynie abstrakcyjne narażenie na niebezpieczeństwo i dla jego dokonania nie jest konieczne wystąpienie skutku[13]. Odpowiedzialność wyłącznie na podstawie tego przepisu wchodzi w grę tylko wówczas, gdy dopuszczenie niesprawnego pojazdu do ruchu albo dopuszczenie do prowadzenia pojazdu osoby znajdującej się w stanie nietrzeźwości, będącej pod wpływem środka odurzającego lub osoby nieposiadającej wymaganych uprawnień, nie pociągnęło za sobą skutków określonych w innych przepisach. W wypadku, gdy w wyniku tych nieprawidłowości dojdzie do sprowadzenia katastrofy (art. 173 k.k.), jej niebezpieczeństwa (art. 174 k.k.) lub wypadku drogowego (art. 177 k.k.), osoba odpowiedzialna za dopuszczenie do ruchu takiego pojazdu lub takiej osoby,

[12] L. Gardocki, *Dopuszczenie do ruchu niesprawnego pojazdu lub osoby niebezpiecznej (art. 179 KK)*, [w:] *Przestępstwa przeciwko państwu i dobrom zbiorowym. System Prawa Karnego. Tom 8*, red. L. Gardocki, Warszawa 2018.

[13] M. Budyn-Kulik, Art. 179, [w:] *Kodeks karny. Komentarz aktualizowany,* red. M. Mozgawa, LEX/el. 2020.

może ponosić odpowiedzialność karną za te przestępstwa jako współsprawca, niezależnie do odpowiedzialności bezpośredniego sprawcy zdarzenia[14].

W tym miejscu wskazać należy na wyrok Sądu Apelacyjnego we Wrocławiu z dnia 24 sierpnia 2016 r., w którym sąd stwierdził, że współwłaściciel firmy transportowej, pełniący funkcję zarządzającego transportem, poprzez zaniechanie swoich obowiązków w zakresie dbałości o stan techniczny pojazdów, popełnił przestępstwo z art. 179 k.k. W treści uzasadnienia sąd podniósł m.in., że: „będąc odpowiedzialnym za kontrolę stanu technicznego tego pojazdu, stosownie do eksploatacji poprzez kontrolę układów odpowiedzialnych za bezpieczeństwo, w tym układu hamulcowego nie dopełnił tych czynności, w wyniku czego doprowadził do stanu, w którym naczepa marki S. posiadała niesprawny układ podnoszenia naczepy, niesprawny hamulec ręczny, brak zamontowanych szczęk hamulcowych na osi II po stronie prawej, brak zamontowanego wałka rozpierającego na osi II koła prawego, brak szczęk hamulcowych na osi II koła lewego, niesprawne opony na osi I koła lewego i na osi III koła lewego i prawego i dopuścił pojazd w takim stanie do ruchu na trasie z K. do P., w tym do przewozu na naczepie załadunku o masie 23 760 kg, w stanie zagrażającym bezpieczeństwu powszechnemu (…)”[15].

Zauważyć należy, że mimo tego, iż polskie prawo przyjęło unormowania Rozporządzenia WE 1071/2009 w dniu 5 kwietnia 2013 r., wprowadzając do ustawy o transporcie drogowym oraz czasie pracy kierowców (obecna ustawa o transporcie drogowym) odesłanie do Rozporządzenia WE 1071/2009 w art. 5 ust 2 pkt 1, to w doktrynie wskazuje się, że podmiotem tego przestępstwa są: dyspozytorzy, dyżurni ruchu, osoby przeprowadzające kontrolę stanu technicznego pojazdu, funkcjonariusze służby ruchu, przełożeni kierowcy, których funkcja polega na kontroli stanu pojazdu, wymaganych kwalifikacji lub trzeźwości osób, dowódca i dysponent wojskowego pojazdu mechanicznego, osoby wykonujące usługi konserwacyjne i naprawcze, pomijając osoby zarządzające transportem drogowym.

W doktrynie istnieją także różne poglądy co do określenia czasu popełnienia przestępstwa z art. 179 k.k. Jeden z wyrażanych poglądów opiera się na założeniu, że już sam fakt zlecenia przewozu (wydania dyspozycji wyjazdu)

[14] Uchwała Sądu Najwyższego z dnia 28 lutego 1975 r., V KZP 2/74, OSNKW 1975, nr 3-4, poz. 33, teza 22.

[15] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 24 sierpnia 2016 r., II AKa 201/16, LEX nr 2115443.

niesprawnym pojazdem jest podstawą do postawienia sprawcy zarzutu z art. 179 k.k. Zwolennicy tego poglądu wskazują, że przestępstwo z art. 179 k.k. dokonane jest już w chwili podjęcia decyzji o dopuszczeniu pojazdu do ruchu lub osoby do jego prowadzenia, a zatem odpowiedzialności podlega np. dyspozytor, który wypuścił z bazy niesprawny samochód już w momencie podjęcia takiej decyzji, nawet jeżeli kierowca zakwestionowałby sprawność pojazdu[16]. Prezentowany jest także odmienny, jak się wydaje słuszny pogląd, że dopuszczenie do ruchu nie oznacza podjęcia samej decyzji o dopuszczeniu do ruchu pojazdu lub osoby wymienionej w tym przepisie, lecz wymagane jest, by znalazły się one w ruchu. Momentem tym jest rozpoczęcie jazdy[17].

Skazanie zarządzającego transportem z art. 179 k.k. oznacza dla niego konsekwencje dodatkowe w postaci wszczęcia przez właściwe organy postępowania administracyjnego w związku z utratą dobrej reputacji[18].

Analiza pojęcia „droga publiczna, strefa zamieszkania, strefa ruchu"

Analizując w dalszym ciągu znamiona przestępstwa z art. 179 k.k. należy uznać, że wprowadzone do opisu czynu pojęcia drogi publicznej, strefy zamieszkania i strefy ruchu winno rozumieć się zgodnie z brzmieniem ustalonym w Ustawie z dnia 21 marca 1985 r. o drogach publicznych[19] oraz Ustawie z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym[20]. I tak, zgodnie z art. 1 ustawy o drogach publicznych, drogą publiczną jest droga zaliczona na podstawie ustawy do jednej z kategorii dróg (krajowe, wojewódzkie, powiatowe, gminne), z której może korzystać każdy, zgodnie z jej przeznaczeniem, z ograniczeniami i wyjątkami określonymi w ustawie lub innych przepisach szczególnych. Przez drogę, zgodnie z art. 4 pkt 2 ustawy, rozumie się natomiast budowlę wraz z drogowymi obiektami inżynierskimi, urządzeniami

[16] B. Świątkiewicz, *Niektóre zagadnienia rozpoznawania znamion przestępstwa z* art. 146 *KK*, ZNASW 1990, nr 60, s. 63; R .Citowicz, [w:] *Kodeks karny. Część szczególna*, red. M. Królikowski, R. Zawłocki, t. I, 2013,s. 434.

[17] R.A. Stefański, *Komentarz do art. 179 k.k.*, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2019.

[18] Rozporządzenie Parlamentu Europejskiego I Rady (WE) NR 1071/2009z dnia 21 października 2009 r. ustanawiające wspólne zasady dotyczące warunków wykonywania zawodu przewoźnika drogowego i uchylające dyrektywę Rady 96/26/WE (L300/51 z 14.11.2009 r.) art. 4 ust 1 w zw z art. 3 ust. 1 lit b i d.

[19] Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2018 r. poz. 2068).

[20] Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2020 r. poz. 110).

oraz instalacjami, stanowiącą całość techniczno-użytkową, przeznaczoną do prowadzenia ruchu drogowego, zlokalizowaną w pasie drogowym. Trudności jednak może przysporzyć rozróżnienie strefy zamieszkania i strefy ruchu. Definicję strefy zamieszkania zawiera art. 2 ustawy – Prawo o ruchu drogowym, według którego strefę zamieszkania stanowi obszar obejmujący drogi publiczne lub inne drogi, na którym obowiązują szczególne zasady ruchu drogowego, a wjazdy i wyjazdy oznaczone są odpowiednimi znakami drogowymi (pkt 16). Natomiast przez strefę ruchu rozumie się obszar obejmujący co najmniej jedną drogę wewnętrzną, na który wjazdy i wyjazdy oznaczone są odpowiednimi znakami drogowymi (pkt 16a). Konieczność rozpoznania, czy mamy do czynienia ze strefą zamieszkania, strefą ruchu lub drogą publiczną wymaga zatem dokładnego zbadania całego analizowanego obszaru. Należy dodać ponadto, że przepis art. 2 pkt 1 ustawy – Prawo o ruchu drogowym definiuje drogę jako wydzielony pas terenu składający się z jezdni, pobocza, chodnika, drogi dla pieszych lub drogi dla rowerów, łącznie z torowiskiem pojazdów szynowych znajdującym się w obrębie tego pasa, przeznaczony do ruchu lub postoju pojazdów, ruchu pieszych, jazdy wierzchem lub pędzenia zwierząt.

Niesprawność pojazdu w kontekście jej wpływu na bezpieczeństwo w ruchu

Dla stwierdzenia realizacji znamion przestępstwa określonego w art. 179 k.k. konieczne jest ustalenie, że pojazd dopuszczony do ruchu znajduje się w stanie bezpośrednio zagrażającym bezpieczeństwu w ruchu pojazdów. Wymaga to wskazania na cechy pojazdu, które sprawiają, że w przypadku udziału pojazdu w ruchu istnieje wysokie prawdopodobieństwo doprowadzenia do uszczerbku w dobrach prawnych uczestników ruchu[21].

Słowo „bezpośrednio" zawęża zakres desygnatów tego określenia, ograniczając je do takich niesprawności pojazdu, które uniemożliwiają lub w poważnym stopniu utrudniają bezpieczne prowadzenie pojazdu. Wskazuje ono na obiektywną niesprawność pojazdu, a więc taką, która niezależnie od tego, kto taki pojazd prowadzi, uniemożliwia lub w poważnym stopniu

[21] Wyrok Sądu Najwyższego z dnia 15 listopada 2012 r., II KK 6/12, OSNKW 2013, nr 5, poz. 39.

utrudnia jego bezpieczne prowadzenie[22]. W orzecznictwie na gruncie kodeksu z 1969 r. wskazywano, że: „nie każda jednak niesprawność pojazdu rodzi odpowiedzialność na podstawie art. 146 (obecnie art. 179 k.k.). Karalne w myśl tego przepisu jest dopuszczenie do ruchu tylko takiego pojazdu (...), którego stan zagraża bezpośrednio bezpieczeństwu ruchu. Chodzi tu więc nie o jakąkolwiek niesprawność pojazdu, lecz o taką, która w sposób ewidentny uniemożliwia lub w poważnym stopniu utrudnia bezpieczne prowadzenie pojazdu. Muszą to więc być tego rodzaju wady w stanie technicznym pojazdu, jak np. niesprawny układ kierowniczy lub hamulcowy, nadmierne zużycie opon, braki czy uszkodzenia urządzeń sygnalizacyjnych lub oświetlenia, wywołujące konkretny i bezpośredni, a nie abstrakcyjny, stan zagrożenia na drodze"[23].

O ile poglądy związane z pojęciem „bezpośredniego zagrożenia" należy uznać za wciąż aktualne, to jednak dominujący w starszym orzecznictwie pogląd, jakoby przestępstwo z art. 179 k.k. było przestępstwem materialnym, nie znajduje aprobaty w aktualnej doktrynie i najnowszym orzecznictwie. Dominującym poglądem jest bowiem uznanie przestępstwa z art. 179 k.k. za przestępstwo formalne, jak już to wskazywano wcześniej[24].

Zaznaczyć należy również, że pojazdem bezpośrednio zagrażającym bezpieczeństwu w ruchu jest nie tylko pojazd z usterkami technicznymi, ale także niewłaściwie załadowany, w wyniku czego kierowanie nim jest znacznie utrudnione lub w każdej chwili może doprowadzić do jego wywrócenia się. W grę może wchodzić umieszczenie ładunku, powodującego przekroczenie dopuszczalnej masy całkowitej lub dopuszczalnej ładowności pojazdu, naruszającego stateczność pojazdu, utrudniającego kierowanie nim, ograniczającego widoczność drogi, zasłaniającego światła lub urządzenia sygnalizacyjne, a także niezabezpieczenie lub wadliwe zabezpieczenie ładunku przed zmianą położenia. Stanem pojazdu zagrażającym bezpośrednio bezpieczeństwu

[22] K. Buchała, *Przestępstwa i wykroczenia przeciwko bezpieczeństwu w komunikacji drogowej: komentarz*, Bydgoszcz 1997, s. 181; M. Starzyk, *Koła jezdne jako element pojazdu mogący stwarzać bezpośrednie zagrożenia bezpieczeństwa ruchu drogowego – w kontekście art. 179 k.k.,* PnD 2015, nr 2, s. 71-73.

[23] Uchwała pełny skład Izby Karnej Sądu Najwyższego z dnia 28 lutego 1975 r., V KZP 2/74, OSNKW 1975, nr 3-4, poz. 33, teza 19.

[24] Tak: G. Bogdan, Art. 179, [w:] *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117-211a*, red. W. Wróbel, A. Zoll, Warszawa R. A. Stefański, Art. 179, [w:] *Kodeks karny. Komentarz*, red. M. Filar, 2016.

w ruchu jest także używanie pojazdu niezgodnie z jego przeznaczeniem, np. przewożenie osób pojazdem do tego nieprzystosowanym[25].

Analiza występku z art. 179 k.k. i wykroczenia z art. 96 k.w.

Odpowiedzialność zarządzającego transportem w świetle art. 179 k.k. rodzi jeszcze jedno interesujące zagadnienie, które wciąż budzi wątpliwości w doktrynie i judykaturze. Analiza przepisów Kodeksu karnego oraz Kodeksu wykroczeń wskazuje bowiem, że przestępstwo z art. 179 k.k. ma swój odpowiednik w art. 96 Kodeksu wykroczeń, a podobny zakres regulacji tych dwóch przepisów sprawia, że należy rozważyć, czy istnieje możliwość, aby wykroczenie z art. 96 k.w. oraz przestępstwo z art. 179 k.k. pozostawały w jednoczynowym zbiegu idealnym.

W art. 96 k.w. opisane są trzy typy wykroczenia: dopuszczenie do ruchu niesprawnego kierującego lub niesprawnego pojazdu (§ 1), nieumyślne dopuszczenie do prowadzenia pojazdu na drodze publicznej przez osobę niemającą wymaganych uprawnień (§ 2) oraz niewskazanie wbrew obowiązkowi na żądanie uprawnionego organu osoby, której został powierzony pojazd do kierowania lub używania w oznaczonym czasie (§ 3)[26]. Pod kątem zbiegu z przestępstwem określonym w art. 179 k.k. należy zbadać wykroczenia opisane w § 1 i § 2, gdyż z samej treści art. 96 § 3 k.w. wynika, że wykroczenie to nie wypełnia jednocześnie znamion art. 179 k.k. W art. 96 § 1 k.w. i art. 179 k.k. inaczej określony jest podmiot, czynność wykonawcza, jak również miejsce popełnienia czynu i strona podmiotowa. W literaturze wskazuje się, że w przypadku, gdy na sprawcy (właścicielu, posiadaczu, użytkowniku) ciąży szczególny prawny obowiązek, wskazany w art. 179 k.k., to popełnione umyślnie wykroczenie z art. 96 § 1 pkt 2 i 5 k.w. jednocześnie wypełnia znamiona przestępstwa z art. 179 k.k.[27]. I w tym przypadku mamy do czynienia ze zbiegiem rzeczywistym pomijalnym art. 96 § 1 pkt 2 i 5 k.w. oraz art. 179 k.k.

[25] I. Andrejew, W. Świda, [w:] Kodeks *karny z komentarzem,* red. W. Wolter, Warszawa 1973, s. 430.

[26] R. A. Stefański, *Wykroczenia drogowe. Komentarz*, LEX 2011.

[27] M. Budyn-Kulik, *Odpowiedzialność za ten sam czyn na podstawie różnych ustaw w orzecznictwie sądów powszechnych*, Instytut Wymiaru Sprawiedliwości Warszawa 2015, s. 17.

Zaś wszystkie pozostałe postaci wykroczenia, opisane w art. 96 § 1 pkt 1, 3, 4 i 6 kw., nie wypełniają jednocześnie znamion przestępstwa z art. 179 k.k.[28]

Natomiast jeżeli zachowanie sprawcy wypełnia znamiona wykroczenia z art. 96 § 2 kw. i polega na dopuszczeniu pojazdu na drodze publicznej pomimo braku odpowiednich urządzeń / przyrządów (czyli wypełniającego także znamiona z art. 96 § 1 pkt 5 kw.), może pozostawać w zbiegu rzeczywistym niewłaściwym pomijalnym z przestępstwem z art. 179 k.k. Jednakże, jeżeli sprawca popełni czyn z art. 96 § 2 k.w. nieumyślnie, wówczas czyn ten nie może jednocześnie wypełniać znamion przestępstwa z art. 179 k.k., gdyż strona podmiotowa przestępstwa z art. 179 k.k. przewiduje jedynie umyślność[29].

W doktrynie oraz judykaturze wskazuje się na możliwy zbieg przestępstwa z art. 179 k.k. czy wykroczeń przewidzianych w art. 96 k.w., z innymi przepisami Kodeksu karnego (m.in. art. 177 § 1 k.k., art. 174 § 2 k.k.)[30].

Podsumowanie

Analiza przepisów rozporządzenia oraz ustawy o transporcie drogowym oraz treści artykułu 179 k.k. prowadzi do stwierdzenia, że na osobie zarządzającej transportem ciąży szczególny obowiązek niedopuszczenia do ruchu pojazdu niesprawnego albo osoby stwarzającej zagrożenie dla ruchu. Obowiązek ten wynika przede wszystkim z powodu pełnienia określonej funkcji, przepisów prawa, tytułu obowiązku dbałości o stan techniczny pojazdów oraz ich konserwację, umowy, w tym umowy o pracę lub umowy cywilnoprawnej. Podmioty, m.in. zarządzający transportem, objęte są odpowiedzialnością karną za przestępstwo art. 179 k.k., mają realny wpływ na stan techniczny pojazdów dopuszczonych do ruchu oraz na zdolność psychomotoryczną kierujących, uczestniczących w ruchu, gdyż są obciążone szczególnym prawnym obowiązkiem dbania o bezpieczeństwo ruchu. Zatem w przypadku realizacji tak znamion przedmiotowych, jak i podmiotowych występku stypizowanego w art. 179 k.k. można przypisać odpowiedzialność karną zarządzającego

[28] M. Budyn-Kulik, *Odpowiedzialność…*, op. cit., s. 18.

[29] Ibidem

[30] R. A. Stefański, *Odpowiedzialność za udostępnienie prowadzenia pojazdu osobie znajdującej się w stanie po użyciu alkoholu lub podobnie działającego środka*, Prokuratura i Prawo, nr 5, 2007.

transportem. Zasadnym i celowym wydaje się, z uwagi na rozwój transportu drogowego, szczegółowe określenie obowiązków zarządzającego transportem w przepisach prawnych, aby nie występowały wątpliwości, jakie uprawnienia oraz obowiązki ciążą na zarządzającym transportem. W literaturze i judykaturze podkreśla się, że możliwy jest zbieg art. 179 k.k. z art. 96 k.w. oraz innymi przestępstwami przeciwko bezpieczeństwu w komunikacji.

Literatura

1. Andrejew I., Świda W., *Kodeks karny z komentarzem*, red. W. Wolter, Warszawa 1973.
2. Bogdan G., *Art. 179*, [w:] *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117-211a*, red. W. Wróbel, A. Zoll, Warszawa 2017.
3. Buchała K., *Przestępstwa i wykroczenia przeciwko bezpieczeństwu w komunikacji drogowej: komentarz*, Bydgoszcz 1997.
4. Budyn-Kulik M., *Odpowiedzialność za ten sam czyn na podstawie różnych ustaw w orzecznictwie sądów powszechnych*, Warszawa 2015.
5. Citowicz R., *Kodeks karny. Część szczególna*, red. M. Królikowski, R. Zawłocki, t. I, Warszawa 2013.
6. Gardocki L., *Dopuszczenie do ruchu niesprawnego pojazdu lub osoby niebezpiecznej (art. 179 KK)*, [w:] *Przestępstwa przeciwko państwu i dobrom zbiorowym. System Prawa Karnego. Tom 8*, red. L. Gardocki, Warszawa 2018.
7. Stefański R. A., Art. 179, [w:] *Kodeks karny. Komentarz*, red. M. Filar, 2016. *Kodeks karny. Komentarz*, red. M. Filar, Warszawa 2016.
8. Mozgawa M., *Kodeks karny. Komentarz aktualizowany,* red. M. Mozgawa, LEX/el. 2020.
9. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1071/2009 z dnia 21 października 2009 r. (Dz.U.UE.L.2009.300.51).
10. Rozporządzenie Ministra Infrastruktury z dnia 31 grudnia 2002 r. w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia (Dz.U. 2016, poz. 2022).
11. Starzyk M., *Koła jezdne jako element pojazdu mogący stwarzać bezpośrednie zagrożenia bezpieczeństwa ruchu drogowego – w kontekście art. 179 k.k.*, PnD 2015, nr 2.
12. Stefański R.A., *Komentarz do art. 179 k.k.*, [w:] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2019.
13. Stefański R.A., *Odpowiedzialność za udostępnienie prowadzenia pojazdu osobie znajdującej się w stanie po użyciu alkoholu lub podobnie działającego środka*, Prokuratura i Prawo 2007, nr 5.
14. Stefański R.A., *Wykroczenia drogowe. Komentarz*, LEX 2011.
15. Świątkiewicz B., *Niektóre zagadnienia rozpoznawania znamion przestępstwa z art. 146 KK*, ZNASW 1990, Nr 60.
16. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. 2019, poz. 1950).
17. Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (t.j. Dz.U. 2019, poz. 821).

18. Ustawa z dnia 6 września 2001 r. o transporcie drogowym (Dz.U. 2019, poz. 2140).
19. Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz.U. 2016, poz. 487 ze zm.).
20. Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz.U. 2018, poz. 2068).
21. Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. 2020, poz. 110).
22. Uchwała Sądu Najwyższego z dnia 28 lutego 1975 r., V KZP 2/74, OSNKW 1975, nr 3-4, poz. 33.
23. Uchwała pełnego składu Izby Karnej Sądu Najwyższego z dnia 28 lutego 1975 r., V KZP 2/74, OSNKW 1975, nr 3-4, poz. 33.
24. Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 24 sierpnia 2016 r., II AKa 201/16, LEX nr 2115443.
25. Wyrok Sądu Najwyższego z dnia 15 listopada 2012 r., II KK 6/12, OSNKW 2013, nr 5, poz. 39.

mgr Beata Spinek
ORCID: 0000-0003-2141-8361

https://doi.org/10.29316/9788368103205_19

PRZECIWDZIAŁANIE ZAGROŻENIOM W OBSZARZE RUCHU DROGOWEGO

COUNTERACTING THREATS IN THE AREA OF ROAD TRAFFIC

Streszczenie

Celem rozdziału jest przedstawienie wieloaspektowych działań służących poprawie bezpieczeństwa w ruchu drogowym w Polsce poprzez analizę zagrożeń, środków prewencyjnych, ram prawnych i wykorzystania nowoczesnych technologii. Autorka przedstawia skalę problemu poprzez dane statystyczne ukazujące liczbę ofiar wypadków drogowych w ostatnich latach, wskazując jednocześnie najważniejsze czynniki ryzyka, takie jak nadmierna prędkość, jazda pod wpływem alkoholu, nieuwaga, zmęczenie czy niestosowanie środków ochronnych. W dalszej części opisany zostaje Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030, którego pięć filarów – zarządzanie systemem, bezpieczny człowiek, droga, pojazd oraz ratownictwo – stanowi kompleksową strukturę działań profilaktycznych. Kolejno zaprezentowano innowacyjne technologie wspierające bezpieczeństwo drogowe, takie jak systemy wspomagania kierowcy (ADAS), inteligentne przejścia dla

Summary

The aim of the chapter is to present multifaceted activities aimed at improving road safety in Poland through the analysis of threats, preventive measures, legal frameworks, and the use of modern technologies. The author presents the scale of the problem through statistical data showing the number of road accident victims in recent years, at the same time indicating the most important risk factors, such as excessive speed, driving under the influence of alcohol, inattention, fatigue, or failure to use protective measures. Further on, the National Road Safety Programme 2021-2030 is described, whose five pillars – system management, safe people, road, vehicle, and rescue – constitute a comprehensive structure of preventive activities. Innovative technologies supporting road safety, such as driver assistance systems (ADAS), intelligent pedestrian crossings, ITS systems and vehicle-to-environment communication (V2X), were then presented. The research problem was formulated in the question:

pieszych, systemy ITS i komunikacja pojazdów z otoczeniem (V2X). Problem badawczy sformułowano w pytaniu: jakie działania są najskuteczniejsze w przeciwdziałaniu zagrożeniom w ruchu drogowym w Polsce w świetle obowiązujących strategii, regulacji i dostępnych technologii? Postawiona hipoteza zakłada, że zintegrowane podejście oparte na współpracy instytucji publicznych, wykorzystaniu nowych technologii, edukacji oraz skutecznym egzekwowaniu przepisów prawa może istotnie zmniejszyć liczbę wypadków drogowych i ich skutki. W rozdziale zastosowano metody teoretyczne, takie jak analiza aktów prawnych, dokumentów strategicznych, danych statystycznych oraz literatury przedmiotu.

Słowa kluczowe: bezpieczeństwo ruchu drogowego, prewencja, edukacja komunikacyjna, technologie transportowe oraz zarządzanie ruchem

what actions are the most effective in counteracting road traffic hazards in Poland in the light of the applicable strategies, regulations, and available technologies? The hypothesis assumes that an integrated approach based on cooperation of public institutions, the use of new technologies, education and effective enforcement of legal regulations can significantly reduce the number of road accidents and their consequences. The chapter uses theoretical methods, such as the analysis of legal acts, strategic documents, statistical data, and literature on the subject.

Keywords: road safety, prevention, transport education, transport technologies and traffic management

Wstęp

Na zagrożenia w ruchu drogowym narażony jest każdy obywatel – niezależnie od tego, czy porusza się samochodem, motocyklem, urządzeniem transportu osobistego, rowerem, czy jest pieszym. W trosce o własne bezpieczeństwo użytkownicy dróg powinni poważnie podchodzić do kwestii związanych z bezpieczeństwem, ponieważ od tego za każdym razem zależy zdrowie i życie nasze, a także i innych uczestników ruchu. W Polsce w latach 2015-2024 zginęło prawie 25 tysięcy osób (średnio około 2 tysięcy rocznie w ciągu ostatnich 5 lat) oraz rany odniosło kolejne prawie 320 tysięcy osób[1]. Dla porównania liczba morderstw waha się w okolicach 500 rocznie, ryzyko śmierci w wypadku drogowym jest więc czterokrotnie wyższe niż bycie ofiarą

[1] Statystyka Policji, https://statystyka.policja.pl/st/ruch-drogowy/76562,wypadki-drogowe-raporty-roczne.html, [dostęp: 04.05.2025].

morderstwa[2]. Niemniej wielu użytkowników ruchu bagatelizuje zagrożenia, na które są wystawieni.

Zagrożenia w obszarze ruchu drogowego

W celu zrozumienia zagadnień związanych z bezpieczeństwem i przeciwdziałaniem zagrożeniom w ruchu drogowym należy poddać analizie odpowiednie dokumenty wydane przez jednostki administracji państwowej, jak również przepisy prawa, a także dane statystyczne oraz opracowania naukowe.

Przyczynami zagrożeń w ruchu drogowym są następujące czynniki wskazane w Narodowym Programie Bezpieczeństwa Ruchu Drogowego 2021-2030:

- prędkość,
- alkohol i inne podobnie działające substancje,
- prowadzenie pojazdów przy rozproszonej uwadze oraz w stanie zmęczenia,
- niestosowanie lub niewłaściwe stosowanie pasów bezpieczeństwa oraz urządzeń przytrzymujących dzieci w pojazdach oraz innego wyposażenia ochronnego[3].

Przekroczenie prędkości lub niedostosowanie jej do warunków i umiejętności kierowcy jest oczywistą przyczyną powstawania wypadków drogowych, oprócz zmniejszenia czasu na reakcję uczestników ruchu. Wraz z jej wzrostem zwiększa się ryzyko cięższych obrażeń u poszkodowanych i ich śmierci.

Według danych ze strony Policji dzięki działaniom policjantów w 2024 r. zostało ujawnionych 91 300 nietrzeźwych kierujących[4]. Spożycie alkoholu lub innych substancji psychoaktywnych wpływa na ocenę sytuacji przez kierowcę, może doprowadzić do pogorszenia funkcji psychomotorycznych, co w efekcie może doprowadzić do błędów.

Ograniczenie skupienia uczestników ruchu poprzez wykonywanie innych czynności, jak np. rozmowa przez telefon, może doprowadzić do

[2] Statystyka Policji, https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko/63411,Zabojstwo-art-148.html, [dostęp: 04.05.2025].

[3] *Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030*, Krajowa Rada Bezpieczeństwa Ruchu Drogowego, Warszawa 2021, s. 50-51.

[4] *Bezpieczeństwo na polskich drogach to priorytet*, https://www.policja.pl/pol/aktualnosci/255080,Bezpieczenstwo-na-polskich-drogach-to-priorytet.html, [dostęp: 04.05.2025].

wypadku. Zagrożenie dotyczy zarówno osób kierujących pojazdami, jak i pieszych. Nieuwaga może doprowadzić do wtargnięcia pieszego na jezdnię pod rozpędzony pojazd, zaś brak uwagi kierowcy doprowadzić do niewykonania lub nienależytego wykonania czynności. Podobnie jak w przypadku alkoholu, brak snu prowadzi do ograniczenia funkcji psychomotorycznych zwiększając czas wykonania reakcji na daną sytuację drogową. W skrajnych przypadkach kierowca może też usnąć za kierownicą tracąc całkowite panowanie nad pojazdem.

Brak lub niewłaściwe stosowanie urządzeń służących ochronie bezpieczeństwa, jak na przykład fotelików lub pasów, podczas wypadku w znaczny sposób może przełożyć się na ciężar obrażeń u osób poszkodowanych. Poduszki powietrzne, które mają cel ochronić pasażerów pojazdu, w przypadku umieszczenia fotelika RWF (tyłem do kierunku jazdy) na przednim siedzeniu, mogą doprowadzić do ciężkiego urazu na skutek jej uwolnienia[5]. Ryzyko większych obrażeń występuje również w przypadku niestosowania ochraniaczy, takich jak kaski czy pancerze przez kierujących jednośladami. Są oni bowiem bezpośrednio narażeni na kontakt z jednią i urazy spowodowane przez upadek ze swojego pojazdu.

Profilaktyka zagrożeń

Do profilaktyki zagrożeń w obszarze ruchu drogowego można stosować wiele środków, od działania służb państwowych, jak Policja, Główny Inspektorat Transportu Drogowego, instytucje oświatowe i sami uczestnicy ruchu.

Pięć filarów, stanowiących główne obszary działań dedykowanych poprawie bezpieczeństwa ruchu drogowego do 2030 r., stanowi podstawę działań w ramach Narodowego Programu Bezpieczeństwa Ruchu Drogowego 2021–2030. W kolejności są to:

1. „Filar I – System zarządzania bezpieczeństwem ruchu drogowego,
2. Filar II – Bezpieczny człowiek,
3. Filar III – Bezpieczne drogi,
4. Filar IV – Bezpieczny pojazd,
5. Filar V – Ratownictwo i opieka powypadkowa”[6].

[5] *Fotelik samochodowy kontra poduszka powietrzna w samochodzie*, https://fotelik.info.pl/fotelik-samochodowy-kontra-poduszka-powietrzna-w-samochodzie/, [dostęp: 04.05.2025].

[6] *Narodowy Program Bezpieczeństwa Ruchu …*, op. cit., s. 26.

W ramach pierwszego filaru, czyli Systemu Zarządzania Bezpieczeństwem Ruchu Drogowego można wyróżnić następujące działania polegające na*:*

- optymalizacji struktur organizacyjnych systemu zarządzania bezpieczeństwem ruchu drogowego na szczeblu krajowym,
- optymalizacji struktur organizacyjnych systemu zarządzania bezpieczeństwem ruchu drogowego na szczeblu regionalnym,
- optymalizacji przepisów prawa w odniesieniu do systemu zarządzania bezpieczeństwem ruchu drogowego,
- utworzenie mechanizmów finansowania w odniesieniu do systemu zarządzania bezpieczeństwem ruchu drogowego,
- optymalizacji systemu zbierania i analizy danych,
- optymalizacji systemu badań i transferu wiedzy w zakresie bezpieczeństwa ruchu drogowego,
- optymalizacji działań komunikacyjnych w zakresie bezpieczeństwa ruchu drogowego[7].

Kolejnym z filarów jest bezpieczny człowiek – dotyczy on uczestników ruchu drogowego zarówno kierowców, pieszych, jak i rowerzystów. Skupia się na kształtowaniu właściwych postaw, edukacji, podnoszeniu świadomości zagrożeń, szkoleniu umiejętności oraz egzekwowaniu przepisów prawa. Celem jest zmniejszenie ryzyka ludzkich błędów i niewłaściwych zachowań prowadzących do wypadków. W ramach tego filaru można wyróżnić:

- Kształtowanie bezpiecznych postaw i zachowań uczestników ruchu drogowego.
- Podnoszenie świadomości społecznej w zakresie zagrożeń i konsekwencji niebezpiecznych zachowań.
- Prowadzenie kampanii edukacyjnych i informacyjnych.
- Szkolenie i doskonalenie umiejętności kierowców, pieszych i rowerzystów.
- Wzmacnianie systemu kontroli przestrzegania przepisów ruchu drogowego (np. dotyczących trzeźwości, prędkości, korzystania z pasów bezpieczeństwa)[8].

Następny z filarów jest zatytułowany – bezpieczne drogi, odnosi się do infrastruktury drogowej i jej wpływu na bezpieczeństwo ruchu. Obejmuje

[7] Ibidem, s. 43.

[8] Ibidem, s. 44.

projektowanie bezpiecznych dróg, modernizację niebezpiecznych odcinków, poprawę oznakowania i oświetlenia, tworzenie przejść dla pieszych oraz infrastruktury rowerowej. Celem jest ograniczenie skutków ewentualnych błędów uczestników ruchu. Zaleca się:

- projektowanie i modernizację infrastruktury drogowej zgodnie z zasadami „forgiving roads" (drogi wybaczające błędy),
- likwidację miejsc szczególnie niebezpiecznych (tzw. czarnych punktów),
- budowę i modernizację przejść dla pieszych z uwzględnieniem ich właściwego oznakowania i oświetlenia,
- wdrażanie rozwiązań poprawiających bezpieczeństwo rowerzystów i pieszych (np. ścieżki rowerowe, separacja ruchu),
- audyt i inspekcje bezpieczeństwa dróg[9].

Kolejnym z filarów jest- bezpieczny pojazd, skupia się on na technicznym stanie pojazdów oraz zastosowaniu nowoczesnych technologii zwiększających bezpieczeństwo. Odnosi się do promowania pojazdów wyposażonych w systemy wspomagające kierowców (np. ABS, ESP, systemy automatycznego hamowania) oraz zapewnienia skutecznych badań technicznych pojazdów. Można wyróżnić następujące działania:

- wspieranie rozwoju i stosowania nowoczesnych technologii bezpieczeństwa w pojazdach (np. systemy wspomagające kierowcę: ABS, ESP, systemy automatycznego hamowania),
- kontrola stanu technicznego pojazdów, w tym skuteczne badania techniczne,
- promowanie zakupu pojazdów spełniających wysokie standardy bezpieczeństwa (np. oceny euro ncap).,
- wspieranie rozwoju elektromobilności i pojazdów niskoemisyjnych[10].

Ostatnim już z filarów jest ratownictwo i opieka powypadkowa, dotyczy systemu ratownictwa drogowego oraz pomocy ofiarom wypadków. Odnosi się do działań mających na celu szybkie udzielanie pomocy poszkodowanym, skracanie czasu reakcji służb ratowniczych, poprawę jakości opieki medycznej oraz wsparcie rehabilitacyjne dla ofiar wypadków. Zaleca się:

- doskonalenie systemu ratownictwa drogowego i skracanie czasu dotarcia służb ratunkowych na miejsce zdarzenia,

[9] Ibidem, s. 57.

[10] Ibidem, s. 66.

- usprawnianie systemu powiadamiania i koordynacji działań ratowniczych (np. system ecall),
- podnoszenie kwalifikacji służb ratowniczych,
- zapewnienie skutecznej pomocy medycznej poszkodowanym,
- wspieranie rehabilitacji i pomocy ofiarom wypadków drogowych[11].

Ramy strategiczne i prawne bezpieczeństwa drogowego

Bezpieczeństwo ruchu drogowego w Polsce jest kształtowane zarówno przez krajowe, jak i międzynarodowe akty prawne oraz dokumenty strategiczne. Wskazują one kierunki działań instytucji odpowiedzialnych za poprawę bezpieczeństwa na drogach, definiują cele, zadania oraz sposoby realizacji polityki w tym zakresie.

Ramy strategiczne

Do ram strategicznych można zaliczyć:

- Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030. Jest to kluczowy dokument strategiczny, który określa politykę państwa w zakresie bezpieczeństwa drogowego [12]. Opiera się na idei „Wizji Zero", zakładającej dążenie do całkowitego wyeliminowania ofiar śmiertelnych i ciężko rannych w wypadkach drogowych.
- Krajowa Polityka Transportowa – dokument ten wskazuje na konieczność zapewnienia zrównoważonego rozwoju transportu, ze szczególnym uwzględnieniem poprawy bezpieczeństwa wszystkich uczestników ruchu drogowego[13].
- Unijna Polityka Bezpieczeństwa Ruchu Drogowego (Strategia Komisji Europejskiej). Polska jako członek Unii Europejskiej, realizuje również cele wyznaczone przez UE, zmierzające do ograniczenia liczby ofiar śmiertelnych w wypadkach drogowych o 50% do 2030 roku[14].

[11] Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030, Krajowa Rada Bezpieczeństwa Ruchu Drogowego, Warszawa 2021, s. 74.

[12] Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030, Krajowa Rada Bezpieczeństwa Ruchu Drogowego, Warszawa 2021.

[13] Krajowa Polityka Transportowa do 2030 roku, Ministerstwo Infrastruktury, Warszawa 2019.

[14] Komisja Europejska, *EU Road Safety Policy Framework 2021-2030*, Bruksela 2019.

Ramy prawne

Przepisy prawa służące przeciwdziałaniu zagrożeniom w ruchu drogowym, to przede wszystkim:

- Ustawa z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym. Jest to podstawowy akt prawny regulujący zasady poruszania się po drogach publicznych, obowiązki uczestników ruchu drogowego oraz warunki techniczne pojazdów[15].
- Ustawa z dnia 6 września 2001 r. o transporcie drogowym. Reguluje kwestie związane z transportem drogowym, w tym przewozami osób i rzeczy, a także normy dotyczące czasu pracy kierowców i bezpieczeństwa przewozów[16].
- Ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami. Określa warunki uzyskiwania uprawnień do kierowania pojazdami, obowiązki kierujących oraz system nadzoru nad szkoleniami i egzaminami[17].
- Kodeks karny[18] oraz Kodeks wykroczeń. Zawierają regulacje dotyczące odpowiedzialności karnej i wykroczeniowej za nieprzestrzeganie przepisów ruchu drogowego, w tym za prowadzenie pojazdu pod wpływem alkoholu lub środków odurzających, spowodowanie wypadków czy przekroczenie dozwolonej prędkości[19].
- Rozporządzenia wykonawcze m.in. w sprawie znaków i sygnałów drogowych[20], warunków technicznych pojazdów[21] i homologacji pojazdów[22]. Uszczegóławiają przepisy ustawowe w zakresie organizacji ruchu drogo-

[15] Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. z 1997 r. Nr 98, poz. 602 ze zm.).

[16] Ustawa z dnia 6 września 2001 r. o transporcie drogowym (Dz. U. z 2001 r. Nr 125, poz. 1371 ze zm.).

[17] Ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2011 r. Nr 30, poz. 151 ze zm.).

[18] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 ze zm.).

[19] Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 1971 r. Nr 12, poz. 114 ze zm.).

[20] Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003 r. w sprawie szczegółowych warunków technicznych dla znaków i sygnałów drogowych oraz urządzeń bezpieczeństwa ruchu drogowego i warunków ich umieszczania na drogach (Dz. U. z 2003 r. Nr 220, poz. 2181).

[21] Rozporządzenie Ministra Infrastruktury z dnia 31 grudnia 2002 r. w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia (Dz. U. z 2003 r. Nr 32, poz. 262 ze zm.).

[22] Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2020 r. w sprawie homologacji pojazdów (Dz. U. z 2020 r. poz. 2412).

wego, infrastruktury drogowej oraz wymagań technicznych dla pojazdów.

Bezpieczeństwo ruchu drogowego w Polsce jest jednym z kluczowych elementów polityki transportowej państwa, mającym na celu ochronę życia i zdrowia uczestników ruchu. Realizacja działań w tym zakresie opiera się na solidnych podstawach prawnych oraz dokumentach strategicznych, takich jak Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030, który wdraża założenia idei „Wizji Zero". Istotną rolę odgrywają również przepisy krajowe i unijne regulujące zasady ruchu drogowego, wymagania techniczne wobec pojazdów oraz organizację ratownictwa drogowego. Kompleksowe podejście do bezpieczeństwa ruchu drogowego, oparte na współpracy instytucji i skutecznym zarządzaniu, ma na celu systematyczne zmniejszanie liczby wypadków drogowych i ich tragicznych skutków.

Prewencja i kontrola – rola służb publicznych

Zwiększenie liczby uczestników ruchu drogowego, jak również rosnąca liczba pojazdów mechanicznych, stawiają przed administracją publiczną nowe wyzwania w zakresie prewencji wypadków oraz skutecznej kontroli przestrzegania przepisów ruchu drogowego. Kluczową rolę w zapewnianiu bezpieczeństwa odgrywają służby publiczne, takie jak Policja, Inspekcja Transportu Drogowego (ITD), Straż Miejska, oraz administracja lokalna, które podejmują działania prewencyjne oraz kontrolne, mające na celu zminimalizowanie liczby wypadków drogowych.

Prewencja

Prewencja w ruchu drogowym obejmuje szereg działań mających na celu zapobieganie wypadkom i poprawę kultury bezpieczeństwa wśród uczestników ruchu. Jest to proces, który ma na celu zwiększenie świadomości uczestników ruchu drogowego oraz zmianę ich zachowań, co skutkuje mniejszym ryzykiem wypadków. W Polsce kluczową rolę w prewencji odgrywają kampanie edukacyjne prowadzone przez różne instytucje i organizacje. Ministerstwo Infrastruktury oraz Komenda Główna Policji realizują szereg programów edukacyjnych, które mają na celu zwiększenie wiedzy obywateli na temat bezpiecznych zachowań na drogach. Przykładem może być kampania

„Bądź widoczny, bądź bezpieczny", która promuje noszenie odblasków przez pieszych oraz innych uczestników ruchu drogowego. Innym przykładem jest kampania „Zatrzymaj się przed torami, nie ryzykuj", która nawołuje do przestrzegania zasad bezpiecznego przejeżdżania przez tory kolejowe. Edukacja skierowana jest do różnych grup wiekowych i zawodowych. Szczególną uwagę zwraca się na młodych kierowców oraz dzieci, którzy są najbardziej narażeni na wypadki.

Kontrola przestrzegania przepisów

Kolejnym ważnym elementem działań na rzecz bezpieczeństwa w ruchu drogowym jest skuteczna kontrola przestrzegania przepisów przez uczestników ruchu. Działania kontrolne prowadzone są przez służby porządkowe, w tym Policję oraz Inspekcję Transportu Drogowego, a ich celem jest egzekwowanie prawa i zapobieganie niebezpiecznym sytuacjom na drodze.

Policja odgrywa kluczową rolę w kontrolowaniu przestrzegania przepisów drogowych. Codzienne kontrole trzeźwości kierowców, sprawdzanie stanu technicznego pojazdów oraz nadzorowanie przestrzegania przepisów dotyczących prędkości są podstawowymi działaniami profilaktycznymi, które mają na celu eliminowanie zagrożeń związanych z nieodpowiedzialnym zachowaniem uczestników ruchu drogowego.

Inspekcja Transportu Drogowego (ITD) zajmuje się kontrolą pojazdów transportu publicznego, w tym transportu towarów. Kontroluje stan techniczny pojazdów, przestrzeganie norm dotyczących czasu pracy kierowców oraz przestrzeganie przepisów związanych z transportem. Dzięki tym działaniom można zapobiegać wypadkom związanym z awariami technicznymi pojazdów czy zmęczeniem kierowców[23].

Rola służb publicznych w poprawie bezpieczeństwa

Służby publiczne, takie jak Policja, Straż Miejska, Inspekcja Transportu Drogowego oraz administracja lokalna, odgrywają nieocenioną rolę w poprawie bezpieczeństwa na drogach. Ich działania prewencyjne oraz kontrolne mają na celu nie tylko egzekwowanie prawa, ale również zapewnienie skutecznego

[23] *Zadania Inspekcji Transportu Drogowego*, GITD, https://www.gov.pl/web/gitd/zadania-inspekcji-transportu-drogowego, [dostęp: 04.05.2025].

monitorowania i poprawy infrastruktury drogowej. Policja jako główny organ odpowiedzialny za egzekwowanie przepisów ruchu drogowego, prowadzi akcje kontrolne, interweniuje w przypadku wykroczeń drogowych oraz organizuje działania prewencyjne. Straż Miejska w miastach również pełni rolę w zakresie kontroli przestrzegania przepisów ruchu drogowego, zwłaszcza w miastach, gdzie monitoruje m.in. parkowanie, prędkość czy przestrzeganie zasad dotyczących pieszych. Dodatkowo, administracja lokalna, na poziomie gminy, odpowiada za poprawę infrastruktury drogowej, w tym budowę nowych świateł, oznakowania czy organizowanie remontów dróg. Samorządy lokalne mają także możliwość wpływania na lokalne przepisy dotyczące ruchu drogowego oraz organizowania działań edukacyjnych i prewencyjnych.

Edukacja i kampanie społeczne

Bezpieczeństwo w ruchu drogowym jest jednym z kluczowych elementów zapewnienia ochrony życia i zdrowia uczestników ruchu. Edukacja oraz kampanie społeczne odgrywają znaczącą rolę w kształtowaniu postaw i świadomości zarówno kierowców, jak i pieszych. Ich celem jest promowanie odpowiedzialnych zachowań na drogach oraz podnoszenie świadomości na temat zagrożeń wynikających z nieprzestrzegania przepisów. Kampanie społeczne, takie jak: „Bezpieczny przejazd – Szlaban na ryzyko!" czy: „Prowadzisz? Nie pij!", skutecznie zwracają uwagę na istotne problemy i zagrożenia na drogach. Działania te są wspierane przez instytucje państwowe, takie jak Policja, Generalna Dyrekcja Dróg Krajowych i Autostrad (GDDKiA) oraz organizacje pozarządowe. Przeprowadzane są także programy edukacyjne w szkołach, które mają na celu uświadamianie młodzieży o odpowiedzialnym uczestnictwie w ruchu drogowym.

Ważnym elementem działań edukacyjnych jest również organizacja warsztatów i szkoleń dla kierowców, w tym szczególnie młodych uczestników ruchu drogowego. Programy, takie jak „Młody Kierowca" czy szkolenia z zakresu pierwszej pomocy, uczą prawidłowego reagowania w sytuacjach kryzysowych. Dzięki współpracy z Policją oraz organizacjami motoryzacyjnymi, młodzi kierowcy mają możliwość zdobywania wiedzy teoretycznej oraz praktycznej, co znacząco wpływa na poprawę bezpieczeństwa na drogach.
Według danych Komendy Głównej Policji, kampanie społeczne w znacznym stopniu przyczyniają się do zmniejszenia liczby wypadków drogowych,

zwłaszcza wśród młodych kierowców oraz pieszych[24]. Statystyki wykazują, że działania edukacyjne i kampanie społeczne obniżyły liczbę wypadków o 15% w ciągu ostatnich pięciu lat[25].
Ponadto, w ramach kampanii społecznych promowane są nowe technologie wspierające bezpieczeństwo, takie jak aplikacje mobilne ostrzegające o niebezpieczeństwach na drodze czy systemy monitorowania prędkości w strefach zamieszkania. Dzięki takim działaniom świadomość kierowców stale rośnie, a drogi stają się bezpieczniejsze.

Nowoczesne technologie w służbie bezpieczeństwa

W ostatnich latach dynamiczny rozwój technologii przyczynił się do poprawy bezpieczeństwa na drogach. Nowoczesne systemy wspomagania kierowcy (ADAS), takie jak automatyczne hamowanie awaryjne (AEB), systemy monitorowania martwego pola (BSM) czy asystenci pasa ruchu (LKA), stały się standardem w nowoczesnych pojazdach. Technologie te nie tylko zwiększają komfort jazdy, ale przede wszystkim minimalizują ryzyko kolizji i wypadków[26].

W Polsce prowadzone są także prace nad wdrażaniem systemów ITS (Inteligentne Systemy Transportowe), które umożliwiają monitorowanie i zarządzanie ruchem w czasie rzeczywistym. Przykładem może być system ViaTOLL, który nie tylko obsługuje pobór opłat, ale również gromadzi dane o ruchu drogowym[27].

Kolejnym przykładem nowoczesnych rozwiązań jest rozwój infrastruktury drogowej, w tym inteligentnych sygnalizacji świetlnych oraz systemów wykrywających niebezpieczne zachowania na przejściach dla pieszych. Inteligentne przejścia dla pieszych wyposażone w czujniki ruchu oraz oświetlenie

[24] *Wypadki drogowe w 2024 roku*, Komenda Główna Polski, https://statystyka.policja.pl/st/ruch-drogowy/76562,Wypadki-drogowe-raporty-roczne.html, [dostęp: 11.05.2025].

[25] *Strategia Zrównoważonego Rozwoju Transportu do 2030 roku*, 24 września 2019 r., Ministerstwo Infrastruktury, https://www.gov.pl/web/infrastruktura/projekt-strategii-zrownowazonego-rozwoju-transportu-do-2030-roku2, [dostęp: 11.05.2025].

[26] *Systemy wspomagania ADAS – dlaczego kalibracja wpływa na bezpieczeństwo?*, https://qservicecastrol.eu/blog-systemy-wspomagania-adas-dlaczego-kalibracja-wplywa-na-bezpieczenstwo/, [dostęp: 11.05.2025].

[27] *Co to jest ITS?*, GDDKIA, https://drogi.gddkia.gov.pl/serwisy-gddkia/krajowy-system-zarzadzania-ruchem/zalozenia-kszr/co-to-jest-its, [dostęp: 11.05.2025].

LED reagują na obecność pieszych, zwiększając tym samym ich widoczność i bezpieczeństwo.

Wprowadzenie technologii V2X (Vehicle to Everything) umożliwia komunikację pojazdów z infrastrukturą drogową oraz innymi uczestnikami ruchu. Rozwiązania te pozwalają na automatyczne ostrzeganie o zagrożeniach, np. o nagłym hamowaniu pojazdu znajdującego się przed nami. Technologia ta testowana jest obecnie na polskich autostradach, gdzie wykazuje dużą skuteczność w zapobieganiu kolizjom[28].

Dodatkowo, technologie takie jak drony do monitorowania ruchu, systemy wykrywania kolizji oparte na AI oraz autonomiczne pojazdy zyskują na znaczeniu w kontekście poprawy bezpieczeństwa drogowego.

Podsumowanie

Bezpieczeństwo ruchu drogowego w Polsce to istotny obszar polityki państwa, mający na celu ochronę życia i zdrowia uczestników ruchu – kierowców, pieszych, rowerzystów i innych. Mimo rosnącej świadomości, każdego roku na polskich drogach giną tysiące osób, a setki tysięcy odnoszą obrażenia. Główne przyczyny wypadków to nadmierna prędkość, alkohol, nieuwaga, zmęczenie oraz niewłaściwe korzystanie z pasów i urządzeń ochronnych.

Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030, oparty na koncepcji „Wizji Zero", zakłada kompleksowe działania w pięciu kluczowych obszarach: zarządzaniu bezpieczeństwem, edukacji uczestników ruchu, infrastrukturze drogowej, stanie technicznym pojazdów oraz ratownictwie i opiece powypadkowej. Wdrażanie programu wspierane jest przez akty prawne i strategie krajowe oraz unijne.

Kluczową rolę w prewencji i kontroli odgrywają służby publiczne, takie jak Policja, ITD, Straż Miejska i administracja lokalna. Ich działania obejmują zarówno kontrole drogowe, jak i kampanie edukacyjne oraz poprawę infrastruktury. Ważnym elementem prewencji są również działania edukacyjne i kampanie społeczne, które wpływają na postawy uczestników ruchu drogowego, zwłaszcza młodzieży i młodych kierowców.

[28] *Znaczenie nowoczesnych technologii w poprawie bezpieczeństwa drogowego*, 19.02.2025 r., https://chromathoughts.pl/znaczenie-nowoczesnych-technologii-w-poprawie-bezpieczenstwa-drogowego/, [dostęp: 11.05.2025].

Literatura

1. *Fotelik samochodowy kontra poduszka powietrzna w samochodzie*, https://fotelik.info.pl/fotelik-samochodowy-kontra-poduszka-powietrzna-w-samochodzie.
2. Generalna Dyrekcja Dróg Krajowych i Autostrad, https://drogi.gddkia.gov.pl/serwisy-gddkia/krajowy-system-zarzadzania-ruchem/zalozenia-kszr/co-to-jest-its.
3. GITD, https://www.gov.pl/web/gitd/zadania-inspekcji-transportu-drogowego
4. Komenda Główna Polski, Wypadki drogowe w 2024 roku, https://statystyka.policja.pl/st/ruch-drogowy/76562,Wypadki-drogowe-raporty-roczne.html.
5. Komisja Europejska, *EU Road Safety Policy Framework 2021-2030*, Bruksela 2019.
6. Krajowa Polityka Transportowa do 2030 roku, Ministerstwo Infrastruktury, Warszawa 2019.
7. Ministerstwo Infrastruktury, https://www.gov.pl/web/infrastruktura/projekt-strategii-zrownowazonego-rozwoju-transportu-do-2030-roku2.
8. Narodowy Program Bezpieczeństwa Ruchu Drogowego 2021-2030, Krajowa Rada Bezpieczeństwa Ruchu Drogowego, Warszawa 2021.
9. Policja, https://www.policja.pl/pol/aktualnosci/255080,Bezpieczenstwo-na-polskich-drogach-to-priorytet.html.
10. Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2020 r. w sprawie homologacji pojazdów (Dz.U. 2020 poz. 2412).
11. Rozporządzenie Ministra Infrastruktury z dnia 3 lipca 2003 r. w sprawie szczegółowych warunków technicznych dla znaków i sygnałów drogowych oraz urządzeń bezpieczeństwa ruchu drogowego i warunków ich umieszczania na drogach (Dz.U. 2003 nr 220 poz. 2181).
12. Rozporządzenie Ministra Infrastruktury z dnia 31 grudnia 2002 r. w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia (Dz.U. 2003 nr 32 poz. 262, z późn. zm.).
13. *Systemy wspomagania ADAS – dlaczego kalibracja wpływa na bezpieczeństwo?*, https://qservicecastrol.eu/blog-systemy-wspomagania-adas-dlaczego-kalibracja-wplywa-na-bezpieczenstwo/.
14. Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz.U. 1997 nr 98 poz. 602, z późn. zm.).
15. Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz.U. 1971 nr 12 poz. 114, z późn. zm.)
16. Ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz.U. 2011 nr 30 poz. 151, z późn. zm.).
17. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997 nr 88 poz. 553, z późn. zm.).
18. Ustawa z dnia 6 września 2001 r. o transporcie drogowym (Dz.U. 2001 nr 125 poz. 1371, z późn. zm.).
19. *Znaczenie nowoczesnych technologii w poprawie bezpieczeństwa drogowego*, 19.02.2025 r., https://chromathoughts.pl/znaczenie-nowoczesnych-technologii-w-poprawie-bezpieczenstwa-drogowego/.

Serhii S. Miamlin, PhD
Ukrainian State University of Science and Technology (Dnipro, Ukraine)
ORCID: 0000-0002-9204-4435

https://doi.org/10.29316/9788368103205_20

CREATION OF MODERN DESIGNS OF HOPPER CARS FOR GRAIN TRANSPORTATION TAKING INTO ACCOUNT SAFETY REQUIREMENTS

Summary

The agricultural sector of Ukraine is a strategically important part of the economy, particularly the production and export of grain crops, which ensure food security and contribute significantly to the country's economic development. One of the main areas of development is the improvement of the logistics infrastructure, including storage systems, transport chains, and port facilities. Grain storage and transportation are critical stages in the export process, as most of the grain is exported through Ukraine's seaports. However, the growing volumes of grain production and increasing transportation demands necessitate the modernization of transport vehicles, particularly grain cars. The analysis shows that due to the aging fleet of grain cars in Ukraine and the increasing transportation needs, it is essential to improve the design of hopper cars, taking into account modern technical solutions and innovative machine-building technologies. The development of a new generation of grain cars is an urgent scientific and practical task for Ukraine's transport infrastructure and the global grain transportation market.

Keywords: agro-industrial complex, grain transportation, logistics, infrastructure, railway hopper cars

Introduction

The agricultural sector of the economy is a strategic and promising area of development of the national economy and many European countries. Cereal crops and products made from them have always been liquid, as the food supply and security of the state are based on them. The natural and climatic conditions of Ukraine and the developed agro-industrial complex of Great Britain ensure high productivity and promote the cultivation of all grain crops and make it possible to obtain high-quality food grain in volumes sufficient to meet domestic needs and build export potential[1].

Therefore, the grain sector is one of the most important branches of agriculture. In recent years, Ukraine has taken the leading positions in the production and export of grain crops among the countries of the world. Of course, the export of grain is not a simple procedure and it involves many related industries, one of which is the storage and transportation of grain, because it is collected in a fairly short period of time. In 2017, the total crop yield, according to[2], amounted to almost 62 million tons. Consequently, it is urgent to improve the infrastructure that would provide all logistics and sufficient volumes of transportation, most of which goes for export.

The logistics infrastructure that ensures the export of grain has three main segments: the storage system, transport chains and port facilities. The grain storage system in Ukraine is represented by grain warehouses of agricultural producers, linear and transfer harvesting and commercial elevators, terminal containers, and elevators of processing enterprises. It is worth inoting that over the past ten years, the grain storage system in Ukraine has undergone significant changes, primarily related to the privatization of the bread industry, the increase in the production of grain and oil crops, and the sharp increase in their export. Thus, while in 2001 the total volume of one-time storage of grain crops was 28 million tons, in the pre-war period the system of grain storage in Ukraine was represented by more than 870 grain warehouses with a total volume of one-time storage of more than 45 million tons.

More than 90% of Ukrainian grain exports go through sea ports. In Ukraine, transshipment of export and transit grain cargoes is carried out in

[1] APK-Inform, *Analysis of grain logistics in Ukraine and proposals for its modernization* (p. 88). APK-Inform Information Agency 2013.

[2] D. M. Baranovskyi, *The problem of aging and wear of freight wagons*. Vagonny Park, 7-8, 112-113, 2016.

the water areas of such sea trade ports as Illichivskyi, Odeskyi, Pivdennyi, Mykolaivskyi, Khersonskyi. Currently, in Ukraine a significant volume of grain transshipment is carried out through non-state terminals, among which the largest are Transinvestservis LLC, Nibulon LLC, etc. The unique position of Ukrainian ports and their proximity to mo st key markets (the Middle East, North Africa, Europe) significantly increase the competitiveness of these ports, despite the efforts of other countries to develop their own port capacities.

In general, in Ukraine, the system of storing grain and ensuring its transshipment in ports is entering the phase of development and orientation to market requirements. In this regard, commercial elevators and port containers are actively developing. The key figures in the grain storage development segment are agricultural holdings and multinational companies that have sufficient investment funds to support modernization and construction projects.

However, the most important component of the logistics infrastructure that ensures the export of grain is transportation. Grain is delivered to seaports by rail (about 61% of exports), road (about 36%) and water transport (about 3%). Thus, the main flows of grain to ports for export transshipment are provided by railway transport[3].

Despite the growth in grain production, the share of rail transport in grain transportation is decreasing. At the same time, the volume of grain transportation by road is increasing. One of the reasons for this situation is the shortage of hopper cars (grain cars). This problem is especially acute during periods of peak grain transportation (from September to December), when the daily load reaches up to 100,000 tons. It is worth mentioning that in the coming years, with the growth of grain production, the problem of shortage of grain cars will increase. This is due to significant moral and physical wear and tear of cars, which reaches more than 90%. Thus, the average age of grain cars in Ukrainian rolling stock is about 28 years (with a standard service life of 30 years)[4]. Therefore, the direction of research related to the improvement of rolling stock designs for the transportation of grain is a topical scientific and applied problem for railway transport and transport engineering.

[3] Center for Transport Strategies, *Agrologistics in Ukraine: Analytical research* (p. 56), Kyiv 2016.

[4] Delo.ua, *Russia destroyed more than 15% of grain storage facilities in Ukraine: how farmers will store the 2022 harvest*, 2022.

Grain transport market overview in Ukraine analysis of logistics on the grain market in Ukraine

Let's consider the infrastructural component of grain transportation in Ukraine. The capacity of certified grain warehouses (Figure 1) at the beginning of 2023 was 32 million tons, and about 10-12 million tons go to non-certified warehouses. The total number of certified warehouses is about 740, of which only 620 elevators have rail connections. And the growth of grain production reveals a deficit of storage capacities of about 18-20 million tons[5],[6],[7]. Unfortunately, it is currently difficult to determine the exact number due to a significant number of damaged and destroyed elevators as a result of hostilities by Russian troops. The US State Department, with reference to the research of the non-governmental organization Conflict Observatory, stated that due to the constant shelling of the Russian troops on the territory of Ukraine, more than 15% of granaries were lost or damaged. Thus, due to the military aggression of the Russian Federation in Ukraine, every sixth granary out of the total volume of grain enterprises was damaged, and 75 objects out of the 344 examined are damaged[8].

Figure 1. Modern grain elevator
Source: ooo-avg.ru.

[5] Elevatorist, *Main elevator site*.
[6] Elevatorist, *Map of elevators in Ukraine*.
[7] Elevatorist, *The working fleet of grain wagons in Ukraine is shrinking.*
[8] FAO., *Crop Prospects and Food Situation: Quarterly Global Report No. 1*. Rome 2023.

In addition to traditional elevator complexes, special sleeve bags are also used for temporary grain storage (Figure 2). This allows for temporary storage and preservation of grain in field conditions.

Figure 2. Temporary grain storage technology in the field
Source: liliani.ru.

The port component of the infrastructure is 44 million tons per year in the nominal capacity of the ports for grain transshipment, but if we do not take into account idle ports, the maximum volume of transshipment will be 39 million tons, with an average capacity utilization factor of 67%.Separate port loading ranges from 65% to 100%[9].

Road transportation accounts for the major part of grain transportation, due to the initial collection for storage in the volume of the harvested crop. Road transport will also play a significant role in the grain transportation to the final consumer – more than 12 million tons. From the point of view of use profitability, the delivery of grain to seaports by motor vehicles is profitable at distances of up to 200 km, but in peak periods truck carriers are involved in longer distances. However, there are some issues when it comes to transporting grain by road, for example:

- high relative cost compared to the railway,
- poor condition of roads,
- high depreciation costs for trucks,
- accumulation of trucks in ports and their entrances during peak periods.

[9] Greenbrier Europe, *Product catalog: Hopper cars.*

In addition to the above-mentioned problems, since May 2016, the "State Transport Safety Service of Ukraine" has tightened weight control on the roads. Such measures increased the cost of delivery by 60-100%. As a result, part of the cargo was transferred to the railway. Therefore, the demand for hopper cars for grain transportation has increased significantly[10].

The railway component of the infrastructure currently allows for the export of up to 30 million tons of grain. The total fleet of hopper cars is 32,309 units, according to data as of 05/10/2023[11]. The possibilities of railway transportation are most often used when sending grain over long distances both within the country and abroad. Transportation by railway makes up 40% of the total amount of import deliveries of grain crops of Ukraine.

The method of grain delivery using railway facilities is characterized by a high degree of reliability, convenience, and speed. Almost all elevators, granaries and mills are located very close to railway junctions. The larger ones have their own sections of the track, which are used to move goods in cars[12].

However, there are significant limitations as well. For example, the working fleet of cars is already at the limit of its capabilities, and later the situation will intensify, taking into account the prospects of the further growth of grain cultivation, up to 90 million tons per year. Again, we should not forget about the aging of the rolling stock and its subsequent removal from the working fleet and decommissioning. In the previous few years, about 4,000 grain trucks were supposed to be decommissioned, but the introduction of amendments to the Procedure for extending the service life of freight cars made it possible to slightly change the overall picture of rolling stock for cargo transportation. Some of the cars received an extension of their service life. The term "useful life" is sometimes used to indicate the operation of a car after the service life appointed by the manufacturer. Most of the grain cars were put into operation

[10] A. V. Kupchenko, *Elevator capacities of Ukraine*. Grain Storage and Processing, (7), 33-37, 2014.

[11] S. S. Myamlin, *Creation and modernization of rolling stock for grain transportation by rail.* In 76th International Scientific and Practical Conference Problems and Prospects for the Development of Railway Transport (p. 44-45), Dnipro 2016.

[12] S. S. Myamlin, *Creation of technical means for grain transportation by rail*. In 77th International Scientific and Practical Conference Problems and Prospects for the Development of Railway Transport (p. 63-64), Dnipro 2017.

in a short period of time, about 30 years ago. The average age of the domestic fleet of hopper cars is 28 years, with a standard service life of 30 years[13, 14].

In addition, there are problems with the capacity of railway approaches to ports. In most cases, the infrastructure has not got any significant investment in the last thirty years. Therefore, port infrastructure is a restraining factor for increasing the transshipment capacity of ports. This is also a limiting factor in increasing the productivity of freight cars.

Moreover, due to difficulties with rolling stock, the railway cannot form warehouses with monoloads, which creates queues and significantly slows down the process of delivering cargo to ports. Due to untimely delivery, shippers suffer losses: vessels are idle, which is additional costs. Therefore, other technical and technological possibilities of railway transport should be considered in order to increase the volume of grain transportation. Next, we will consider the structure of the working fleet of hopper cars for grain transportation in Ukraine.

Analysis of logistics on the grain market in Ukraine

According to the statistical data, the working fleet of hopper cars on the railways of Ukraine includes 32,309 cars. The quantitative composition of the hopper cars by model is presented in Table 1.

Table 1. Information on the available models of hopper cars on the railways of Ukraine

Hopper car model	Number
Total	**32309**
11-739	1760
19-3054	382
19-4109-01	814
19-4146	2134
19-4146-01	694
19-4152	15

[13] S. S. Myamlin, *Development of modern freight wagon designs for trans-European transportation*. In 2nd International Scientific and Technical Conference "Advanced Technologies of Transport Means" (p. 72-74), Kharkiv 2014.

[14] S. S. Myamlin, *Mathematical modeling of spatial oscillations of railway rolling stock*. In International Scientific and Technical Conference "Information Technologies in Metallurgy and Mechanical Engineering" (p. 320-323), 2024.

Hopper car model	Number
19-6869	2311
19-6938	3
19-752	17157
19-7053-02	5765
19-970	350
19-970-01	300
19-9951	291
19-9950	130
19-9870-01	1
19-9945	65
19-923-07	9
19-9549	8
19-7053-03	120

Source: own study.

According to Table 1, 19-752 model prevails among the hopper cars used for grain transportation, which is 53% of their total number. This indicates the demand for this model among grain carriers.

The main operational indicators of hopper cars are shown in Table 2. It is worth mentioning that the shortage of hopper cars for grain transportation is 2,600 cars per day, which once again emphasizes the relevance of research related to the improvement of the designs of hopper cars for grain transportation.

Table 2. The main indicators of the operation of hopper cars as of 2023

№	The name of the indicator	Indicator
1	The average age of the cars	28 years old
2	A share in the rolling stock	11%
3	Stock shortage	2600 cars
4	The average time of circulation by Ukrzaliznytsia	13 days
5	Loading share	11%
6	Objective rental rate	UAH 3850 without VAT per day

Source: own study.

Undoubtedly, the deficit of the car fleet can be reduced by reducing the turnover time of cars, but this indicator cannot be significantly reduced without

improving the technical and economic indicators of the car and without significantly improving the technology of transportation on railways.

In recent years, the ratio of the number of cars by form of ownership has significantly changed in the direction of an increase in the number of cars owned by private operating companies compared to the fleet of hopper cars owned by the JSC Ukrainian railway (hereinafter UR). Figure 3 presents a diagram of the ratio of the fleet of hopper cars by ownership. According to the diagram in Figure 3 UR owns 11,658 hopper cars for grain transportation, which is 36%, and operator companies own 20,651, which is 64% of grain transportation hopper cars. The tendency to increase the fleet of hopper cars of private companies is increasing, both due to the purchase of new cars and the purchase of cars whose useful life has been extended.

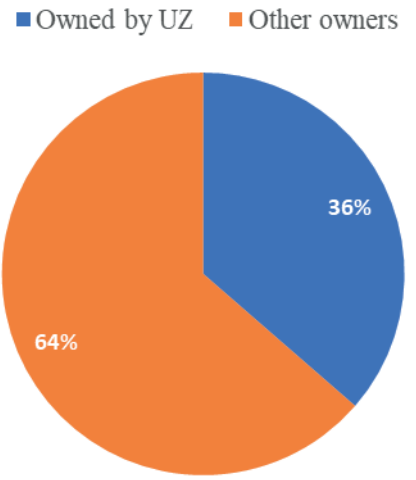


Figure 3. Comparison of the hopper cars number by ownership %
Source: own study.

As can be seen from Table 3, the main technical and economic indicators of hopper cars used on the railways of Ukraine for the transportation of grain are given.

Table 3. Information on available models of hopper cars on Ukrainian railways

№	Model code	Load capacity, t	Minimum tare, t	Maximum tare, t	Length, over couplers, mm	Axle load, t	Volume, m3	Year		Standard term of service, years	Loading gauge
								Year of production start	End of production year		
1	11-739	65	21,3	22,7	14720	21,93	93	1975	1982	30	1-VM
2	19-3054	71	22,3	23	14720	23,5	94	1993	0	30	1-VM
3	19-4109-01	70	22,3	23,7	14720	23,43	94	2003	2010	30	1-VM
4	19-752	70	21,3	23	14720	23,25	94	1982	0	30	1-VM
5	19-752	70	21,3	23,5	14720	23,38	94	1975	1987	30	1-VM
6	19-7016	69,5	23	24,4	14720	23,48	108	2004	2004	30	1-T
7	19-7016	70,2	23,2	23,8	14720	23,5	108	2005	0	30	1-T
8	19-3116-01	70	22,6	24	13870	23,5	96,5	2007	0	30	1-T
9	19-7017-03	71	22	23	13720	23,5	91	2008	0	30	1-T
10	19-7017-04	71	22	23	13720	23,5	87	2008	0	30	1-T
11	19-3054-04	70,5	22,1	23,5	14720	23,5	112	2009	0	30	1-T
12	19-4109-01	70,3	22,3	23,7	14720	23,5	94	2010	2018	30	1-VM
13	19-9871	70,5	22,5	23,5	13920	23,5	96	2010	0	30	1-T
14	19-9814	70	23	24	14220	23,5	104	2010	0	30	1-T
15	19-7016-01	70,2	23,2	23,8	14720	23,5	108	2011	0	30	1-T
16	19-9882	70	23	24	14720	23,5	94	2011	0	30	1-VM
17	19-7053-01	70,5	22,5	23,5	14720	23,5	116	2011	0	30	1-T
18	19-7017-06	71	22	23	13720	23,5	96	2011	0	30	1-T
19	19-7053-02	70,5	22,5	23,5	14720	23,5	116	2011	0	30	1-T
20	19-9863	70	23	24	14720	23,5	94	2011	0	30	1-VM
21	19-4146	69,5	23,8	24,5	14720	23,5	116	2012	2020	30	1-T

№	Model code	Load capacity, t	Minimum tare, t	Maxi-mum tare, t	Length, over couplers, mm	Axle load, t	Volume, m3	Year		Standard term of service, years	Loading gauge
								Year of produc-tion start	End of produc-tion year		
22	19-970	70,8	21,8	23,2	14720	23,5	100	2012	0	30	1-T
23	19-970-01	70,5	22,1	23,5	14720	23,5	110	2012	0	30	1-T
24	19-1761-03	70,5	22,1	23,5	14720	23,5	112,5	2012	0	30	1-T
25	19-9951	70	23	24	14720	23,5	104	2013	0	30	1-T
26	19-9835-02	71	22,2	23	14720	23,5	101	2013	0	30	1-T
27	19-9835-03	71	22,2	23	14720	23,5	101	2013	0	32	1-T
28	19-9950	70,5	22,5	23,5	14720	23,5	105	2013	0	30	1-T
29	19-9858	70,3	23,2	23,7	14520	23,5	108	2013	0	30	1-T
30	19-9870-01	76,5	22,5	23,5	14720	25	101	2013	0	32	1-T
31	19-9945	70,5	22,5	23,5	14720	23,5	100	2014	0	30	1-T
32	19-923-07	70	22	23	13200	23,25	81	1979	0	26	1-T
33	19-6869	70,5	23	23,5	14720	23,5	120	2014	0	30	1-T
34	19-6870	76,2	23,3	23,8	14720	25	120	2015	2018	32	1-T
35	19-3058	70,5	22,5	23,5	14720	23,5	118	2015	0	30	1-T
36	19-9549	76	23	24	14720	25	120	2015	0	32	1-T
37	19-6870	76,2	23,3	23,8	14720	25	120	2015	2018	32	1-T
38	19-7053	76	23	24	14720	25	116	2015	0	30	1-T
39	19-6870	76,2	23,3	23,8	14720	25	120	2015	2018	32	1-T
40	19-6869	70,5	23	23,5	14720	23,5	120	2017	0	30	1-T
41	19-9549-02	77	22	23	14720	25	120	2017	0	30	1-T
42	19-4152	71,5	22,2	22,5	14720	23,5	133	2018	0	30	1-T

№	Model code	Load capacity, t	Minimum tare, t	Maximum tare, t	Length, over couplers, mm	Axle load, t	Volume, m3	Year		Standard term of service, years	Loading gauge
								Year of production start	End of production year		
43	19-9549-01	76	23	24	14720	25	126	2018	0	40	1-T
44	19-9549-04	76	23	24	14720	25	120	2018	0	32	1-T
45	19-6870	76	23,3	24	14720	25	120	2019	0	32	1-T
46	19-6870	76	23,3	24	14720	25	120	2019	0	32	1-T
47	19-6870	76	23,3	24	14720	25	120	2019	0	32	1-T
48	19-6938	70	23	24	14720	23,5	120	2019	0	30	1-T
49	19-7053-03	71	22	23	14720	23,5	124	2018	0	30	1-T
50	19-7053-04	76,5	22,5	23,5	14720	25	124	2018	0	32	1-T
51	19-1259	76	23	24	14720	25	127	2018	0	30	1-T
52	19-1259-01	76	23	24	14720	25	127	2018	0	30	1-T
53	19-6943	69,5	23,5	24,5	14720	23,5	120	2018	0	30	1-T
54	19-4109-01	70,3	22,3	23,7	14720	23,5	94	2019	0	30	1-VM
55	19-9567	71,5	21,8	22,5	14720	23,5	118	2018	0	30	1-T
56	19-1273-01	77	22	23	14220	25	107	2019	0	30	1-T
57	19-1274-01	71	22	23	14220	23,5	107	2019	0	30	1-T
58	19-6978	113,5	35,1	36,5	19380	25	160	2019	0	40	1-T
59	19-4146	69,5	23,8	24,5	14720	23,5	116	2020	0	30	1-T
60	19-4146-01	71,5	22	22,5	14720	23,5	126	2020	0	30	1-T
61	19-3058	70,5	22,5	23,5	14720	23,5	118	2020	0	30	1-T
62	19-641	69,5	23	24	14720	23,5	114	2020	0	30	1-T
63	19-3058	70,5	22,5	23,5	14720	23,5	118	2021	0	30	1-T

Source: own study.

As can be seen from the data in Table 3, the developers offer 63 models of hopper cars for grain transportation, of which 19 are operated on the territory of Ukraine. The rest of the hopper car models are designed as concept models and can potentially be purchased by operating companies for the transportation of grain, but at the moment exist in the form of prototypes that have passed the necessary set of acceptance tests and are ready for serial production in case of receiving orders from businesses. The analysis of the main technical characteristics of hoppers developed in Ukraine for transporting grain shows that the carrying capacity is in the range of 65-77 tons, the weight of the tare varies from 22 to 24.4, almost all models have a length along the coupling axes of 14720 mm, which is related to the parameters terminals for loading and unloading cars. The body volume of models developed before the 2000s does not exceed 94 m^3. Car models developed after 2000 generally have a body volume exceeding 100 m^3, and in recent years they are trying to make the body volume in the range of 116-126 m^3. The axle load is generally in the range of 23.5-25 tons. Separately, the car model 19-6978 should be singled out, which has a carrying capacity of 113.5 tons, a slightly increased tare weight of 35.1-36.5 tons, while the distance along the coupling axes is 19380 mm, the axle load is 25 tons, the body volume is 160 m^3. The standard service life for almost all cars is generally 30 years, although for some models it is 32 years, and for models 19-9549-01 and 19-6978 it is 40 years.

In this way, the main technical features of the models of hopper cars, which are developed and used on the railways of Ukraine and can be proposed for use on the railways of other countries, have been considered. Taking into account the analysis of the technical characteristics of the models that were developed at the car-building enterprises of Ukraine and are in demand among cargo transportation operators, it is possible to form the technical requirements for a promising hopper model for grain transportation. Next, we will carefully consider the main technical characteristics of a promising model of a hopper car for further development.

Technical requirements for the design of a hopper car for the transportation of grain of a prospective design

A prospective design of a hopper car for grain transportation should take into account the advantages and disadvantages of existing models and be more

reliable. Taking into account the analysis of the design features of the main models of hopper cars, 19-7016, which has the following characteristics listed in Table 4, can be chosen as an analogue.

Table 4. Technical characteristics of the prototype and perspective car

TECHNICAL CHARACTERISTICS		
	19-7016	**Perspective car**
Cargo capacity, t	70,2	71
Body volume, m^3	108	
Tare weight, t	23,8	
Calculated load from wheelset on rail, kN (tf)	230,5 (23,5)	
Car base, mm	10 500	
Car length as per coupling axles, mm	14 720	
Loading gauge	1-T	
Quantity of hatches: - loading - unloading	 4(5) 3	
Design speed, km/h	120	
Inter-repair mileage, km	210 000	500 000
Term of service, years	30	32

Source: own study.

At the same time, it should be taken into account that the main design solutions must be original and not repeat the design of the analog car, despite the fact that the technical characteristics of these cars are similar. In order to determine patent purity, the authors separately performed patent studies to determine the absence of constructive plagiarism and proposed the registration of copyright and protection documents for intellectual property objects related to the main structural solutions of the hopper car for transporting grain, which is being developed in this study. With the participation of the author, original innovative designs of hopper cars for grain transportation were

developed[15,16,17,18,19,20], and research was also carried out on the strength and dynamic qualities of hopper cars for grain transportation and platform wagons for container transportation, including grain containers, taking into account traffic safety requirements[21,22,23,24,25].

Analysis of alternative options of grain transportation by rail transport

The deficit of the hopper car fleet is the second largest among all other types of freight cars and, depending on the season, can range from 1 to 2.4 thousand cars per day during the year. Challenges for railway transport from the business side are also related to the lack of freight cars owned by Ukrainian railway, which carry out export transportation. Therefore, in order to

[15] A. O. Lovska, V. P. Nerubatskyi, S. S. Myamlin, A. O. Plakhtiy, *Situational adaptation of 13-7024 flat wagon model for transportation of strategic goods.* Eastern-European Journal of Enterprise Technologies, 2(7), 38-46, 2024.

[16] A. O. Lovska, V. P. Nerubatskyi, S. S. Myamlin, A. O. Plakhtiy, *Determining the effect of sandwich-type components on the stress state of the universal gondola hatch cover*. Eastern-European Journal of Enterprise Technologies, 1(7), 6-13, 2024.

[17] Perevozki-Kiev, *Grain transportation in Ukraine*. http://перевозки-киев.com/perevozka-zerna-po-ukraine.html

[18] S. V. Panchenko, A. O. Lovska, S. S. Myamlin, A. V. Rybin, M. V. Pavlyuchenkov, *Hopper car with corrugated beams in the load-bearing structure*. Utility Model Patent of Ukraine, 156986, 2024.

[19] S. V. Panchenko, A. O. Lovska, S. S. Myamlin, A. V. Rybin, M. V. Pavlyuchenkov, *Covered hopper car for grain transportation*. Utility Model Patent of Ukraine, 156985, 2024.

[20] S. V. Panchenko, A. O. Lovska, S. S. Myamlin, A. V. Rybin, M. V. Pavlyuchenkov, *Hopper car for grain transportation*. Utility Model Patent of Ukraine, 156984, 2024.

[21] S. V. Panchenko, A. O. Lovska, S. S. Myamlin, A. V. Rybin, M. V. Pavlyuchenkov, *Hopper car with corrugated beams in the load-bearing structure*. Utility Model Patent of Ukraine, 156986, 2024.

[22] S. V. Panchenko, G. L. Vatulia, A. O. Lovska, V. G. Ravlyuk, S. S. Myamlin, *Modernized brake lever transmission of the bogie as a way to ensure the safety of freight trains*. Rail Transport of Ukraine, (4), 10-26, 2024.

[23] R. Sh. Rustamov, *Assessment of prospects for the development of grain logistics in Ukraine*. Colected Scientific Papers of the Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan, (8), 127-133, 2014.

[24] D. Salin, *Ukraine Grain Transportation*. U.S. Department of Agriculture, Agricultural Marketing Service, 2020.

[25] I. Samoylenko, O. Sterniy, V. Nabok, *Wagons, routes. But there's nothing to carry the grain*. Zerno, 2012.

compensate for the shortage of hopper cars, carriers are looking for alternative options for grain transportation by rail. Let us consider some of them[26,27].

An alternative to the production of new hopper cars is the introduction of the latest solutions, for example, the use of containers of standard sizes with certain design changes that would allow grain crops to be transported in them. The production technology of such a container is much simpler than the production of a car, and it can be multi-purposeful. In addition, the unloading of such containers in ports can be performed much faster than the unloading of grain cars, which will contribute to reducing the turnover time of the cars that transport the containers, and the turnover time of the containers themselves. The platforms have sliding fittings, which allows them to be used for transporting both 20-foot and 40-foot containers. The main advantage of containers for grain transportation is the possibility of their transportation not only by railway platforms, but also by road and sea transport, which can significantly improve the entire grain transportation infrastructure as a whole.

A grain container must have a hatch in the roof for its loading and a device for unloading at the lowest point of the floor. At the same time, the shape of the container, in which grain is supposed to be transported, should be rounded to prevent the appearance of cargo residues.

Technical characteristics of the container are given in Table 5.

[26] A. O. Lovska, V. P. Nerubatskyi, S. S. Myamlin, A. O. Plakhtiy, *Situational adaptation of 13-7024 flat wagon model for transportation of strategic goods*. Eastern-European Journal of Enterprise Technologies, 2(7), 38-46, 2024.

[27] A. O. Lovska, V. P. Nerubatskyi, S. S. Myamlin, A. O. Plakhtiy, *Determining the effect of sandwich-type components on the stress state of the universal gondola hatch cover*. Eastern-European Journal of Enterprise Technologies, 1(7), 6-13, 2024.

Table 5. Technical characteristics of a 20-foot container for grain transportation

Characteristics	Data
1. Tank capacity, litre	28300
2. Weight of empty container (tare), kg	4200
3. Filling volume (with a coefficient of 0.8), litre	22640
4. Useful weight, kg (with a unit weight of 0.8 kg/m3)	22600
5. Maximum gross weight, kg	26800
6. Dimensions in accordance with ISO668:1195 1CC	
Length, mm	6058±6
Width, mm	2438±5
Height, mm	1591±5
The distance between the centers of fitting holes	
lengthwise, mm	5853±3
widthwise, mm	2259±3
7. Operating temperature range, ºC	-40…+50
8. Corner fittings in accordance with the requirements	ISO 1161:1984
9. The size of the hatch located on top, mm	1188 x 600
10. The hatch for unloading located at the bottom on the side, mm	500
11. Service ladders, number	4
12. Stairs	outside and inside
13. Vent hole	available

Source: own study.

The main disadvantage of the container presented in Table 5 is an underutilization of the useful volume according to the dimensions of the container. This negative factor can be avoided by extending the side walls of the grain container to the upper strapping of the container.

The design of the container allows increasing the usable volume of the grain container from 20,000 litres to 28,300 by raising the side and end walls for a standard 20-foot container.

To exploit all the useful volume of the container, it is possible to use end doors in its design for the possibility of unloading. Roof hatches can be provided for loading such containers or the entire roof can be completely sliding, which will significantly speed up the process of loading grain crops into the container.

The are capable of increasing the useful volume up to 34,500 litres for the dimensions of a standard 20-foot container. Another advantage of this type of grain container is that, in addition to grain, they can transport artificial

cargo, which can significantly reduce the empty mileage of the container and the fitting platform for its transportation. Thus, it is possible to transport grain from the elevator to the port, and artificial cargo brought to the port in the reverse direction.

Also, grain in containers can be transported in bulk using a hard wall, a transport liner (LINER-BAG) or using soft container-bags (BIG-BAG). By the way, container-bags can also be transported by semi-cars.

Also the method of transporting grain by semi-cars with external attachment of the shelter is used. However, this is a forced measure and it is supposed to be abandoned in the future.

There are several reasons for this, namely: this way of placing the cargo or securing the shelter caused traffic safety threats, and the transportation of grain in an open mobile warehouse poses many risks, including grain spoilage, theft, increased time for technological operations, safety risks etc.

All of the above-mentioned alternative methods of transporting grain by rail transport are promising, but there are some issues. The main thing is how well-preserved the grain transported will be. Moreover, attention should be paid to how long it is stored in a closed container, whether it is ventilated, etc. In addition, the entire basic infrastructure is adapted specifically to hopper cars. Therefore, it is suggested to consider solving the problems of grain transportation by rail precisely by improving the hopper car design.

Analysis of the worldwide agriculture market

Before proceeding to consider the global market for hopper cars, it makes sense to first analyze the volume of the agricultural market. Agricultural season 2022–2023 is coming to an end, and Food and Agriculture Organization of the United Nation (FAO)[28] estimates that global cereal production fell by 1.0 percent year-on-year in 2022, mainly as a result of a decline in maize production and, to a lesser extent, growth in sorghum. Cereal consumption is expected to decline by 0.9 percent between 2022 and 2023, driven primarily by lower consumption of coarse grains and rice, as well as unhealthy and unhealthy consumption of other staple grains; at the same time, there is an increase in consumption for food purposes. Forecasts for age, cereal production as a result of

[28] State Statistics Service of Ukraine.

exceeding consumption, and, as received, cereal stocks at the end of the 2023 season are significant (0.2 percent), exceeding those of the beginning of the season: the increase in stocks of wheat and barley is likely to more than offset the incidence of stocks corn, rice and sorghum. Trading volume in 2022-2023 season may fall by 2.3 percent from growth in 2021-2022, with this high trade volume expected to affect all major cereals except wheat.

For the 2023-2024 season, according to preliminary forecasts, grain production in 2023 could range from 1.0 percent to 2,813 million tons (including rice in flour equivalent). In the case of the main cereal crops, the main increase is provided by an increase in the volume of corn, as well as the production, in part, of rice and sorghum. At the same time, the volume of wheat and barley production may decrease compared to 2022, partially offsetting the above-mentioned growth.

According to the first forecast of world cereal consumption volumes for the 2023-2024 season, the annual volume is about 2,803 million tons, which is 0.9 percent higher than the results of the 2022-2023 season, with this increase almost in full volume will be provided due to the predicted growth in the consumption of feed grains. Expected growth in consumption both for food purposes, primarily corn, and for food products, mainly wheat and rice. In the industrial sector, there is also a foreign economic service.

Coverage from FAO's initial projections of global grain production in 2023 and consumption in the 2023-2024 range, global cereal stocks stand at 1.7 percent, reaching a record 873 million tonnes. As expected, among the main grain crops, an increase in stocks will be demonstrated by rice and barley. At the same time, stocks of wheat and sorghum are probably described below the level of the beginning of the season. Based on current projections of relative consumption and stock levels, the World Cereal Stocks-to-Consumption estimate is slightly down from 30.6 percent in the 2022-23 season to 30.4 percent in the 2023-24 season.

According to expectations, the volume of grain trade in the world will remain at the level of the 2022-2023 season and will amount to 472 million tons. Projected growth in global trade in coarse grains and rice will be partly offset by a decline in global trade in wheat. In May 2023, the FAO Cereal Price Index averaged 129.7 points, down 43.9 points (25.3 percent) from last year; such a high sharp decline in international prices for wheat and coarse grains on the increase in growth rates compared to their past values. While the FAO

Cereal Price Index is below the May 2022 high in May 2023, it is still 8.8 points (7.1 percent) higher than the average for the same month over the past five years (Table 6).

Table 6. World food situation summary tables

WORLD CEREAL MARKET							
	Production	**Supply**	**Utilization**	**Trade**	**Ending stocks**	**World stock-to-use ratio**	**Major exporters' stock-to-disappearance ratio**
	million tonnes					**percent**	
2014/15	2 608,0	3 277,8	2 508,1	375,9	767,7	30,1	19,4
2015/16	2 584,9	3 352,6	2 552,8	392,9	790,4	30,1	17,0
2016/17	2 665,2	3 455,6	2 630,2	406,6	826,3	31,1	17,8
2017/18	2 693,2	3 519,5	2 657,6	423,0	858,1	31,9	18,1
2018/19	2 645,8	3 503,9	2 686,1	411,7	836,0	30,8	18,8
2019/20	2 714,9	3 550,9	2 711,4	439,7	832,5	30,2	18,6
2020/21	2 776,6	3 609,1	2 760,4	480,7	839,7	30,0	18,4
2021/22	2 813,4	3 653,1	2 801,7	482,8	856,8	30,8	19,2
2022/23	2 786,5	3 643,3	2 777,6	471,6	858,2	30,6	20,5
2023/24	2 813,1	3 671,3	2 803,8	471,6	873,0	30,4	20,9
WORLD WHEAT MARKET							
	Production	**Supply**	**Utilization**	**Trade**	**Ending stocks**	**World stock-to-use ratio**	**Major exporters' stock-to-disappearance ratio**
	million tonnes					**percent**	
2014/15	735,6	935,1	708,7	156,4	228,1	31,8	18,8
2015/16	737,3	965,4	717,4	167,5	242,3	32,9	18,0
2016/17	763,5	1 005,8	737,2	177,2	266,6	36,1	19,9
2017/18	761,5	1 028,1	738,5	177,9	289,1	38,6	21,0
2018/19	731,4	1 020,6	749,2	169,1	274,7	36,8	18,1
2019/20	759,3	1 034,0	746,3	183,8	286,1	37,6	15,6
2020/21	775,3	1 061,4	761,6	189,4	294,6	38,0	15,2
2021/22	777,7	1 072,3	774,6	195,9	295,1	37,8	16,0
2022/23	800,9	1 095,9	779,7	199,6	310,7	39,8	19,1
2023/24	776,7	1 087,4	780,3	193,7	308,5	38,9	17,7

WORLD COARSE GRAIN MARKET							
	Production	**Supply**	**Utilization**	**Trade**	**Ending stocks**	**World stock-to-use ratio**	**Major exporters' stock-to-disappearance ratio**
	million tonnes					**percent**	
2014/15	1 381,9	1 679,3	1 312,9	174,5	363,9	27,1	14,7
2015/16	1 358,7	1 722,6	1 344,5	184,1	374,6	26,8	13,4
2016/17	1 404,7	1 779,2	1 397,9	181,0	385,5	27,1	14,6
2017/18	1 431,8	1 817,4	1 421,2	196,6	391,7	27,3	15,3
2018/19	1 406,3	1 797,9	1 435,9	198,3	374,3	25,6	15,6
2019/20	1 452,0	1 826,3	1 464,0	210,1	358,6	24,1	14,0
2020/21	1 483,4	1 842,0	1 489,0	239,2	350,1	23,3	11,5
2021/22	1 509,7	1 859,8	1 504,4	230,9	364,8	24,7	13,1
2022/23	1 468,8	1 833,5	1 478,2	218,4	352,6	23,5	13,0
2023/24	1 513,0	1 865,6	1 503,3	221,4	366,2	23,6	14,5
WORLD RICE MARKET							
	Production	**Supply**	**Utilization**	**Trade**	**Ending stocks**	**World stock-to-use ratio**	**Major exporters' stock-to-disappearance ratio**
	million tonnes					**percent**	
2014/15	490,4	663,5	486,5	45,0	175,6	35,8	24,6
2015/16	489,0	664,6	490,9	41,3	173,6	35,1	19,7
2016/17	497,1	670,6	495,1	48,4	174,2	35,0	18,8
2017/18	499,9	674,1	497,9	48,5	177,3	35,4	18,1
2018/19	508,1	685,4	501,0	44,3	187,0	37,3	22,6
2019/20	503,6	690,5	501,1	45,8	187,8	36,8	26,1
2020/21	518,0	705,8	509,8	52,1	195,0	37,3	28,5
2021/22	526,0	720,9	522,7	56,0	197,0	37,9	28,7
2022/23	516,9	713,8	519,8	53,6	194,8	37,5	29,5
2023/24	523,5	718,3	520,1	56,6	198,3	37,8	30,6

Source: own study.

Ukraine is a strong player in the global wheat market. Black Sea wheat successfully competes on the basis of lower prices, favorable exchange rates, and the region's advantageous location (FAS, Grain: World Market and Trade). Ports on the Black Sea have easy access to the growing rapidly markets in the Middle East and North Africa where wheat and feed demand has grown. The U.S. share of the global wheat market has been declining as the European

Union (EU) have risen in prominence. Globally, wheat is mainly used for human consumption. But Ukraine exports wheat both for milling and feed[29].

In the corn market, the United States is still the leading exporter, but faces strong competition from Brazil,

Argentina, and Ukraine. U.S. corn prices are still competitive, but Black Sea prices are declining and production is increasing (FAS, Grain Market and Trade February 2019). The U.S. Department of Agriculture forecasts that Ukraine is expected to grow as a major corn exporter, reaching shipments of 31.2 million metric tons (mmt) in 2029. Corn is mainly used for feed in the Middle East and North Africa. Because of challenges obtaining specific data from the full Black Sea region, Ukraine is being used as a proxy for the entire region. To assess the relevance of the development of hopper cars, let's consider what part they occupy in the share of agricultural products transportation. It is proposed to consider the example of Ukraine and the USA. Most Ukrainian grain is transported by rail (68 percent), followed by truck (23 percent) and river (9 percent) (Figure 4). At the same time, in the United States, the rail traffic figure is not as high at 37 percent, but it is still a significant percentage of total traffic.

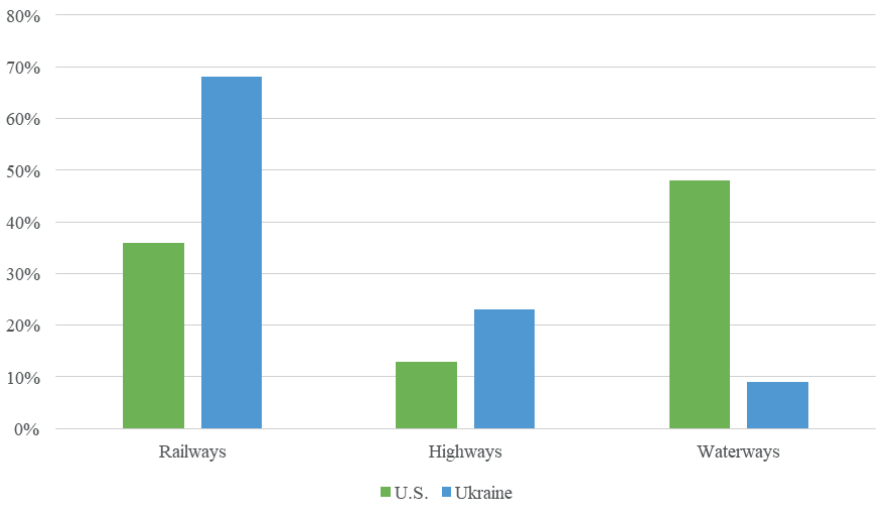


Figure 4. U.S. and Ukrainian grain and oilseeds exports by mode
Source: own study.

[29] O. Zaruba, *The biggest problem in grain transportation is the lack of responsible planning*. Ukrainian Grain Association 2023.

And in general, in countries where there is a network of railways, a similar situation is observed. Somewhere more, and somewhere less, but often rail transportation in such countries takes, if not a key, then quite a significant share in the total transportation of grain in the country. And the annual growth of the market, and with it the need for transportation, once again confirms the relevance of developments in the field of car building, namely hopper cars for transporting grain.

Analysis of the worldwide trends in global hopper car market

According to Zion[30], the global hopper car market size was worth around USD 2.1 Billion in 2022 and is further expected to grow to around USD 3.3 Billion by 2030 with a compound annual growth rate (CAGR) of approximately 5.25 percent over the forecast period (Figure 5).

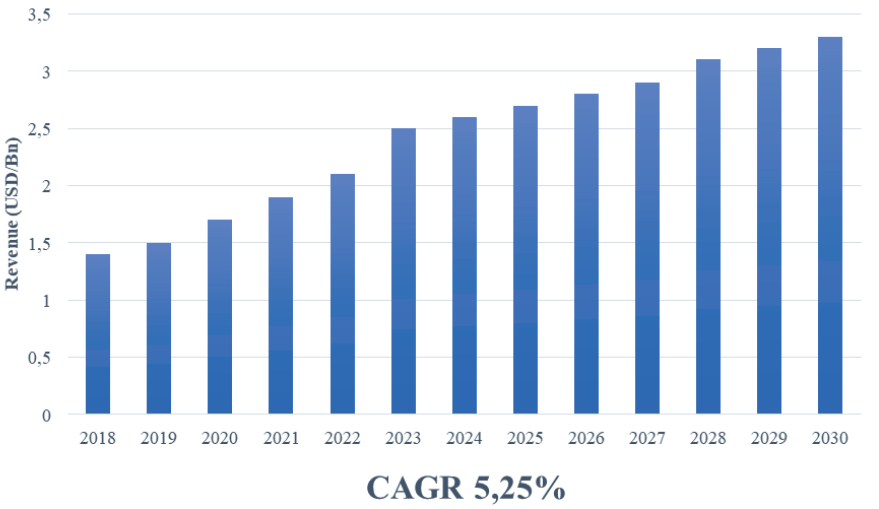


Figure 5. Global Hopper car market size (2018-2030)
Source: own study.

Demand in the global hopper car market is expected to grow exponentially due to a significant increase in demand for bulk cargo transported by rail. The cost-effectiveness of rail transportation of bulk cargo compared to

[30] Zerno Ukrainy, *Grain of Ukraine 2015*, Kyiv 2011.

road transportation and the increased focus on sustainable transportation due to minimal carbon emissions and reduced road congestion, especially in densely populated regions, are expected to contribute to the growth of the global hopper car market.

In addition, the introduction of technological advances such as digitalization, automation and the Internet of Things in the rail industry has greatly helped to streamline operations, minimize overall costs and improve operational efficiency. These factors are expected to create strong growth opportunities for the hopper car industry during the forecast period. However, the need for high capital costs for the production and rental of hopper cars, along with the costs of their maintenance and regular repairs, may hinder the growth of the hopper car market in the forecast period.

The global hopper car market is dominated by players such as:

- Novatec,
- PIOVAN S.p.A.,
- Summit Systems,
- UK Plastics Machinery Limited,
- Maguire Products Inc.,
- National Steel Car,
- TrinityRail,
- The Greenbrier Companies,
- American Rail Car Industries,
- FreightCar America,
- Vertex Railcar Corporation,
- ARI Fleet Management. Jenco Controls & Export Limited,
- SIMAR GmbH,
- Budzar Industries, Inc.,
- Movacolor,
- Advanced Auxiliary Equipment, Inc.

Next, consider a few examples of products from the previously mentioned manufacturers in the hopper car market. For example, consider the model range of cars from the The Greenbrier Companies. This 4-axled hopper cars[31] is used for the transportation of grain like corn, wheat, barley, rice corn,

[31] Zion Market Research, *Hopper Car Market by Type, Application, and Region – Global and Regiona Forecasts 2023-2030*, 2023.

rape, sunflower, rye, oat, or soy. The main characteristics of these cars are given in the Table 7.

Table 7. Technical characteristics of grain hopper cars manufactured by The Greenbrier Company

Model name General parameters	Tagnoos 898 90 m^3 4-axle hopper car	Tagnpps 95 m^3 4-axle grain hopper	Tagnpps 102 m^3 4-axle grain hopper car	Tagnpps 130 m^3 4-axle grain hopper car
Axle load	22.5 t / axle	22.5 t / axle	22.5 t / axle	22.5 t / axle
Track gauge	1,435 mm	1,435 mm	1,435 mm	1,435 mm
Loading gauge	G1-TSI	G1-TSI	G1-TSI	G1-TSI
Max. speed at 90.0 t	100 km/h	100 km/h	100 km/h	100 km/h
Max. speed (unloaded)	120 km/h	120 km/h	120 km/h	120 km/h
Climate condition	T1	T1	T1	T1
Length over buffers	17,180 mm	14,800 mm	15,400 mm	20,000 mm
Tare weight	~ 24.0 t	20.0 t ± 2 % t	~ 20.8 t	~ 22.0 t
Box volume	90.0 m^3 ± 1%	95.0 m^3 ± 1%	102.0 m^3 ± 1%	130.0 m^3 ± 1%
Loading opening	12,934 x 1200 mm	12,400 x 800 mm	13,400 x 800 mm	18,000 x 800 mm
Material of box	Carbon steel	Carbon steel	Carbon steel	Carbon steel
Operations	Manually	Manually	Manually	Manually

Source: own study.

Thus, general trends in the market for the production of hopper cars were considered, the largest manufacturers of hopper cars were given, and an example of hopper products for grain transportation from one of the largest representatives in the market for the production of hopper cars for grain transportation was presented.

Conclusions

The volumes of grain transportation in Ukraine and the share of grain transportation accounted for by rail transport were considered. Every year there is an increase in the transportation of grain, and, taking into account the prospect of growth of grain cultivation to 90 million tons per year, it is necessary to increase the share of transportation by railway transport.

An analysis of the working fleet of freight cars was carried out, with the number of hopper cars for grain transportation being singled out, which make up 11% of the total fleet of freight cars. The ratio of the state and private sector of grain transportation by rail is also shown. Thus, the relevance of carrying out research on the improvement of hopper cars for the transportation of grain is substantiated. The main stages of grain transportation logistics, as well as the advantages and disadvantages of grain transportation by road and rail transport, are considered. The composition of the working fleet of hopper cars for grain transportation of Ukrainian Railways, which is 32,309 units, most of which are morally and physically worn out, was analyzed. The average age of these cars is 28 years with a standard service life of 30 years.

The main model range of hopper cars for the transportation of grain is considered. Their main structural features are determined. Alternative options for transporting grain by rail were considered. The expediency of improving the design of the hopper car for the transportation of grain, taking into account modern technical solutions and innovative machine-building technologies, has been confirmed.

The grain transportation market in Ukraine and the world is analyzed. The orientation of the main directions of transportation of grain for export has been determined.

A general overview of the world market of hopper car manufacturers was also presented, and a brief overview of the model range of hoppers for grain transportation was presented.

Based on the results of the analysis of the above information, the following conclusions can be drawn:

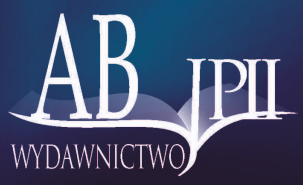
- the overall world grain market is growing;
- there is an acute shortage of vehicles in the grain transportation market in Ukraine and in the world, and the situation is especially acute with hopper cars;
- Significant growth is predicted in the market of hopper cars manufacturers.

Therefore, we can conclude that the development of a promising hopper cars for the transportation of grain taking into account traffic safety requirements is an urgent scientific and applied task.

Literature

1. APK-Inform, *Analysis of grain logistics in Ukraine and proposals for its modernization* (p. 88). APK-Inform Information Agency 2013.
2. Baranovskyi, D. M., *The problem of aging and wear of freight wagons*. Vagonny Park, 7-8, 112-113, 2016.
3. Center for Transport Strategies, *Agrologistics in Ukraine: Analytical research* (p. 56), Kyiv 2016.
4. Delo.ua., *Russia destroyed more than 15% of grain storage facilities in Ukraine: how farmers will store the 2022 harvest*, 2022. https://delo.ua/ru/agro/rf-unictozila-v-ukraine-bolee-15-zernoxranilishh-kak-fermery-budut-xranit-zerno-urozaya-2022-goda-404298/
5. Elevatorist, *Main elevator site*. https://elevatorist.com/kompanii/
6. Elevatorist, *Map of elevators in Ukraine*. http://elevatorist.com/karta-elevatorov-ukrainy
7. Elevatorist, *The working fleet of grain wagons in Ukraine is shrinking*. https://elevatorist.com/novosti/13015-v-ukraine-sokraschaetsya-rabochiy-park-zernovozov
8. FAO, *Crop Prospects and Food Situation: Quarterly Global Report No. 1*. Rome 2023.
9. Greenbrier Europe, *Product catalog: Hopper cars*. https://www.greenbrier-europe.com/product-catalog/hopper-cars/
10. Kupchenko, A. V., *Elevator capacities of Ukraine*. Grain Storage and Processing, (7), 33-37, 2014.
11. Myamlin, S. S., *Creation and modernization of rolling stock for grain transportation by rail.* In 76th International Scientific and Practical Conference Problems and Prospects for the Development of Railway Transport (p. 44-45), Dnipro 2016.
12. Myamlin, S. S., *Creation of technical means for grain transportation by rail*. In 77th International Scientific and Practical Conference Problems and Prospects for the Development of Railway Transport (p. 63-64), Dnipro 2017.
13. Myamlin, S. S., *Development of modern freight wagon designs for trans-European transportation*. In 2nd International Scientific and Technical Conference Advanced Technologies of Transport Means (p. 72-74), Kharkiv 2014.
14. Myamlin, S. S., *Mathematical modeling of spatial oscillations of railway rolling stock*. In International Scientific and Technical Conference Information Technologies in Metallurgy and Mechanical Engineering (p. 320-323), 2024.
15. Lovska, A. O., Nerubatskyi, V. P., Myamlin, S. S., Plakhtiy, O. A., *Situational adaptation of 13-7024 flat wagon model for transportation of strategic goods*. Eastern-European Journal of Enterprise Technologies, 2(7), 38-46, 2024.
16. Lovska, A. O., Nerubatskyi, V. P., Myamlin, S. S., Plakhtiy, O. A., *Determining the effect of sandwich-type components on the stress state of the universal gondola hatch cover*. Eastern-European Journal of Enterprise Technologies, 1(7), 6-13, 2024.
17. Perevozki-Kyiv, *Grain transportation in Ukraine*. http://перевозки-киев.com/perevozka-zerna-po-ukraine.html

18. Panchenko, S. V., Lovska, A. O., Myamlin, S. S., Rybin, A. V., Pavlyuchenkov, M. V., *Hopper car for grain transportation*. Utility Model Patent of Ukraine, 156818, 2024.
19. Panchenko, S. V., Lovska, A. O., Myamlin, S. S., Rybin, A. V., Pavlyuchenkov, M. V., *Covered hopper car for grain transportation*. Utility Model Patent of Ukraine, 156985, 2024.
20. Panchenko, S. V., Lovska, A. O., Myamlin, S. S., Rybin, A. V., Pavlyuchenkov, M. V., *Hopper car for grain transportation*. Utility Model Patent of Ukraine, 156984, 2024.
21. Panchenko, S. V., Lovska, A. O., Myamlin, S. S., Rybin, A. V., Pavlyuchenkov, M. V., *Hopper car with corrugated beams in the load-bearing structure*. Utility Model Patent of Ukraine, 156986, 2024.
22. Panchenko, S. V., Vatulia, G. L., Lovska, A. O., Ravlyuk, V. G., & Myamlin, S. S., *Modernized brake lever transmission of the bogie as a way to ensure the safety of freight trains*. Rail Transport of Ukraine, (4), 10-26, 2024.
23. Rustamov, R. Sh., *Assessment of prospects for the development of grain logistics in Ukraine*. Colected Scientific Papers of the Dnipropetrovsk National University of Railway Transport named after Academician V. Lazaryan, (8), 127-133, 2014.
24. Salin, D., *Ukraine Grain Transportation*. U.S. Department of Agriculture, Agricultural Marketing Service, 2020.
25. Samoylenko, I., Sterniy, O., Nabok, V., *Wagons, routes. But there's nothing to carry the grain*. Zerno, 2012.
26. State Statistics Service of Ukraine. http://www.ukrstat.gov.ua.
27. Zaruba, O*., The biggest problem in grain transportation is the lack of responsible planning*. Ukrainian Grain Association 2023.
28. Zerno Ukrainy, *Grain of Ukraine 2015*, Kyiv 2011.
29. Zion Market Research, *Hopper Car Market by Type, Application, and Region – Global and Regiona Forecasts 2023-2030*, 2023.



ISBN 978-83-68103-20-5