

WYBRANE ASPEKTY BEZPIECZEŃSTWA POZAMILITARNEGO

ZAGROŻENIA - WYZWANIA - KONCEPCJE

Monografia

redakcja

Felicjan Bylok, Agnieszka Kwiatek, Maja Skiba



Częstochowa 2022

Politechnika Częstochowska

**WYBRANE ASPEKTY BEZPIECZEŃSTWA
POZAMILITARNEGO**
Zagrożenia, wyzwania, koncepcje

Monografia

redakcja
Felicjan Byłok, Agnieszka Kwiatek, Maja Skiba



Wydawnictwo Politechniki Częstochowskiej

Częstochowa 2022

Recenzent

Prof. dr hab. Jan Maciejewski

Redakcja

Anita Ganoun

Redakcja techniczna

Dorota Boratyńska

Projekt okładki

Mateusz Kwiatek

ISBN 978-83-7193-871-9

e-ISBN 978-83-7193-872-6

- © Copyright by Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2022
- © Copyright by Felicjan Bylok, Agnieszka Kwiatek, Maja Skiba, Częstochowa 2022



Publikacja udostępniona na licencji Creative Commons Uznanie autorstwa – Użycie niekomercyjne 4.0 Międzynarodowa (CC BY-NC 4.0) <https://creativecommons.org/licenses/by-nc/4.0/legalcode>

Wydawnictwo Politechniki Częstochowskiej, 42-202 Częstochowa, al. Armii Krajowej 36 B
redakcja tel. 34 325 04 80, dystrybucja tel. 34 325 03 93
e-mail: wydawnictwo@pcz.pl, www.wydawnictwo.pcz.pl

Spis treści

Wprowadzenie	5
--------------------	---

I. Bezpieczeństwo zdrowotne

Rozdział 1. Suplementy diety a zarządzanie bezpieczeństwem zdrowotnym konsumentów – Magdalena Bsoul-Kopowska	11
Rozdział 2. Akredytacja podmiotów leczniczych celem zwiększenia poczucia bezpieczeństwa pacjentów – Żaneta Mrożek	21
Rozdział 3. Rola wsparcia psychologicznego i terapii w procesie adaptacji społecznej osób niepełnosprawnych – Dorota Lizoń-Szłapowska	31

II. Bezpieczeństwo w dobie COVID-19

Rozdział 4. Zaufanie społeczne jako czynnik wpływający na szczepienia przeciw COVID-19 – Felicjan Bylok	43
Rozdział 5. Rozwiązania Smart City służące zarządzaniu miastem w okresie pandemii COVID-19 – Katarzyna Zadros	55
Rozdział 6. Wpływ komunikacji na poczucie bezpieczeństwa pracowników w dobie pandemii – Agata Przewoźna-Krzemińska	62

III. Bezpieczeństwo informacyjne

Rozdział 7. Zarządzanie bezpieczeństwem cyfrowym w Smart City – Konrad Głębocki	73
Rozdział 8. Nowoczesne technologie wspomagające analizę zagrożeń systemu przetwarzającego informacje niejawne – Ewelina Włodarczyk, Aurelia Rybak	82
Rozdział 9. Nowoczesne technologie wspomagające analizę ryzyka dla bezpieczeństwa danych osobowych – Ewelina Włodarczyk, Aurelia Rybak	90

IV. Bezpieczeństwo w instytucjach i samorządzie terytorialnym

Rozdział 10. Znaczenie doskonalenia w procesie rozwoju zawodowego pracowników administracji publicznej i podnoszenia bezpieczeństwa kraju – Łukasz Skiba	101
---	------------

Rozdział 11. Wpływ pracy zdalnej w warunkach podwyższonego ryzyka na bezpieczeństwo i higienę pracy nauczycieli akademickich w myśl koncepcji <i>work-life balance</i> – Aleksandra Zyska, Adam Pawlak, Michał Braczkowski	112
Rozdział 12. Rozwój Smart Cities w Polsce w kontekście wykorzystania energii odnawialnej – Wioletta Skrodzka	121

V. Bezpieczeństwo ideologiczne, kulturowe i religijne

Rozdział 13. Bezpieczeństwo ideologiczne w polskiej przestrzeni naukowo-badawczej na tle teorii sekurytyzacji – Paweł Łubiński	139
Rozdział 14. Bezpieczeństwo kulturowe a program współpracy transgranicznej Polska – Białoruś – Ukraina 2014-2020 – Agnieszka Pieniążek	149
Rozdział 15. Bezpieczeństwo religijne w II RP. Rozważania na kanwie ustaw z dnia 21 kwietnia 1936 r. – Jerzy Nikołajew	157
Rozdział 16. The Elements of Management in Destructive Apocalyptic Groups on Selected Examples – Robert Janik	169

VI. Inne formy bezpieczeństwa pozamilitarnego

Rozdział 17. Strategia rozwoju zrównoważonego a bezpieczeństwo ekologiczne na obszarach przyrodniczo cennych – Ewa Albińska	181
Rozdział 18. Bezpieczeństwo socjalne rodziny poprzez zasilek wychowawczy 500+ a wpływ na wzrost zamożności rodziny – Tomasz Odzimek	190
Rozdział 19. Służby specjalne uczestnikami walki z terroryzmem na początku XXI wieku (wybrane aspekty) – Andrzej Żebrowski, Izabela Szkuřłat	201
Rozdział 20. Bezpieczeństwo służb specjalnych. Wybrane aspekty – Andrzej Żebrowski	207

Wprowadzenie

Problemy i zagadnienia związane z bezpieczeństwem są nieodłącznym elementem funkcjonowania i egzystencji każdej jednostki, a także wszystkich grup społecznych, społeczeństw, państw oraz wspólnot międzynarodowych. Termin „bezpieczeństwo” jest pojęciem wieloznacznym, interdyscyplinarnym, dotyczącym umiejętności zabezpieczenia potrzeb o charakterze egzystencjalnym: przetrwania, istnienia i rozwoju. W związku z tym może być opisywane i badane z różnych perspektyw. Jedną z nich jest bezpieczeństwo pozamilitarne, związane z różnorodnymi zagrożeniami obejmującymi obszary bezpieczeństwa publicznego (zwłaszcza przestępczość zorganizowana), bezpieczeństwa informacyjnego (działania wywiadowcze), terroryzmu i związanego z nim ekstremizmu politycznego, obszaru cyberprzestrzeni (cyberprzestępczość, szpiegostwo w sieci, działania hakerskie itd.), a także zagrożeniami ekologicznymi, ekonomicznymi, religijnymi itp. Wydaje się, że do ich badań najodpowiedniejsze jest podejście interdyscyplinarne, umożliwiające wyjaśnienie i opis mechanizmów tych zagrożeń.

Z uwagi na rozległość problematyki badawczej dotyczącej bezpieczeństwa pozamilitarnego zaistniała potrzeba dokonania wyboru problemów teoretyczno-empirycznych, które pozwolą zrozumieć jego złożoność. Biorąc pod uwagę aspekty teoretyczne i empiryczne, dokonano wyboru sześciu problemów, które zostały szerzej omówione w poszczególnych rozdziałach monografii. Każdy problem jest omawiany przy użyciu kluczowych dla niego pojęć i ukazuje ramy teoretyczno-analityczne, w których bezpieczeństwo pozamilitarne jest opisane i wyjaśnione.

Monografia składa się z sześciu obszarów tematycznych. W pierwszym autorzy podjęli problematykę bezpieczeństwa zdrowotnego. Pierwszy rozdział pt. *Suplementy diety a zarządzanie bezpieczeństwem zdrowotnym konsumentów* poświęcono problemowi rosnącej tendencji do konsumpcji suplementów diety oraz sposobom przeciwdziałania i minimalizowania zagrożeń, jakie mogą wynikać z tego zjawiska. W drugim rozdziale pt. *Akredytacja podmiotów leczniczych celem zwiększenia poczucia bezpieczeństwa pacjentów* przedstawiono problematykę wdrażania akredytacji w podmiotach leczniczych, w szczególności jej wpływu na poczucie bezpieczeństwa pacjentów. Wysoka jakość usług medycznych zwiększa poczucie bezpieczeństwa pacjentów, a także wpływa na cały system ochrony zdrowia. W trzecim rozdziale pt. *Rola wsparcia psychologicznego i terapii w procesie adaptacji społecznej osób niepełnosprawnych* omówiono problematykę wsparcia, rozumianego jako działanie dostępne, wysokospecjalistyczne oraz dostosowane do potrzeb i oczekiwań osób niepełnosprawnych. Wsparcie takie przeciwdziała zaburzeniom w funkcjonowaniu tych jednostek, służy budowaniu i podtrzymywaniu relacji społecznych, indywidualnej niezależności i autonomii osobistej zapobiegającej wykluczeniu i izolacji społecznej.

Drugą część monografii poświęcono zagadnieniom bezpieczeństwa w dobie pandemii COVID-19. W czwartym rozdziale pt. *Zaufanie społeczne jako czynnik*

wplywający na szczepienia przeciw COVID-19 przedstawiono rolę zaufania społecznego wspomagającego działania instytucji ochrony zdrowia na rzecz propagowania szczepień przeciw COVID-19. Przyjęto założenie, że zaufanie do rządu, instytucji publicznych i do innych ludzi w istotny sposób determinuje decyzje ludzi o przyjęciu szczepionki przeciw COVID-19. W rozdziale piątym pt. *Rozwiązania Smart City służące zarządzaniu miastem w okresie pandemii COVID-19* poddano analizie działania typowe dla inteligentnego miasta, które umożliwiają ograniczanie emisji wirusa, a tym samym zmniejszają liczbę zakażeń i zachorowań na COVID-19. W kolejnym rozdziale pt. *Wpływ komunikacji na poczucie bezpieczeństwa pracowników w dobie pandemii* omówiono znaczenie komunikacji interpersonalnej w zapewnianiu bezpieczeństwa i poprawy jakości życia pracownikom w warunkach kryzysu wywołanego pandemią COVID-19.

W części trzeciej monografii podjęto dyskusję nad kwestią bezpieczeństwa informatycznego w społeczeństwie. W siódmym rozdziale pt. *Zarządzanie bezpieczeństwem cyfrowym w Smart City* dokonano systematyzacji zagadnień związanych z bezpieczeństwem cyfrowym w Smart City oraz sformułowano rekomendację dla miast w tym obszarze. Kolejny rozdział pt. *Nowoczesne technologie wspomagające analizę zagrożeń systemu przetwarzającego informacje niejawne* poświęcono zagadnieniu ochrony informacji niejawnych. Przedstawiono analizę zagrożeń systemu przetwarzającego informacje niejawne, a także zaprezentowano program komputerowy, który umożliwia przeprowadzenie analizy zagrożeń. W następnym rozdziale pt. *Nowoczesne technologie wspomagające analizę ryzyka dla bezpieczeństwa danych osobowych* omówiono problematykę bezpieczeństwa informacyjnego i bezpieczeństwa danych osobowych. Przedstawiono program komputerowy służący do analizy ryzyka dla bezpieczeństwa danych osobowych.

Czwarta część monografii obejmuje problematykę bezpieczeństwa w instytucjach i samorządzie terytorialnym. Część tę rozpoczyna rozdział dziesiąty pt. *Znaczenie doskonalenia w procesie rozwoju zawodowego pracowników administracji publicznej i podnoszenia bezpieczeństwa kraju*, w którym poruszono kwestię szkoleń związanych z bezpieczeństwem zdrowotnym, cybernetycznym i militarnym. W kolejnym rozdziale pt. *Wpływ pracy zdalnej w warunkach podwyższonego ryzyka na bezpieczeństwo i higienę pracy nauczycieli akademickich w myśl koncepcji work-life-balance* przedstawiono wyniki badań nad wpływem pracy zdalnej w czasach pandemicznych na bezpieczeństwo i higienę pracy nauczycieli akademickich. W rozdziale dwunastym pt. *Rozwój Smart Cities w Polsce w kontekście wykorzystania energii odnawialnej* zaprezentowano koncepcję inteligentnego miasta w kontekście wykorzystania energii odnawialnej. Przedstawiono analizę i ocenę poziomu stopnia wdrożenia energetyki odnawialnej w przestrzeni miejskiej jako filaru koncepcji Smart City.

Piątą część monografii poświęcono zagadnieniom bezpieczeństwa ideologicznego, kulturowego i religijnego. W trzynastym rozdziale pt. *Bezpieczeństwo ideologiczne w polskiej przestrzeni naukowo-badawczej na tle teorii sekurytyzacji* omówiono zagadnienia sekurytyzacji uwarunkowań i zagrożeń o charakterze ideologiczno-politycznym w nawiązaniu do teorii sektorów bezpieczeństwa. Czternasty rozdział pt. *Bezpieczeństwo kulturowe a Program Współpracy Transgranicznej*

Polska – Białoruś – Ukraina 2014-2020 przedstawia ocenę możliwości oddziaływania Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina na bezpieczeństwo kulturowe w Polsce. Analizą objęto unijną perspektywę finansową 2014-2020. W piętnastym rozdziale pt. *Bezpieczeństwo religijne w II RP. Rozważania na kanwie ustaw z dnia 21 kwietnia 1936 r.* poruszono zagadnienie zabezpieczenia przez władze państwowe interesów w zakresie bezpieczeństwa religijnego w relacjach ze związkami wyznaniowymi mniejszościowymi. Szesnasty rozdział pt. *The Elements of Management in Destructive Apocalyptic Groups on Selected Examples* poświęcono skutkom destrukcyjnych kultów w społeczeństwie, w szczególności sektom apokaliptycznym, które odgrywają istotną rolę wśród organizacji religijnych, wykazując się specyficznymi formami organizacyjnymi.

Ostatnia część monografii obejmuje zróżnicowaną problematykę bezpieczeństwa pozamilitarnego. W rozdziale siedemnastym pt. *Strategia rozwoju zrównoważonego a bezpieczeństwo ekologiczne na obszarach przyrodniczo cennych* omówiono proces przygotowania ekostrategii dla obszaru chronionego o uznanych walorach przyrodniczych, uwzględniającej bezpieczeństwo ekologiczne. Osiemnasty rozdział pt. *Bezpieczeństwo socjalne rodziny poprzez zasilek wychowawczy 500+ a wpływ na wzrost zamożności rodziny* poświęcono zagadnieniu pomocy materialnej państwa dla polskich rodzin, ze szczególnym uwzględnieniem wspierania finansowego rodzin wielodzietnych, w aspekcie bezpieczeństwa socjalnego. W rozdziale dziewiętnastym pt. *Służby specjalne uczestnikami walki z terroryzmem na początku XXI wieku. Wybrane aspekty* przedstawiono zagadnienie roli służb specjalnych w walce z terroryzmem zarówno w działaniach ofensywnych, jak i defensywnych. Kolejny rozdział pt. *Bezpieczeństwo służb specjalnych. Wybrane aspekty* przedstawia problematykę służb specjalnych, które stanowią podstawę aparatu zasilania w informacje uprawnionych użytkowników. Omawia działania o charakterze wywiadowczym i kontrwywiadowczym realizowane w otoczeniu wewnętrznym i zewnętrznym państwa.

Monografia kierowana jest do przedstawicieli środowisk naukowych, administracji publicznej, jednostek samorządów terytorialnych, służb mundurowych, organizacji pozarządowych, firm i osób zainteresowanych problematyką bezpieczeństwa pozamilitarnego, a także studentów, w tym studentów kierunków związanych z bezpieczeństwem. Redaktorzy mają nadzieję, że problemy poruszone w monografii staną się punktem wyjścia do refleksji nad procesami związanymi z bezpieczeństwem we współczesnym społeczeństwie i w jego organizacjach.



Bezpieczeństwo zdrowotne

Rozdział 1

SUPLEMENTY DIETY A ZARZĄDZANIE BEZPIECZEŃSTWEM ZDROWOTNYM KONSUMENTÓW

Magdalena Bsoul-Kopowska¹

Streszczenie: Niniejszy rozdział poświęcony jest problemowi rosnącej w ostatnich latach tendencji do konsumpcji suplementów diety oraz sposobom przeciwdziałania i minimalizowania zagrożeń, jakie mogą wynikać z tego zjawiska. Przeprowadzone badanie polegało na analizie dostępnych publikacji naukowych, raportów oraz danych statystycznych. Na podstawie badań stwierdzono, że Polacy coraz częściej sięgają po suplementy diety, mimo że ich wiedza o korzyściach i zagrożeniach z ich zażywania oraz o przepisach regulujących ich dopuszczenie do sprzedaży jest ograniczona oraz że stosowanie suplementów diety nie zawsze jest bezpieczne. Uzyskane wyniki wskazują również na potrzebę podjęcia działań w zakresie zarządzania bezpieczeństwem zdrowotnym, mających na celu edukację dotyczącą stosowania suplementów diety, a także na wprowadzenie zmian w regulacjach prawnych i rozwiązaniach instytucjonalnych funkcjonujących na rynku suplementów diety.

Słowa kluczowe: bezpieczeństwo zdrowotne, suplementy diety, zarządzanie

Wprowadzenie

Od ponad dekady wartość światowego rynku suplementów diety systematycznie rośnie, osiągając w 2018 roku 100 mld dolarów. Prognozy wskazują, że do 2025 roku wartość ta będzie zwiększać się o około 7% w skali roku. Również na europejskim rynku można zaobserwować gwałtowny wzrost liczby suplementów diety, które są wprowadzane w krajach Unii Europejskiej. Ta wzrostowa tendencja jest także widoczna na rynku polskim, na co wskazuje wartość sprzedaży w wysokości ponad 4 mld zł w 2017 roku. W okresie od roku 2008 do roku 2017 zwiększyła się ona ponad trzykrotnie. Przewiduje się, że w najbliższej przyszłości sprzedaż suplementów diety na krajowym rynku wzrośnie o około 5% rocznie (Czerwiński, Liebers 2019, s. 7).

Zgodnie z obowiązującymi przepisami prawa żywnościowego suplementy diety są definiowane jako środki spożywcze. Tłumaczy to ich powszechną dostępność, co

¹ Politechnika Częstochowska, Wydział Zarządzania

z kolei przekłada się na wzrost zainteresowania nimi przez konsumentów dbających o swoje zdrowie. Często są one traktowane jako środek mający rekompensować brak aktywności fizycznej czy złe samopoczucie. Według Ustawy z dnia 25 sierpnia 2006 roku o bezpieczeństwie żywności i żywienia (Dz.U. nr 171 poz. 1225) celem suplementu diety jest uzupełnienie normalnej diety konsumenta. Środki te mają zatem za zadanie bilansowanie niedoborów w diecie i korygowanie niedożywienia. Przeprowadzone badania wykazały, że przy odpowiednim ich zastosowaniu suplementacja osiąga wspomniane cele. Zaznacza się jednak, że większość stosowanych suplementów nie daje prawie żadnych korzyści, a część z nich jest wręcz szkodliwa (Czerwiński, Liebers 2019, s. 10).

W roku 2017 aż 72% Polaków przyznało się do zażywania suplementów diety, a 48% robiło to regularnie, przy czym zaledwie 17% z nich skonsultowała tę kwestię z lekarzem lub farmaceutą (SW Research 2017). Wyniki te pokazują, że suplementowanie staje się w Polsce coraz bardziej powszechne, co z kolei rodzi zapotrzebowanie na badania poświęcone różnym aspektom bezpieczeństwa stosowania suplementów diety przez różne grupy konsumentów.

Celem tego rozdziału jest próba określenia zagrożeń, jakie mogą się wiązać z rosnącą konsumpcją suplementów diety przez Polaków, a także zbadanie stanu wiedzy konsumentów i analiza ich zachowań w stosunku do tych specyfików. W rozdziale zwrócono również uwagę na rozwiązania regulacyjno-instytucjonalne, które mogłyby poprawić bezpieczeństwo i świadomość konsumentów.

Suplementy diety - definicja i regulacje prawne

Suplementy diety są środkami spożywczymi i muszą odpowiadać definicji żywności zawartej w rozporządzeniu Parlamentu Europejskiego i Rady z 2002 roku, zgodnie z którą „żywność (środek spożywczy) oznacza jakiegokolwiek substancje lub produkty, przetworzone, częściowo przetworzone lub nieprzetworzone, przeznaczone do spożycia przez ludzi lub których spożycia przez ludzi można się spodziewać” (Rozporządzenie... 2002, s. 469).

UE definiuje suplementy diety jako „środki spożywcze, których celem jest uzupełnianie normalnej diety i które są skoncentrowanym źródłem substancji odżywczych lub innych substancji wykazujących efekt odżywczy lub fizjologiczny, pojedynczych lub złożonych, sprzedawanych w postaci dawek, a mianowicie w postaci kapsułek, pastylek, tabletek, pigułek i w innych podobnych formach, jak również w postaci saszetek z proszkiem, ampułek z płynem, butelek z kroplomierzem i w tym podobnych postaciach płynów lub proszków przeznaczonych do przyjmowania w niewielkich ilościach jednostkowych” (Dyrektywa... 2002, s. 491). Jednym z ważniejszych aktów dotyczących suplementów diety jest Rozporządzenie WE nr 178/2002 Parlamentu Europejskiego i Rady z 28 stycznia 2002 roku, ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd do Spraw Bezpieczeństwa Żywności oraz ustanawiające procedury w sprawie bezpieczeństwa żywności (Dz.Urz. WE L 31/1 z 1.2.2002). Rozporządzenie to stosuje się do wszystkich etapów produkcji, przetwarzania i dystrybucji żywności.

W Polsce aktami regulującymi rynek suplementów diety są: Ustawa z dnia 25 sierpnia 2006 roku o bezpieczeństwie żywności i żywienia (Dz.U. nr 171 poz. 1225) oraz Rozporządzenie Ministra Zdrowia z dnia 9 października 2007 r. w sprawie składu oraz oznakowania suplementów diety (Dz.U. 2007 nr 196 poz. 1425). Zgodnie z definicją, jaka została zawarta w ustawie, suplement diety to: „środek spożywczy, którego celem jest uzupełnienie normalnej diety, będący skoncentrowanym źródłem witamin lub składników mineralnych, lub innych substancji wykazujących efekt odżywczy, lub inny fizjologiczny, pojedynczych lub złożonych, wprowadzany do obrotu w formie umożliwiającej dawkowanie (...), z wyłączeniem produktów posiadających właściwości produktu leczniczego w rozumieniu prawa farmaceutycznego” (Ustawa... 2006, art. 3 ust. 3 pkt 39).

Na stronie Głównego Inspektora Sanitarnego znajdujemy zapis nawiązujący do rozporządzenia Ministra Zdrowia z roku 2007: „Maksymalny dopuszczalny poziom zawartości witamin i składników mineralnych oraz innych substancji wykazujących efekt odżywczy lub inny efekt fizjologiczny zapewnia, że zwykle stosowanie suplementu diety zgodnie z informacją zamieszczoną w oznakowaniu będzie bezpieczne dla zdrowia i życia człowieka” (GIS 2018). Z dalszych przepisów wspomnianego rozporządzenia wynika również, że suplementy diety, które są wprowadzane do obrotu, wymagają odpowiedniego oznakowania umieszczonego na opakowaniu, zawierającego informacje dotyczące: określenia „suplement diety”, nazwy kategorii substancji odżywczych lub substancji charakteryzujących produkt albo wskazanie charakteru tych substancji, zalecaną do spożycia dzienną porcją produktu, ostrzeżenie dotyczące nieprzekraczania zalecanej porcji do spożycia w ciągu dnia, stwierdzenie, że suplementy diety nie mogą być stosowane jako substytut zróżnicowanej diety oraz że powinny być przechowywane w sposób niedostępny dla małych dzieci. Podsumowując, można stwierdzić, że polskie prawo definiuje suplementy diety w sposób podobny do dyrektywy UE, dodając jednak na końcu, że definicja nie obejmuje produktów „posiadających właściwości produktu leczniczego w rozumieniu przepisów prawa farmaceutycznego” (Baraniak i in. 2020, s. 161-168).

Na polskim rynku zauważalnych jest coraz więcej produktów, których skład oraz przeznaczenie może sugerować, że są one „odpowiednikami” lub produktami mogącymi zastąpić „lek”. Dzieje się tak dlatego, że suplementy diety oferowane są do sprzedaży pod taką samą postacią jak leki czy wyroby medyczne (tabletki, kapsułki, drażetki). Jednak różnice między tymi produktami są zasadnicze. Dotyczy to zarówno sposobu działania, jak i zasad dopuszczania czy wprowadzania do obrotu. Lek od wyrobu medycznego różni się przede wszystkim sposobem działania. Produkty lecznicze mają działanie farmakologiczne, natomiast wyroby medyczne charakteryzują się działaniem fizycznym czy mechanicznym. Przykładowo krople do oczu zawierające antybiotyk będą lekiem, a krople do nawilżania soczewek stanowią już tylko wyrób medyczny. W przypadku leku jego wskazania do stosowania są określone w charakterystyce produktu leczniczego i muszą być zatwierdzone przez Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych. Lek wymaga również ciągłego nadzoru i monitorowania jakości przez Inspekcję Farmaceutyczną. Dodatkowo sprawdza się bezpieczeństwo stosowania przez lekarzy, farmaceutów i podmiot wprowadzający do obrotu.

W przypadku suplementu diety prawo nie wymaga ani rejestracji, ani szczegółowej dokumentacji. Wobec suplementów diety nie ma również ustawowego wymogu ciągłego monitorowania bezpieczeństwa jego stosowania, a jakość jest nadzorowana przez Inspekcję Sanitarną. Oznacza to, iż osoby kupujące tego typu preparaty nie mają pewności, czy zawierają one deklarowaną substancję czynną oraz czy określona substancja występuje w deklarowanej przez producenta ilości. Dodatkowo występuje potencjalne ryzyko obecności w preparacie substancji niedozwolonych dla suplementów diety.

Wprowadzając suplement diety na rynek, należy tylko powiadomić Główny Inspektorat Sanitarny i dostarczyć wzór opakowania. W powiadomieniu tym należy podać dokładny skład produktu, czyli jakie składniki, w jakiej formie i w jakiej ilości w nim występują. Nie jest natomiast wymagana dokumentacja potwierdzająca jakość oraz deklarowane efekty działania. Spełnienie tego warunku formalnego pozwala na sprzedaż zgłoszonego produktu. Tak ograniczone wymogi sprzyjają szybkiemu rozwojowi rynku suplementów diety w Polsce, co przekłada się na rosnącą liczbę ich zarejestrowań. W rejestrze Głównego Inspektoratu Sanitarnego (GIS) w 2009 roku dokonano 3066 notyfikacji, natomiast w 2019 roku zanotowano ich już 15 170. Według danych GIS z 2020 roku w latach 2007-2019 wpisano łącznie ponad 84 tys. produktów zgłoszonych jako suplementy diety (Departament Bezpieczeństwa... 2020). Ze względu na dużą liczbę występujących na rynku suplementów diety również ich kontrola ma bardzo ograniczony zasięg, co z kolei powoduje, że za jakość oraz bezpieczeństwo produktu odpowiada przede wszystkim jego producent lub importer.

Wpływ suplementów diety na bezpieczeństwo zdrowotne

Suplementacja diety stanowi dobry sposób na uzupełnienie niedoborów niektórych składników w organizmie człowieka. Stwarza też możliwość wystąpienia zagrożeń dla konsumenta w przypadku nieuzasadnionego i nadmiernego spożycia tych produktów. Suplementy diety – jak wynika z definicji – są środkami spożywczymi składającymi się z witamin i związków mineralnych, które powinny być zażywane w sytuacji wystąpienia ich niedoboru w organizmie. Natomiast sformułowanie, które jest zawarte w definicji suplementu diety, dotyczące „innych substancji wykazujących efekt odżywczy lub inny fizjologiczny”, daje pozwolenie na dodawanie w składzie suplementów diety składników innych niż witaminy i minerały. Składnikami suplementów są więc m.in. witaminy (A, D, E, K, B₁, B₂, niacyna, kwas pantotemowy, B₆, kwas foliowy, B₁₂, biotyna, witamina C), składniki mineralne (wapń, magnez, żelazo, miedź, jod, cynk, mangan, sód, potas, selen, chrom, molibden, fluorki, chlorki, fosfor, bor i krzem), ale także takie substancje jak np. aminokwasy, kwasy tłuszczowe, błonnik pokarmowy, luteina, probiotyki i prebiotyki oraz produkty pochodzenia roślinnego. Niestety w krajowych przepisach prawnych nie ma listy innych składników, które można stosować w suplementach diety. Składniki oraz ich poziomy zawarte w poszczególnych suplementach diety muszą jedynie zagwarantować, że normalne ich stosowanie, zgodne z zaleceniami producenta, będzie bezpieczne dla konsumenta.

Konsumenci traktują suplementy diety jako produkty prozdrowotne, włączając je do swojej diety i stosując jednocześnie produkty wzbogacane. Dbając o swoje zdrowie, zapominają o zagrożeniu spożycia nadmiernych ilości witamin i składników mineralnych, co może wywołać skutki uboczne i stać się szkodliwe dla stanu ich zdrowia. Decyzja o zażywaniu suplementów powinna być skonsultowana z lekarzem lub dietetykiem, a przed zaleceniem powinien zostać przeprowadzony wywiad dotyczący sposobu żywienia, stanu zdrowia, chorób, stosowanych leków, palenia tytoniu i stylu życia.

Rosnące zainteresowanie Polaków uzupełnianiem diety suplementami niestety nie jest skorelowane ze wzrostem poziomu wiedzy dotyczącej przyjmowanych preparatów. Przeciętny Polak stosujący suplementy przejawia brak świadomości ryzyka wystąpienia konsekwencji zdrowotnych na skutek niewłaściwego ich spożycia. Wynika to po pierwsze z ograniczonej wiedzy o korzyściach zażywania suplementów, po drugie z braku znajomości przepisów regulujących ich dopuszczenie do sprzedaży i po trzecie z wątpliwego profilu bezpieczeństwa suplementów, który jest efektem niewłaściwych zabezpieczeń mających chronić konsumenta zarówno przed szkodliwymi produktami, jak i nieuczciwymi producentami (Dziedziński i in. 2019, s. 235-242).

Ograniczona wiedza konsumentów o korzyściach zażywania suplementów diety

Konsumenci często postrzegają suplementację jako szybką i wygodną drogę do poprawy swojego stanu zdrowia oraz skorygowania sposobu żywienia bez konieczności zmiany diety, a ich świadomość na temat suplementów nie jest kształtowana przez ekspertów, lekarzy czy dietetyków, lecz przede wszystkim przez media i spoty reklamowe. Prawie połowa (48%) Polaków spożywa suplementy diety regularnie, a tylko 27% potrafi je poprawnie zdefiniować. W znacznej mierze wynika to z nieświadomości, czym są suplementy diety i czym różnią się od leków dostępnych bez recepty. Badanie przeprowadzone przez TNS Polska w 2014 roku wykazało, że wiele osób mylnie uznało suplementy za „witaminy” (31%) czy „minerały” (8%) (NIK 2017). Natomiast 37% Polaków jest przekonanych, że suplementy diety są testowane pod względem skuteczności, a aż 50% wierzy, że podlegają one takim samym standardom nadzoru jak leki (Czerwiński, Liebers 2019, s. 4).

Brak wiedzy na temat możliwych skutków ich stosowania to jeden z głównych problemów bezpieczeństwa zdrowotnego. Wyniki prowadzonych w tym zakresie badań świadczą, iż dobór suplementu diety i jego stosowanie przez konsumenta jest często nieuzasadnione. W niektórych przypadkach stosowanie wybranych suplementów diety może powodować przekroczenie zalecanych norm żywienia, a to z kolei może skutkować poważnymi zaburzeniami funkcjonowania organizmu. Przykładowo przyjmowanie witaminy A powyżej zalecanej normy staje się toksyczne dla organizmu. Objawiać się to może m.in. zwiększoną drażliwością, torsjami, zmianami skórными, zaburzeniami czynności śledziony i wątroby. Z kolei nadmiar żelaza może powodować choroby układu krążenia, udary, miażdżycę,

choroby Alzheimera i Parkinsona (Stępień, Niewiarowski, Harasimiuk 2019, s. 51-59).

Na podstawie danych o spożyciu suplementów diety w UE wśród składników, dla których istnieje ryzyko związane z nadmiernym spożyciem, wymienia się m.in. witaminę A, β -karoten, miedź, jod i żelazo. Stwierdzono także, że np. u osób palących papierosy suplementacja β -karotenem w dawkach od 20 do 50 mg dziennie zwiększa ryzyko wystąpienia raka płuc.

Istotnym zagadnieniem są również interakcje przyjmowanych suplementów diety z produktami leczniczymi, a producenci suplementów diety nie mają obowiązku zamieszczania na opakowaniach informacji o działaniach niepożądanych lub przeciwwskazaniach. Instytut Żywności i Żywienia wyszczególnia kilka grup konsumentów, które powinny rozważyć suplementację swojej diety, a wśród nich wymienia: 1) osoby dorosłe będące na diecie niskoenergetycznej; 2) osoby starsze; 3) osoby stosujące diety z ograniczeniami bądź eliminacją niektórych składników pokarmowych; 4) kobiety po menopauzie; 5) kobiety ciężarne.

Brak znajomości przepisów regulujących ich dopuszczenie do sprzedaży

Konsumentom brakuje wiedzy na temat przepisów regulujących sprzedaż suplementów diety, a ponadto często nie rozróżniają suplementów diety od leków bez recepty. Prawdopodobnie wynika to z podobieństw między reklamami, opakowaniami i miejscami sprzedaży (apteki) tych dwóch grup produktów, niewystarczającego dostępu do informacji oraz braku potrzeby konsultowania przyjmowanych suplementów z lekarzem lub dietetykiem. Ze względów bezpieczeństwa zdrowia swoich obywateli w większości krajów suplementy diety poprzez etykiety, reklamę czy ulotkę nie mogą sugerować konsumentom, że zapobiegają chorobom lub też łagodzą ich skutki. Przeprowadzone w krajach rozwiniętych badania dotyczące wiedzy konsumentów o skuteczności suplementów diety i ich przeznaczeniu wskazują, że jest ona niewielka, a mimo to przynajmniej połowa ich populacji przyznaje się do systematycznego zażywania wspomnianych produktów (Czerwiński, Liebers 2019, s. 10).

Na dynamiczny rozwój rynku suplementów diety niewątpliwym wpływ ma ich reklama. Z danych udostępnionych przez KRRiT wynika, że od 1997 roku do 2015 roku liczba reklam suplementów diety wzrosła blisko dwudziestokrotnie. Dla porównania ogólna liczba reklam wzrosła jedynie trzykrotnie. W wyniku kontroli NIK wykazano, że reklamy poszczególnych suplementów diety zamieszczanych na stronach internetowych zawierają m.in. treści przypisujące suplementom właściwości lecznicze. Reklamy te sugerują również, że suplementy diety są niezbędnym elementem codziennej diety. Treści reklam wprowadzają konsumenta w błąd sugestią, że stanowią one remedium na liczne dolegliwości i potrzeby, i obiecują szybką poprawę zdrowia, wykorzystując niewiedzę klientów i nadużywając tym samym ich zaufanie (NIK 2017).

Zdarzają się również nieuczciwe formy promocji suplementów diety, polegające na upodobnieniu do siebie produktów należących do różnych kategorii poprzez

stosowanie tzw. znaków parasolowych (ang. *umbrella branding*). Dotyczy to przypadków, gdy pod określoną marką zostaje wypromowany środek leczniczy, a następnie pod tą samą albo zbliżoną zostaje wprowadzony na rynek suplement diety, który właściwości leczniczych nie wykazuje.

Przeprowadzona kontrola NIK wykazała, że w Polsce poziom bezpieczeństwa suplementów diety nie jest zapewniony na właściwym poziomie. Organy, które są odpowiedzialne za bezpieczeństwo ich stosowania, w sposób nierzetelny realizowały zadania związane z wprowadzaniem ich po raz pierwszy do obrotu. Niewłaściwy był także nadzór nad jakością zdrowotną suplementów diety. NIK stwierdził również niedostateczny poziom prowadzonej edukacji żywieniowej w badanym zakresie, a dotyczący przede wszystkim nieadekwatnego zapewnienia bezpieczeństwa suplementów diety rozwiązaniami legislacyjnymi, szczególnie w zakresie ich wprowadzania na rynek.

Suplementy diety a bezpieczeństwo zdrowotne konsumentów. Wątpliwy profil bezpieczeństwa suplementów diety

Badania laboratoryjne suplementów diety przeprowadzone przez NIK pozwoliły na stwierdzenie, że wiele suplementów nie wykazuje cech deklarowanych przez producentów, a zdarzają się też po prostu szkodliwe dla zdrowia. W sprzedaży prowadzonej zarówno w aptekach i sklepach stacjonarnych, jak i sklepach internetowych obok rzetelnych preparatów znajdowały się suplementy diety zafałszowane, zawierające np. bakterie chorobotwórcze, substancje zakazane z listy psychoaktywnych czy stymulanty podobne strukturalnie do amfetaminy, czyli działające jak narkotyki.

Suplementy diety nie podlegają obowiązkowej kontroli jakości, jakiej podlegają produkty lecznicze. Nie jest też wymagane sprawdzanie trwałości tych preparatów oraz badanie ich interakcji z produktami leczniczymi. Suplementy diety nie są również monitorowane pod względem wywoływania potencjalnych działań niepożądanych, ponieważ Główny Inspektorat Farmaceutyczny nie sprawuje nad nimi kontroli. Każdy przedsiębiorca – zgodnie z obowiązującym prawem – może wprowadzić na rynek suplement diety. W przypadku otrzymania zgłoszenia o potencjalnej wadzie jakościowej suplementu diety GIS wszczyna kontrolę danego preparatu. Najwyższa Izba Kontroli wykazała, że wobec połowy zgłoszeń rejestracyjnych suplementów diety z lat 2014-2016, tj. około 6 tys. preparatów, w ogóle nie rozpoczęto żadnego procesu weryfikacji, co oznacza, że produkty te nie były w jakikolwiek sposób sprawdzone pod względem bezpieczeństwa stosowania przez konsumentów. Nie oznacza to, że w odniesieniu do tych produktów, co do których rozpoczęto proces weryfikacji, podejmowane działania zapewniały konsumentom bezpieczeństwo. Wpływał na to niewiarygodnie długi czas realizacji procedur. Postępowania wyjaśniające wszczęte we wcześniejszym okresie, tj. w latach 2009-2010, trwały blisko 2300 dni (ponad 6 lat), przy czym najdłuższe z tych postępowań – ponad 3100 dni (ok. 8,5 roku). W latach 2014-2016 średni czas trwania weryfikacji powiadomień wynosił 455 dni (maksymalnie 817 dni). Natomiast w 2018 roku 6,24% kontroli suplementów diety przeprowadzonych przez GIS dało negatywny, dyskwalifikujący

wynik. Postępowanie weryfikacyjne średnio trwa około dwóch lat. Warto dodać, że w tym czasie produkt może być dostępny w sprzedaży detalicznej (Stoś 2017).

Wyniki badań jakościowych wybranych suplementów diety pokazują również, że obecne na rynku produkty mogą nie spełniać podstawowych wymagań jakościowych. Przykładem może być suplement diety wspomagający odchudzanie, w którym wykryto roślinę *Aciacia rigidula* zawierającą dimetylotryptaminę, która jest substancją psychoaktywną wymienioną w ustawie o przeciwdziałaniu narkomanii. Po badaniu wycofano z obiegu 316 opakowań suplementu, podczas gdy jego sprzedaż przez jednego importera wynosiła już ponad 10 tys. opakowań (Stępień, Niewiarowski, Harasimiuk 2019, s. 51-59).

Spośród wybranych do kontroli 45 suplementów diety, które nie powinny być wprowadzone do obrotu z uwagi na zawartość niedozwolonych składników, aż 38 w czasie prowadzenia badań kontrolnych przez NIK znajdowało się w sprzedaży (sprawdzono sprzedaż internetową). Pomimo poinformowania przez NIK Głównego Inspektora Sanitarnego nie zostały podjęte działania mające na celu wyeliminowanie zagrożeń. Według stanu na 2017 rok 33 z kwestionowanych 38 suplementów diety nadal znajdowało się w sprzedaży internetowej i zawierało szkodliwe substancje (Stoś 2017).

Podsumowanie

Rynek suplementów diety w Polsce należy ocenić jako obszar wysokiego ryzyka w zarządzaniu bezpieczeństwem zdrowotnym. Co prawda prawo europejskie reguluje rynek suplementów diety odpowiednimi rozporządzeniami i dyrektywami oraz zabrania wprowadzania w błąd ich konsumentów, ale konsekwentne egzekwowanie tych zapisów w praktyce nie jest już takie proste – jest bardzo ograniczone. Dlatego też w celu wyegzekwowania od organów sprawujących nadzór nad bezpieczeństwem suplementów diety realizacji wszystkich obowiązków, wynikających z już obowiązujących aktów prawnych, zaleca się przekazanie ich pod kontrolę Ministra Zdrowia. Powinny zostać wprowadzone działania legislacyjne zmierzające do wdrożenia nowych kompleksowych rozwiązań prawnych dotyczących suplementów diety, np.: wprowadzenie opłaty za zgłaszanie nowych suplementów diety do Głównego Inspektoratu Sanitarnego; wydzielenie w rejestrze GIS suplementów, wobec których wszczęto procedury weryfikujące; wprowadzenie systemu wczesnego ostrzegania umożliwiającego szybkie zawiadamianie konsumentów o suplementach, które pojawiają się na rynku bez powiadomienia GIS oraz regulacje procedur wycofywania suplementów diety z rynku.

Ponadto pożądane jest podjęcie działań zarówno edukacyjnych, jak i informacyjnych w zakresie stosowania suplementów diety. Wskazane jest, aby były one prowadzone we współpracy z Ministerstwem Edukacji Narodowej oraz Ministerstwem Nauki i Szkolnictwa Wyższego w celu informowania i edukowania o zagrożeniach związanych z nieodpowiednim zażywaniem suplementów diety w placówkach oświatowych.

Dodatkowo zmiany powinny dotyczyć także reklamy suplementów diety. Miałyby one polegać na podwyższeniu maksymalnych poziomów kar, które mogą

być nakładane przez GIS na przedsiębiorstwa niespełniające wymogów co do opakowań, reklamy i promocji suplementów oraz na usprawnieniu monitoringu reklamy suplementów diety przez GIS oraz Urząd Ochrony Konkurencji i Konsumentów. Powinien też być wprowadzony zakaz reklamowania suplementów diety jako mających właściwości lecznicze lub terapeutyczne (Czerwiński, Liebers 2019, s. 19).

Literatura

1. Baraniak J. i in. (2020), *Istotne problemy związane z bezpieczeństwem surowców roślinnych obecnych w wybranych grupach suplementów diety*, „Postępy Fitoterapii”, 21, 3, s. 161-168.
2. Czerwiński A., Liebers D. (2019), *Regulacja rynku suplementów diety. Czy Polska ma szansę zostać europejskim liderem?*, Polski Instytut Ekonomiczny, Warszawa.
3. Departament Bezpieczeństwa Żywności i Żywienia (2020), *Rejestr produktów objętych powiadomieniem o pierwszym wprowadzeniu do obrotu*, <https://rejestrzp.gis.gov.pl/index.php/przegladaj/2008/169> (dostęp: 14.09.2021).
4. Dyrektywa 2002/46/WE Parlamentu Europejskiego i Rady z dnia 10 czerwca 2002 r. w sprawie zbliżenia ustawodawstw Państw Członkowskich odnoszących się do suplementów żywnościowych (Dz.Urz. WE L 185/51 z 12.7.2002).
5. Dziędziński M. i in. (2019), *Problem nadkonsumpcji suplementów diety przez Polaków*, „Intercathedra”, 3, 40, s. 235-242.
6. GIS (2018), *Szczegółowe wymagania prawne dotyczące suplementów diety*, <https://www.gov.pl/web/gis/szczegolowe-wymagania-prawne-dotyczace-suplementow-diety> (dostęp: 14.09.2021).
7. Karbownik M.S. in. (2019), *Knowledge about Dietary Supplements and Trust in Advertising Them: Development and Validation of the Questionnaires and Preliminary Results of the Association between Constructs*, „PLoS One”, 14, 6, s. 1-24.
8. NIK (2017), *NIK o dopuszczaniu do obrotu suplementów diety*, <https://www.nik.gov.pl/aktualnosc/NIK-o-dopuszczaniu-do-obrotu-suplementow-diety.html> (dostęp: 14.09.2021).
9. Rozporządzenie WE nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz.Urz. WE L 31/1 z 1.2.2002).
10. Stępień K.A., Niewiarowski J., Harasimiuk A. (2019), *Powszechność suplementów diety a zagrożenia związane z ich stosowaniem*, „Biuletyn Wydziału Farmaceutycznego Warszawskiego Uniwersytetu Medycznego”, 9, s. 51-59.
11. Stoś K. (2017), *Czy suplementy diety są bezpieczne*, <https://ncez.pzh.gov.pl/abc-zywienia/czy-suplementy-diety-sa-bezpieczne> (dostęp: 15.09.2021).
12. SW Research (2017), *Polacy a suplementy diety. Raport badawczy*, https://swresearch.pl/pdf/Polacy%20a%20suplementy%20diety_raport%20badawczy.pdf (dostęp: 15.09.2021).
13. Ustawa z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (Dz.U. nr 171 poz. 1225, ze zm.).

DIET SUPPLEMENTS AND CONSUMER HEALTH MANAGEMENT

Abstract: This chapter is addressing the problem of a growing tendency to consume dietary supplements in recent years as well as the methods of counteracting and minimizing the threats that may result from this phenomenon. The conducted research comprised the analysis of available scientific publications, reports and statistical data. On the basis of the research, it was found that Poles more and more often reach for dietary supplements, even though their knowledge about the benefits and risks of taking them and about the regulations governing their admission to sale is limited and

that the use of dietary supplements is not always safe. The obtained results also suggest the need to undertake the activities in the field of health safety management aiming at education in the use of dietary supplements and the introduction of changes in legal regulations and institutional solutions functioning on the dietary supplements market.

Keywords: dietary supplements, health safety, management

Rozdział 2

AKREDYTACJA PODMIOTÓW LECZNICZYCH CELEM ZWIĘKSZENIA POCZUCIA BEZPIECZEŃSTWA PACJENTÓW

Żaneta Mrozek²

Streszczenie: Wdrażanie akredytacji w podmiotach leczniczych ma w pierwszej kolejności wpływać na poszukiwanie rozwiązań podnoszących funkcjonowanie i jakość placówek oraz świadczeń medycznych. Wysoka jakość usług medycznych zwiększa poczucie bezpieczeństwa pacjentów, a także wpływa na cały system ochrony zdrowia. Jednak wdrażane rozwiązania projakościowe nie spełniają standardów oczekiwanych przez pacjentów. Samo posiadanie akredytacji łączy się przede wszystkim z kwestiami finansowymi. Bez stworzenia warunków i zaangażowania personelu trudno realizować misję akredytacji, tym bardziej w zmieniającym się środowisku bezpieczeństwa. Celem rozdziału jest próba oceny wpływu akredytacji na poczucie bezpieczeństwa pacjentów.

Słowa kluczowe: akredytacja, bezpieczeństwo, jakość, pacjent, podmiot leczniczy

Wprowadzenie

Jakość w ochronie zdrowia oznacza zbiór działań odnoszących się do różnych obszarów funkcjonowania systemu opieki zdrowotnej. Zaspokojenie potrzeb w zakresie profilaktyki, leczenia czy diagnostyki wpływa na poziom zadowolenia, a tym samym na bezpieczeństwo pacjenta, i jest realizowane na poziomie konkretnych podmiotów leczniczych. Akredytacja nie jest jedynym gwarantem jakości usług medycznych, ani żaden inny wdrażany projakościowy system zarządzania podmiotem leczniczym. Należy pamiętać, że ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, przepisy o działalności leczniczej czy inne rozporządzenia już regulują kwestie dotyczące jakości poprzez określone wymagania, które należy spełniać przy realizacji konkretnych świadczeń medycznych, np. dotyczące zasobów rzeczowych lub personelu medycznego (Dz.U. 2018 poz. 2190, ze zm.; Dz.U. 2019 poz. 1373, ze zm.). Akredytacja określa zasady i standardy, jakie musi wypełniać podmiot leczniczy, aby został uznany za jednostkę, w której

² Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie, Instytut Nauk o Bezpieczeństwie

świadczenia medyczne są udzielane w sposób właściwy i pożądanym (Dobska, Dobski 2016, s. 225). Posiadanie akredytacji daje przywileje jednostce oraz jest korzystne w obszarze finansowania, a więc jest kluczowe dla kadry zarządzającej podmiotem. Sytuacja natomiast wygląda inaczej w przypadku personelu medycznego i niemedycznego zatrudnionego w takiej placówce oraz dla pacjentów. Oprócz pożądanego korzyści wynikających z poprawy warunków udzielania świadczeń oraz ustalonych algorytmów i procedur nie ma zadawalających benefitów dla personelu. Idea i misja akredytacji są obietnicą lepszej jakości udzielania świadczeń medycznych. Nie można jednak pominąć faktu, że za jakością usług stoją konkretne osoby, bez zaangażowania których nie ma szans na realizację misji. Akredytacja jawi się więc jako ten element funkcjonowania podmiotu leczniczego, który ma służyć tylko celom finansowym, nie zwiększając poczucia bezpieczeństwa wśród pacjentów, co potwierdziła m.in. kontrola NIK w wybranych podmiotach. Istotna jest tu również kwestia rozumienia złożoności relacji uczestników w usługach zdrowotnych, a w szczególności ważnego jej elementu, jakim jest asymetria informacji, która wpływa na poczucie bezpieczeństwa. Bezpieczeństwo zdrowotne w tym przypadku jest również determinowane ogólnym funkcjonowaniem systemu opieki zdrowotnej, zwłaszcza jego newralgiczny aspekt związany z dostępnością do świadczeń medycznych, który oceniany jest źle w licznych badaniach opinii społeczeństwa.

Specyfika akredytacji

Akredytacja miała swój początek w USA w 1910 roku, kiedy to E. Codman zaproponował ocenę funkcjonowania szpitali opartą na wynikach leczenia. W roku 1918 Kolegium Chirurgów opublikowało pierwszy standard, który zapoczątkował akredytację. Następnie na przestrzeni lat wprowadzono kolejne standardy i sposoby oceny placówek oraz powołano Komisję Wspólną ds. Akredytacji Szpitali (1965 r.), której nazwa została zmieniona w 1987 roku na Komisję Wspólną ds. Akredytacji Instytucji Opieki Zdrowotnej. Standardy akredytacyjne były adaptowane do zmieniającego się sposobu funkcjonowania placówek medycznych, obejmując swoim zasięgiem różne obszary ich działalności. W 1995 roku zdefiniowano akredytację jako zewnętrzny, wykonywany przez niezależną instytucję proces oceny podmiotów, które zdecydowały się poddać tej ocenie w sposób dobrowolny. W Polsce powołano Centrum Monitorowania Jakości w Ochronie Zdrowia (CMJ) jako tę jednostkę, która przy współpracy z ministerstwem zdrowia miała wspierać działania na rzecz poprawy jakości usług medycznych, m.in. poprzez opracowanie standardów akredytacyjnych (Dz.Urz. MZ nr 9 poz. 59, ze zm.). W świetle najnowszego projektu ustawy o jakości w ochronie zdrowia (Projekt ustawy 2021) CMJ miałyby zostać zlikwidowane, a Narodowy Fundusz Zdrowia (NFZ) przejąłby funkcję przyznawania podmiotom leczniczym akredytacji. Należy tu dodać, że NFZ jest płatnikiem świadczeń, a posiadanie akredytacji stanowi element dodatkowy uwzględniany w finansowaniu placówek.

Program Akredytacji Szpitali w Polsce powstał w 1998 roku, a po 10 latach doświadczenia ze standardami akredytacyjnymi uchwalona została ustawa o akredytacji w ochronie zdrowia (Dz.U. 2009 r. nr 52 poz. 418). Ustawa ta reguluje kwestie

jakości w ochronie zdrowia. Obejmuje wszystkie obszary działalności podmiotu leczniczego, zarówno te dotyczące świadczeń medycznych, jak również zarządzania i administracji, gdyż sprawnie funkcjonujący podmiot leczniczy determinuje jakość usług medycznych. Akredytację przyznaje minister zdrowia na podstawie rekomendacji Rady Akredytacyjnej na okres 3 lat (Dz.U. nr 150 poz. 1216, ze zm.; Dz.U. nr 130 poz. 1074, ze zm.). Standardy akredytacyjne są opracowane przez Centrum Monitorowania Jakości w Ochronie Zdrowia dla szpitali i POZ i są zatwierdzone przez ministra zdrowia (CMJ 2016; CMJ 2016a). Ponadto jednostka ta jest podległa ministrowi i monitoruje jakość świadczeń zdrowotnych. Akredytacja jest dobrowolna, ale ma znaczenie w przypadku podpisywania umów z NFZ. W opinii wielu ekspertów może ona wpływać na decyzje zmierzające do poddania się procesowi akredytacji nie tylko z uwagi na finansowanie, ale także z chęci podnoszenia jakości usług medycznych. Według CMJ założeniem akredytacji, oprócz dobrowolnego uczestnictwa, jest jego autonomiczność, tzn. program akredytacji jest jednolity dla wszystkich ubiegających się jednostek, opiera się na standardach, ma cel edukacyjny polegający na informowaniu, prowadzeniu szkoleń i wymiany doświadczeń z innymi organizacjami posiadającymi już akredytację. Ponadto założeniem akredytacji jest działanie z określoną procedurą oraz rzetelna i wiarygodna ocena podmiotów według wcześniej ustalonych zasad (CMJ 2011; Dytko 2019, s. 40-55).

Procedura przyznawania akredytacji składa się z 3 faz: przygotowawczej, wizyty oraz decyzji akredytacyjnej. Bazuje na standardach, które zostały opracowane osobno dla szpitali i osobno dla podstawowej opieki zdrowotnej. Standardy te głównie dotyczą opieki nad pacjentem, ogólnego funkcjonowania jednostki oraz sposobu udzielania świadczeń pacjentowi. Ocena takiej placówki ma charakter ilościowy (np. dostępność personelu, aparatura medyczna) oraz jakościowy (np. poziom wykształcenia personelu medycznego) i jest dokonywana przez zewnętrzny podmiot (por. Romańczyk, Biedlicki 2006; Szetela 2010, s. 70-75).

Sama akredytacja jest metodą, która ma zapewnić jakość i w odróżnieniu od innych systemów zarządzania jakością, np. zgodnych z normami ISO 9001 czy ISO 9004, jest stworzona tylko do oceny podmiotów ochrony zdrowia. Inne systemy projakościowe również mogą i często wraz z akredytacją są wdrażane w placówce, natomiast odróżnia te systemy sposób oceniania oraz zasady przyznania certyfikatu (por. Głód 2017, s. 82-93). W przypadku ISO 9001 czasem jedna niezgodność może przekreślić możliwość uzyskania certyfikatu. Chociaż akredytacja bazuje i wymaga spełnienia wielu standardów, jej przyznawanie jest bardziej liberalne, tzn. może być przyznana podmiotowi, gdy spełnia on 75-100% tych standardów. Podmiot leczniczy może również otrzymać akredytację warunkową w sytuacji, kiedy spełnia 70-74% standardów, a zastrzeżenia dotyczą wybranego obszaru działań (np. leki – standardy w tym przypadku dotyczą kwalifikacji osób zajmujących się farmaceutykami, a także receptariusza ze stosowaną listą leków, która jest na bieżąco aktualizowana i monitorowana itp.). Placówka taka otrzymuje akredytację na okres jednego roku, po czym dokonuje się rewizyty i powtórnej oceny. Akredytacja może też zostać przyznana tymczasowo dla organizacji rozpoczynających działalność. Natomiast odmowa akredytacji ma miejsce wtedy, gdy podmiot spełnia standardy poniżej 70% (Dobska, Dobski 2004, s. 163-170; Opolski, Dykowska, Możdżonek

2009, s. 77-80; Dobska, Rogoziński 2012, s. 280-282). Wśród korzyści i celów akredytacji, prócz zwiększenia poziomu jakości usług, wymienia się: zwiększenie bezpieczeństwa pracowników m.in. poprzez wdrożenie standardów epidemiologicznych, zwiększenie zadowolenia i satysfakcji pacjentów, ujednoczenie zasad sprawowania opieki nad chorym, redukcję kosztów, zwiększenie efektywności, poznanie oczekiwań pracowników, monitorowanie funkcjonowania i własnej działalności, sprzyjanie konkurencyjności szpitala, polepszenie stanu technicznego placówki oraz budowanie strategii marketingowej (Opolski, Dykowska, Możdżonek 2009, s. 73-74).

Akredytacja jest znana, a jej zasady stosowane nie tylko w Polsce, ale i w innych krajach. Ideą jest zapewnienie okoliczności, które przysporzą maksymalnych korzyści dla pacjenta, uwzględniając możliwości danego państwa. Aktualnie poszukuje się przede wszystkim takich rozwiązań, które mają kluczowe znaczenie dla jakości usług medycznych. Nigdzie nie ma jednolitego wzorca, co wynika z dynamiki zmian w ochronie zdrowia. Uskutecznienie działań projakościowych wymaga więc przeznaczenia odpowiednich środków finansowych, wykorzystania doświadczenia innych państw oraz wbudowanie pewnych komponentów w cały system.

Złożoność relacji w usługach zdrowotnych

Jakość usług zdrowotnych zależy od wielu zmiennych, a ocena pacjenta dotycząca realizacji świadczenia ma charakter subiektywny. Od jakości i sposobu udzielenia świadczenia zdrowotnego zależy życie, zdrowie i satysfakcja pacjenta. Dlatego przyjmuje się, że jakość powinna być stale udoskonalana, ponieważ przyczynia się do zwiększenia poczucia bezpieczeństwa. Jest wiele koncepcji określających, czym jest jakość usług. Według jednej z nich (koncepcja A. Donabediana) podejście do usług medycznych ma trzy wymiary: pierwszy dotyczy wartości technicznej (np. wiedza, technologia, procedury), drugi wymiar związany jest z wartością stosunków międzyludzkich, natomiast trzeci, ostatni wymiar, to oprawa usług, czyli np. poczucie komfortu, estetyka, obsługa itd. Zadowolenie pacjenta zależy więc od harmonii wszystkich wymienionych wymiarów. Zauważa się tu złożoność relacji, jaka zachodzi między świadczeniodawcą, świadczeniobiorcą oraz podmiotami zewnętrznymi biorącymi udział w procesie. Satysfakcja pacjenta jest zatem determinowana wieloma kryteriami (Krot 2008, s. 37-42). W ocenie satysfakcji należy uwzględnić medyczne i niemedyczne aspekty usługi. Przykładowo ważnym elementem będzie kwestia dotycząca poszanowania godności pacjenta, wiarygodność, zaufanie i uczciwość, prawo do dokładnej i wyczerpującej informacji, poufność, kontynuacja leczenia, dostęp do wsparcia socjalnego i psychicznego, niezawodność związana z odpowiednimi kwalifikacjami personelu, odpowiednie warunki bytowe, możliwość wyboru lekarza, ale także dostępność do świadczenia. Należy tu dodać, że dostępność zależy od środków finansowych, jak również od polityki zdrowotnej, niemniej jednak w kontekście bezpieczeństwa jest kluczowa, gdyż ważne jest, aby pacjent uzyskał pomoc w momencie, kiedy tego potrzebuje. Prócz doskonałości technicznej i relacji między pacjentem a personelem medycznym, w celu zapewnienia i doskonalenia jakości, kadra zarządzająca powinna także dbać o kontakty

z personelem medycznym (marketing wewnętrzny). Placówki posiadające systemy zarządzania jakością powinny uwzględniać ocenę subiektywną oraz aspekt pożądaných oczekiwań co do poziomu świadczonej usługi poprzez identyfikację i eliminację błędów (Jedynak 2007, s. 94-95; Staszewska 2010, s. 116-117). Akredytacja jest tu więc pewnym gwarantem i informacją dla pacjenta, że usługi medyczne wykonywane w tym podmiocie spełniają wszelkie wymagania proceduralne, co ma zapewnić poczucie bezpieczeństwa i komfort. Pacjent, wybierając konkretną placówkę, kieruje się różnymi kryteriami, m.in. o wyborze decyduje oferta, jaką składa podmiot. Wybór ten wiąże się z wejściem w określoną relację. Pojęcie relacji świadczeniodawca – świadczeniobiorca również jest szeroko rozumiane, ponieważ pacjent wchodzi w interakcję z różnym, licznym personelem medycznym, który jest zatrudniony w danym podmiocie leczniczym. Relacja ta jest częścią bardziej złożonej struktury, w skład której wchodzi także płatnik, determinujący możliwość i dostępność świadczeń medycznych dla pacjenta, ale też i inne instytucje oddziałujące na funkcjonowanie podmiotu. Najistotniejsze jednostki uczestniczące i mające wpływ na realizację usług medycznych i ich jakość z uwzględnieniem akredytacji przedstawia rysunek 2.1



Rysunek 2.1. Zakres relacji między świadczeniobiorcą, świadczeniodawcą i płatnikiem z uwzględnieniem akredytacji

Źródło: opracowanie własne

Interakcja, jaka zachodzi między pacjentem a personelem medycznym, jest istotna w końcowej ocenie zadowolenia pacjenta z usługi medycznej. Kluczowe elementy procesu realizacji usługi to odpowiednia komunikacja i profesjonalizm, ale ważny jest także aspekt emocjonalny (empatia), społeczny czy edukacyjny.

Oczekiwanym efektem każdej usługi zdrowotnej jest rozwiązanie problemu dotyczącego zdrowia. Należy tu zwrócić uwagę na komunikację, gdyż świadcząc usługę zdrowotną, mamy przede wszystkim do czynienia z wymianą informacji między stronami relacji. Pacjent zgłaszający się z problemem zdrowotnym jest uzależniony od opinii i wyboru sposobu postępowania personelu medycznego (najczęściej lekarza), któremu musi zaufać (co wynika z jego niekompetencji i braku wiedzy w dziedzinie medycyny). Zachodzi tu zjawisko asymetrii informacji, które polega na tym, że pacjent nie zgłasza się z jasno określonymi wymaganiami co do technicznej strony usługi i decyduje się na to, co zostanie zaproponowane przez usługodawcę, w tym przypadku lekarza (Rudawska 2007, s. 28-30). Lekarz decyduje także o liczbie oraz rodzaju świadczeń medycznych, które zostaną zrealizowane. Na lekarzu spoczywa w tym przypadku odpowiedzialność za stworzenie takiej relacji z chorym, która umożliwi mu skuteczne przeprowadzenie procedur medycznych adekwatnych do danego problemu zdrowotnego i ku zadowoleniu pacjenta. Należy tu dodać, że efektem realizacji usługi medycznej nie zawsze jest wyzdrowienie, ale czasami tylko wpłynięcie na poprawę jakości życia chorego, np. w chorobach terminalnych. Dlatego w komunikacji między lekarzem a pacjentem ważny jest każdy szczegół: od przekazania informacji, poprzez zachowanie intymności i poufności, po aspekty werbalne i niewerbalne towarzyszące temu procesowi. Dodatkowo pacjent, z uwagi na troskę o własne życie i zdrowie, jest wymagający, bardziej wrażliwy i krytyczny na aspekty towarzyszące procesowi świadczenia usług (Tobiasz-Adamczyk 2002, s. 39-52; Barański 2002, s. 158-161; Mrożek 2018, s. 276-281). Skuteczność komunikacyjna jest kluczowa, gdyż wiąże się z konsekwencjami ekonomicznymi, wpływa m.in. na liczbę błędów medycznych, trafność diagnozy czy szybkość rekonwalescencji. Każdy z tych skutków wiąże się z kosztami, które wpływają na efektywność funkcjonowania podmiotów leczniczych. Podsumowując, można stwierdzić, że rola personelu medycznego, głównie lekarza, jest priorytetowa, jeśli mówimy o jakości realizacji usług zdrowotnych i bezpieczeństwie pacjenta. Akredytacja ma tu na celu stworzenie warunków do budowania jak najlepszych relacji, wpływając jednocześnie na całe otoczenie podmiotu, uwypuklając jego walory i kreując wizerunek.

Akredytacja a bezpieczeństwo pacjenta

Placówki posiadające akredytację są traktowane jako kompetentne podmioty, które spełniają określone zadania wobec pacjenta, przyczyniając się do zwiększenia jego poczucia bezpieczeństwa. Misją akredytacji jest poprawa jakości usług zdrowotnych poprzez m.in. polepszenie warunków technicznych podmiotów leczniczych czy polepszenie sytuacji finansowej.

Aktualnie w Polsce akredytację posiadają 173 szpitale oraz 243 placówki podstawowej opieki zdrowotnej (stan na 20.09.2021). Według danych CMJ wśród szpitali najwyższy uzyskany wynik to 95% zgodności ze standardami, natomiast średni poziom spełniania standardów to 81,4%. W przypadku akredytowanych POZ maksymalny uzyskany poziom zgodności wyniósł 99%, a średni poziom spełniania standardów stanowił 85,8% (CMJ 2021; CMJ 2021a). Podczas wizyt akredytacyjnych w 2020 roku w przypadku POZ najniższy poziom spełniania standardów

odnotowano w działach Dokumentacji Medycznej oraz w Zespole Współpracowników, mediana wyników wyniosła 70%. W przypadku szpitali w tym samym roku najniższe wyniki uzyskały działy zajmujące się Poprawą Jakości i Bezpieczeństwem Pacjenta, gdzie prawie 18% szpitali uzyskało mniej niż 50% spełnienia wymogów standardów akredytacyjnych (CMJ 2021; CMJ 2021a). Standardy Poprawy Jakości i Bezpieczeństwa Pacjenta dotyczą ciągłego monitorowania, analizowania i doskonalenia procesów klinicznych i zarządzania. Skuteczność tutaj jest uzależniona od koordynacji wszystkich działań osób zatrudnionych w danym podmiocie. Natomiast poprawa jakości jest nakierowana na redukcję ryzyka zarówno pacjenta, jak i personelu. Standardy w tym obszarze dotyczą bezpieczeństwa pacjenta, które jest podstawowym wymiarem jakości opieki i stanowi integralny element systemu poprawy opieki. Dlatego niepokojące jest to, że szpitale ubiegające się o certyfikat, mając czas na przygotowanie się, zaniedbują ten dział (CMJ 2016). Co więcej, również podmioty posiadające certyfikat nie zawsze wywiązują się z założeń akredytacyjnych, co potwierdziła m.in. kontrola NIK, która została przeprowadzona w wybranych placówkach i obszarach ich funkcjonowania podlegających ocenie. Kontrola NIK obejmowała lata 2016-2019, liczba szpitali posiadających w tym czasie certyfikat była większa i wynosiła prawie 220, a placówek POZ – 170. Według raportu NIK system akredytacji zamiast stymulować podmioty do wdrażania rozwiązań poprawiających ich funkcjonowanie m.in. poprzez identyfikację zdarzeń niepożądanych czy propagowanie idei projakościowych, w praktyce nie zapewniał trwałości wdrażanych zmian. Zamiast prowadzenia działalności zgodnie ze standardami, szpitale koncentrowały się jedynie na samym uzyskaniu certyfikatu celem podniesienia prestiżu placówki oraz z uwagi na korzyści finansowe, które od 2018 roku dawało wymierne korzyści w ramach ryczałtu systemu zabezpieczeń świadczeń zdrowotnych. Według NIK 75% szpitali, które zostały objęte kontrolą i posiadały certyfikat, nie zapewniało standardów, które CMJ uznało za wdrożone. Dopatrzone się wielu uchybień w takich obszarach działalności jak np. poprawa jakości (spotkania zespołów do spraw jakości), szkoleń personelu w zakresie zakażeń i resuscytacji krążeniowo-oddechowej, farmakoterapii oraz w opiece nad pacjentem, gdzie nie zapewniano kompleksowości zestawów stosowanych w stanach nagłego zagrożenia życia. Ponadto zarzucono CMJ, że wytyczne zawarte w standardach były niejednoznaczne i przez to różnie interpretowane przez podmioty. Skutkowało to tym, że CMJ przyznawało punkty w sposób uznaniowy, szpital przekonywał, że funkcjonuje zgodnie ze standardami, chociaż tak nie było. Również ministrowi zarzucono brak właściwego nadzoru na działalnością CMJ. Ministerstwo tłumaczyło się pracami nad nowym projektem ustawy o jakości w ochronie zdrowia i bezpieczeństwie pacjenta (NIK 2020). Projekt, o którym mowa, przewiduje m.in. przeniesienie uprawnień do przyznawania akredytacji z CMJ do NFZ. NIK przedstawił także działania naprawcze mające na celu poprawę funkcjonowania systemu akredytacji poprzez zmianę standardów polegającą na tym, że powinny zostać wprowadzone wytyczne umożliwiające poprawne zweryfikowanie i ocenę podczas procesu akredytacji. Drugą sugestią naprawczą było wzmocnienie liczebności wizytatorów oraz wydłużenie samej wizyty akredytacyjnej. Główne zalecenia oscylowały wokół doprecyzowania procesu

akredytacji. Pominięty został na przykład aspekt zaangażowania personelu medycznego realizującego świadczenia zdrowotne, od którego zależy skuteczność wdrożonych zmian.

Projekt ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, prócz wspomnianego przeniesienia uprawnień do przyznawania akredytacji na płatnika świadczeń, przewiduje zmiany poprzez wdrożenie rozwiązań prawno-organizacyjnych, które mają w sposób kompleksowy realizować priorytety polityki zdrowotnej w obszarze jakości. Rozwiązania, o których mowa, dotyczą: usprawnienia akredytacji, monitorowania zdarzeń niepożądanych, autoryzacji podmiotów wykonujących działalność leczniczą, którą mają dokonywać dyrektorzy oddziałów NFZ, usprawnienia związane z wypłatą pacjentom rekompensat za zdarzenia medyczne oraz tworzenia i prowadzenia rejestrów medycznych. Autoryzacja podmiotów będzie warunkowała uczestnictwo szpitala w systemie podstawowego zabezpieczenia zdrowotnego tzw. „sieci szpitali”. Projekt przewiduje wewnętrzny system zapewnienia jakości i bezpieczeństwa, który będzie obligatoryjny dla szpitali, niezależnie od faktu korzystania ze środków publicznych (Projekt ustawy 2021). Usprawnienie akredytacji ma polegać m.in. na uporządkowaniu procesu akredytacji, wprowadzeniu możliwości cofnięcia akredytacji oraz określeniu warunków udzielania akredytacji poprzez spełnienie standardów obligatoryjnych i uzyskania minimum 50% punktów z każdego działu standardów.

Wdrażanie standardów akredytacyjnych nie uwzględnia sytuacji wynikającej z faktu, że podmioty lecznicze funkcjonują w zmieniającym się środowisku bezpieczeństwa. Takie zjawiska jak epidemie, pandemie czy masowe zdarzenia kryzysowe wymagają innych procedur, nierzadko niestandardowych, stwarzając tym samym warunki, które uniemożliwiają stosowanie się do ustalonych algorytmów postępowania. Prócz tego w każdych kolejnych badaniach opinii społeczeństwa funkcjonowanie systemu opieki zdrowotnej oceniane było negatywnie: w 2020 roku tak uważało 58%, a w 2018 roku 66%. Niewielki spadek ocen negatywnych wynika z tego, że Polacy doceniają zaangażowanie personelu medycznego w walce z pandemią. Przed pandemią respondenci stosunkowo dobrze ocenili dostępność do usług lekarzy podstawowej opieki, natomiast najgorzej ocenili dostępność usług lekarzy specjalistów i badań specjalistycznych oraz liczbę personelu medycznego w szpitalach. Niemniej jednak docenili kompetencje personelu i infrastrukturę podmiotów. Uważali, że problemy z dostępnością i jakością świadczeń wynikają z niewystarczających, a także źle zagospodarowanych środków finansowych. Problem z dostępnością pogłębił się z powodu pandemii COVID-19, blisko co trzeci badany zadeklarował, że przełożono lub odwołano mu wizytę u lekarza specjalisty (30%), i ci, którzy doświadczyli tych trudności, bardziej krytycznie postrzegają funkcjonowanie opieki zdrowotnej (CBOS 2018; CBOS 2020). Resumując, należy podkreślić, że wprowadzanie rozwiązań projakościowych do podmiotów leczniczych nie gwarantuje jakości oczekiwanej, wpływa natomiast na finansowanie. Sam proces akredytacji wymaga doskonalenia i zmian. Trudno stwierdzić, czy dotychczasowe działania wpłynęły

znacząco na zwiększenie poczucia bezpieczeństwa pacjentów. Są to jednak metody, które dają obietnicę lepszej jakości.

Podsumowanie

Idea rozwiązań projakościowych jest jak najbardziej pożądana, tym bardziej, że przy zaangażowaniu personelu jest większa szansa na zmniejszenie zdarzeń niepożądanych ku satysfakcji pacjenta i kadry zarządzającej, przyczyniając się do zwiększenia poczucia bezpieczeństwa. Jednak wdrożenie ich w podmiotach to dla personelu medycznego kolejne, dodatkowe obowiązki, których wypełnianie w żaden sposób nie jest wynagradzane. Dodatkowo szpitale, zwłaszcza publiczne, borykają się z problemami kadrowymi i finansowymi, co wiąże się z ograniczoną dostępnością do świadczeń medycznych. Niemniej jednak prowadzenie rachunku kosztów jakości powinno przynosić korzyści dla podmiotu poprzez monitorowanie jego działalności. Koszty jakości traktuje się jako mierniki jakości. Dla przykładu przestrzeganie norm i większe zaangażowanie personelu to mniej błędów, mniej spraw sądowych, co automatycznie obniża koszty funkcjonowania podmiotu wynikające ze złej jakości (Opolski, Dykowska, Możdżonek 2009, s. 185). Ponadto jeżeli system reglamentuje świadczenia, a finansowanie jest niewystarczające, oraz gdy brakuje procedur zabezpieczających potrzeby zdrowotne w zmieniającym się środowisku bezpieczeństwa, to nawet najlepiej wdrożone systemy projakościowe w placówkach nie wpłyną istotnie na poczucie bezpieczeństwa, co jest widoczne zwłaszcza w publicznych podmiotach.

Literatura

1. Barański J. (2002), *Interakcja lekarz – pacjent*, [w:] Barański J., Piątkowski W. (red.), *Zdrowie i choroba. Wybrane problemy socjologii medycyny*, s. 158-161, Oficyna Wydawnicza Atut, Wrocław.
2. CBOS (2018), *Opinie na temat funkcjonowania opieki zdrowotnej*, „Komunikat z Badań”, 89.
3. CBOS (2020), *Opieka medyczna w czasie epidemii*, „Komunikat z Badań”, 88.
4. CMJ (2011), *Program akredytacji szpitali. Przewodnik po procesie*, Kraków.
5. CMJ (2016), *Zestaw standardów akredytacyjnych. Szpitale*, Kraków.
6. CMJ (2016a), *Zestaw standardów akredytacyjnych. Podstawowa opieka zdrowotna*, Kraków.
7. CMJ (2021), *Poziomy spełniania standardów akredytacyjnych dla placówek podstawowej opieki zdrowotnej w 2020 roku*, Kraków.
8. CMJ (2021a), *Poziomy spełniania standardów akredytacyjnych dla szpitali w 2020 roku*, Kraków.
9. Dobska M., Dobski P. (2004), *TQM zarządzanie przez jakość w zakładach opieki zdrowotnej*, Mars Graf, Poznań.
10. Dobska M., Dobski P. (2016), *Systemy zarządzania jakością w podmiotach leczniczych*, Wolters Kluwer, Warszawa.
11. Dobska M., Rogoziński K. (2012), *Podstawy zarządzania zakładem opieki zdrowotnej*, Wydawnictwo Naukowe PWN, Warszawa.
12. Dytko J. (2019), *Postępowania w sprawie akredytacji w ochronie zdrowia*, „Studia Prawnicze KUL”, 2, 78, s. 40-55.

13. Głód G. (2017), *W kierunku integracji systemów zarządzania jakością i ryzykiem w publicznych jednostkach ochrony zdrowia*, „Studia Ekonomiczne. Zeszyty Naukowe”, 316, s. 82-93.
14. <https://www.cmj.org.pl/> (dostęp: 14.09.2021).
15. Jedynak P. (2007), *Ocena znormalizowanych systemów zarządzania jakością. Instrumenty i uwarunkowania wartości*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków.
16. Krot K. (2008), *Jakość i marketing usług medycznych*, Wolters Kluwer, Warszawa.
17. Mrożek Ż. (2018), *Polityczny i prakseologiczny wymiar przekształceń systemu ochrony zdrowia w Polsce w latach 1997-2015*, Wydawnictwo Sztafeta, Kraków.
18. NIK (2020), *Akredytacja podmiotów leczniczych*, nr ewid. 187/2019/P/19/095/LPO.
19. Opolski K., Dykowska G., Moźdzzonek M. (2009), *Zarządzanie przez jakość w usługach zdrowotnych. Teoria i praktyka*, CeDeWu, Warszawa.
20. Projekt ustawy z dnia 22 lipca 2021 r. o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, nr UD 255.
21. Romańczyk T., Bedlicki M. (2006), *Zharmonizowany system zarządzania jakością w ochronie zdrowia. Wymagania dla normy ISO 9001:2000 i dla akredytacji wg standardów CMJ, TÜV NORD Polska*, Katowice.
22. Rozporządzenie Ministra Zdrowia z 31 sierpnia 2009 r. w sprawie procedury oceniającej spełnienie przez podmiot udzielający świadczeń zdrowotnych standardów akredytacyjnych oraz wysokości opłat za jej przeprowadzenie (Dz.U. nr 150 poz. 1216, ze zm.).
23. Rozporządzenie Ministra Zdrowia z 6 sierpnia 2009 r. w sprawie Rady Akredytacyjnej (Dz.U. nr 130 poz. 1074, ze zm.).
24. Rudawska I. (2007), *Opieka zdrowotna aspekty rynkowe i marketingowe*, Wydawnictwo Naukowe PWN, Warszawa.
25. Staszewska A. (2010), *Ocena jakości usług medycznych w opinii pacjentów*, [w:] Lisiecka-Bielanowicz M., Samoliński B., Warczyński P. (red.), *Kierunki doskonalenia usług w ochronie zdrowia*, s. 115-125, Ministerstwo Zdrowia, Warszawa.
26. Szetela P. (2010), *Zewnętrzne systemy oceny jakości w zakładach opieki zdrowotnej: system zarządzania jakością wg normy EN-ISO 9001:2008 a system akredytacji*, [w:] Lisiecka-Bielanowicz M., Samoliński B., Warczyński P. (red.), *Kierunki doskonalenia usług w ochronie zdrowia*, Ministerstwo Zdrowia, Warszawa.
27. Tobiasz-Adamczyk B. (2002), *Relacje lekarz – pacjent w perspektywie socjologii medycyny*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków.
28. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. 2018 poz. 2190, ze zm.).
29. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2019 poz. 1373, ze zm.).
30. Ustawa z dnia 6 listopada 2008 r. o akredytacji w ochronie zdrowia (Dz.U. 2009 nr 52 poz. 418).
31. Zarządzenie Ministra Zdrowia z 2 lipca 2010 r. w sprawie Centrum Monitorowania Jakości w Ochronie Zdrowia (Dz.Ur. MZ nr 9 poz. 59, ze zm.).

ACCREDITATION OF HEALTHCARE PROVIDERS TO INCREASE PATIENT SAFETY

Abstract: The implementation of accreditation in medical entities is to primarily affect the search for solutions to improve the functioning and quality of facilities and medical services. High quality of medical services increases the sense of security of patients, and also affects the entire health care system. However, the implemented pro-quality solutions do not meet the standards expected by patients. Having accreditation itself is primarily associated with financial issues. Without the creation of conditions and involvement of staff, it is difficult to carry out the mission of accreditation, even more so in the changing security environment. The aim of this chapter is to assess the impact of accreditation on patients' sense of security.

Keywords: accreditation, patient, healthcare provider, quality, safety

Rozdział 3

ROLA WSPARCIA PSYCHOLOGICZNEGO I TERAPII W PROCESIE ADAPTACJI SPOŁECZNEJ OSÓB NIEPEŁNOSPRAWNYCH

Dorota Lizoń-Szłapowska³

Streszczenie: Rozdział poświęcony jest ocenie istoty i znaczenia wsparcia psychologicznego, w tym terapii indywidualnej, w procesie budowania bezpieczeństwa społecznego osób niepełnosprawnych posiadających orzeczenie o stopniu niepełnosprawności. Potrzeba organizacji tego typu działań w wymiarze instytucjonalnym stanowi istotny czynnik decydujący o wzmocnieniu indywidualnego mechanizmu przystosowania i adaptacji społecznej osoby z niepełnosprawnością (zwłaszcza w sytuacji pandemii). Celem rozdziału jest analiza problematyki wsparcia rozumianego jako działanie dostępne i wysokospecjalistyczne, dostosowane do potrzeb oraz oczekiwań osoby niepełnosprawnej, które przeciwdziałają zaburzeniom w funkcjonowaniu jednostki. Jest to działanie na rzecz budowania i podtrzymywania relacji społecznych, indywidualnej niezależności i autonomii osobistej zapobiegającej wykluczeniu i izolacji społecznej.

Słowa kluczowe: niepełnosprawność, terapia, wsparcie psychologiczne, zaburzenia

Wprowadzenie

Obserwacje, badania i liczne analizy badawcze procesu adaptacji osób niepełnosprawnych ukazują nie tylko złożony kontekst problematyki, ale skłaniają do refleksji na temat roli, jaką może odegrać wsparcie psychologiczne oraz terapia w procesie adaptacji społecznej osób niepełnosprawnych. Proces rehabilitacji społecznej, który bazuje na wszystkich sferach aktywności życiowej jednostki, będzie dążył do utrzymania względnie stałej równowagi jednostki i jej otoczenia. Koncepcje humanistyczne odnoszą się do szeroko rozumianej idei człowieka wszechstronnego, który – odpowiednio wspierany – potrafi mobilizować się do zmian.

Pojęcie „niepełnosprawności”

Niepełnosprawność to stan psychofizyczny, który w perspektywie czasowej może w sposób trwały lub czasowy uniemożliwiać jednostce realizację życiową.

³ Politechnika Częstochowska, Wydział Zarządzania

Niektóre lub wszystkie funkcje życiowe mogą być zaburzone, co powoduje w konsekwencji sytuację, w której człowiek wymaga pomocy specjalistycznej, takiej jak: rehabilitacja, leczenie, rewalidacja, kompensacja, korekcja, terapia czy wsparcie. Literatura problemu wskazuje na zróżnicowane przyczyny niepełnosprawności, co prowadzi do wyodrębnienia się w praktyce dwóch modeli:

- Model medyczny – bazuje na diagnozie możliwości jednostki dokonywanej przez specjalistów. Model ten jest ukierunkowany na przywracanie wszelkimi możliwymi sposobami sprawności jednostce, opierając się na opracowanych wcześniej strategiach (leczenie, rehabilitacja).
- Model społeczny – rozumiany jest jako wzbudzenie w jednostce motywacji do powrotu do zdrowia poprzez stworzenie optymalnych warunków do przywracania aktywności mimo choroby, zaburzeń, deficytów czy ograniczeń.

Niepełnosprawność może być określona jako swego rodzaju luka między stanem biologicznym, zdolnościami i możliwościami jednostki a barierami rozwojowymi, oczekiwaniami i wymogami ze strony społeczeństwa. Dochodzi tu do zaburzenia równowagi między zasobami a możliwościami jednostki (Wiliński 2010, za: Zawisła 2011, s. 16).

W literaturze socjologicznej występują dwie grupy koncepcji wyjaśniających niepełnosprawność:

- Koncepcje przynależności (funkcjonalne i funkcjonalno-strukturalne) – niepełnosprawność wpływa na ograniczone uczestnictwo w procesie socjalizacji, poprzez trudności w procesie komunikacji i współpracy, co prowadzi do powstania dystansu społecznego i może prowadzić do praktyk deprywacyjnych. Analiza niepełnosprawności oparta jest na kryteriach przydatności, użyteczności, wydajności jednostki.
- Koncepcje interakcyjne (dewiacji, atrybucji) – zaburzenia zachowania i ich przejawy są oceniane w kategorii ról. Kiedy jednostka nie jest w stanie jej sprostać, pojawiają się symptomy zaburzeń. W próbach definiowania odchyłeń mogą być stosowane sankcje i środki przemocy, co może doprowadzić do przypisania etykiety osobie niepełnosprawnej i definiowania jej odmienności, a to z kolei sprzyja praktykom dyskryminacyjnym, jak dyskryminacja stereotypowa czy ekskluzja, czyli wykluczenie z głównego nurtu życia (Jaglarz 2018, s. 197-200).

Pojęcie „wsparcia”

Termin „wsparcie społeczne” jest kojarzony z takimi pojęciami jak: pomoc, rodzaj interakcji społecznej, działania, troski, kompleks powiązanych ze sobą czynności. Wsparciu przypisuje się następujące wyjaśnienia:

- Po pierwsze – wsparcie jest procesem ciągłym, ukierunkowanym, może być udzielane indywidualnie lub grupowo.
- Po drugie – jest to także cykl działania, które może być: świadome, nieświadome, zamierzone, niezamierzone, niesformalizowane, nieprofesjonalne, ustrukturalizowane, nieformalne. Można przyjąć, że proces wspierania prowadzi do uzyskania autonomii osobistej, niezależności oraz samostanowienia o sobie.

Pomoc powinna być zorganizowana racjonalnie i logicznie, uwzględniając potrzeby jednostki, ale także jej możliwości. Praktycy sugerują również rozpoznanie słabych i mocnych stron. Źródła wsparcia określa się w praktyce jako pobudki, którymi kierujemy się przy udzielaniu pomocy, wynikające z etyki, religii, powinności, moralności czy altruizmu. W badaniach zwraca się uwagę na czynniki, które mogą wpływać na skuteczność wsparcia. Należą do nich: faza trudności, która często może mieć związek ze specyfiką problemu osoby niepełnosprawnej, dopasowanie do potrzeb, kontakt, współdziałanie, zrozumienie. W analizie i wyjaśnieniu terminu „wsparcia” przyjmujemy dwie perspektywy:

- Socjologiczna – rozumiana jako wsparcie zawarte w tle społecznym podejmowanych i doświadczanych kontaktów oraz stosunków społecznych, służy stabilizowaniu i integracji struktur społecznych (Modrzewski 2010, s. 18-19).
- Psychologiczna – rozumiana jako udzielanie pomocy dla jednostki w sytuacjach trudnych, wsparcie polega na dostarczeniu zasobów jednostce poprzez interakcje z innymi ludźmi (osoby znaczące, grupy odniesienia) (Walter 2016, s. 44).

Wsparcie w ujęciu strukturalnym oznacza istnienie obiektywnych i dostępnych sieci społecznych, które pełnią funkcję pomocową. Natomiast wsparcie w ujęciu funkcjonalnym oznacza rodzaj interakcji społecznej opartej na wzajemnych relacjach i sieci powiązań interpersonalnych. Podejście funkcjonalne wyróżnia model efektu głównego, czyli bezpośredniego, oraz model buforowy (obniżenie napięcia stresu), wykorzystanie własnych zasobów poprzez samostanowienie o sobie (Lewko 2016, s. 17).

Typy i formy (funkcje) wsparcia

W literaturze problemu znajdujemy podział wsparcia uwzględniający konkretne kryteria:

- Emocjonalne – wyraża troskę, zainteresowanie, daje przestrzeń do autorefleksji jednostki. Zawiera komunikaty podtrzymujące, uspakajające, których celem jest zmniejszenie stresu, opieka, przywrócenie dobrostanu psychicznego. Ten rodzaj wsparcia stwarza poczucie przynależności do wspólnoty, grupy. Wsparcie emocjonalne korzystnie oddziałuje na samoocenę i samopoczucie jednostki (Hetherington 2004, s. 28; Kondracka-Szala 2015, s. 18).
- Informacyjne (poznawcze) – jego celem jest nabycie umiejętności, pozyskanie informacji, rady – wymiana doświadczeń z osobami, które doświadczyły podobnych sytuacji, celem jest zrozumienie własnej sytuacji, problemu.
- Instrumentalne – obejmuje dobra materialne, rozwiązywanie problemów, konkretne sposoby i metody działania.
- Rzeczowe (materialne) – oznacza pomoc materialną, finansową, rzeczową.
- Oceniające (duchowe) – oznacza akceptację, zrozumienie, bazuje na wierze i transcendencji.

S. Kawula (1996, s. 60-64) wymienia wsparcie informacyjne, emocjonalne, wartościujące, instrumentalne. Już sama informacja w udzielanym wsparciu może być instrumentalna i jednocześnie zawierać ładunek emocjonalny (pozytywny, obojętny, negatywny). Źródłami wsparcia może być rodzina, grupa rówieśnicza, szkoła,

organizacje, Kościół. Skuteczność udzielanego wsparcia warunkowana jest przez trzy grupy czynników (Bartosz 1992, za: Kondracka-Szala 2015, s. 21-22):

- Sytuacyjne – ograniczony dostęp i możliwości korzystania ze wsparcia. Ta grupa czynników jest wynikiem konkretnych sytuacji, w których osoba niepełnosprawna nie ma możliwości skorzystania z pomocy (mogą to być ograniczenia w poruszaniu, mobilności, brak środków finansowych, czynniki chorobowe, charakter niepełnosprawności).
- Osobowościowe – predyspozycje osobowościowe osób wspieranych, mogą stanowić przeszkodę w udzielaniu wsparcia (odmawianie przyjęcia pomocy, brak gotowości do współpracy i wysiłku, samoizolacja, wycofanie, zaburzenia na poziomie osobowości).
- Czynniki relacji: osoba – problem (czynniki ograniczające) – mamy tu do czynienia z negatywnym sprzężeniem zwrotnym, problem przerasta możliwości osoby, jest poważny, wymaga wieloetapowych rozwiązań i nierzadko zaangażowania wielu osób, instytucji.

W badaniach zwraca się także uwagę na czynniki, które mogą wpływać na skuteczność wsparcia. Należą do nich: faza trudności, która często może wynikać ze specyfiki problemu osoby niepełnosprawnej, dopasowania do potrzeb, kontakt, współdziałanie, zrozumienie.

Kryzys - stres - terapia. Pojęcie „terapii”

Pojęcie „kryzysu” w literaturze problemu jest szerokie i w zasadzie samo pojęcie dynamicznie się poszerza o sytuacje i zjawiska, które mogą stanowić zagrożenie dla jednostki: katastrofy ekologiczne, zmiany klimatyczne, ataki terrorystyczne, wypadki, konflikty i wojny. Kryzys jest opisywany jako stan, w którym człowiek traci równowagę emocjonalną pod wpływem zdarzenia (czynnika) szkodliwego. Terminy związane z kryzysem to: „dezorientacja jednostki”, „utrata równowagi”, „załamanie”, a pojawiające się reakcje emocjonalne to: apatia, przygnębienie, poczucie winy, nieadekwatna, zaniżona samoocena, lęk i frustracja (Okun 2002, s. 254). Kryzys ma ramy czasowe, natomiast stres może być trwały i pozostawiać w psychice jednostki daleko idące skutki.

Kryzys w życiu osoby niepełnosprawnej może wiązać się z chorobami somatycznymi lub psychicznymi, deficytami czy zaburzeniami, które wywołują i utrzymują lęk. Ten typ sytuacji zawiera elementy trudne i stresogenne (Kawula 1996, s. 6). Niepełnosprawność jednostki mieści się w takiej interpretacji, ponieważ udzielane wsparcie ma charakter normalizacyjny i często decyduje nie tylko o pełnionych rolach, ale także rozwiązuje szereg życiowych problemów. W tym sensie może mieć charakter zarówno jednostkowy, jak i systemowy (Kwaśniewska, Wojnarowska 2004, s. 76). Cytowani autorzy, opierając się na teorii Caplana, wymieniają cztery fazy kryzysu (Okun 2002, s. 258):

- Faza 1 – określana jako wstępna, której towarzyszy odczuwanie napięcia i próba utrzymania równowagi poprzez znane jednostce sposoby. Sposoby te są często wynikiem wcześniejszych doświadczeń, zostały zapamiętane przez jednostkę jako całkowicie lub częściowo skuteczne, ponieważ sprawdzały się na

wcześniejszych etapach. Stosując je, osoba mogła pozbyć się napięcia i potrafiła sama wrócić do równowagi.

- Faza 2 – wzrost napięcia, stosowanie znanych strategii nie rozwiązuje problemów jednostki. Mamy tu do czynienia ze stosowaniem strategii polegającej na wdrażaniu działania opartego na planie, w którym jednostka wykorzystuje zasoby.
- Faza 3 – silne napięcie, które wymaga wykorzystania dodatkowych zasobów, nowych, nieznanymi lub niestosowanych dotąd strategii rozwiązywania problemów. Jednostka jest zdeterminowana i podejmuje ryzyko.
- Faza 4 – nierozwiązanie problemu może prowadzić do dezintegracji (zaburzeń) osobowości i kryzysu emocjonalnego.

W zależności od teorii skupionych na pomaganiu w kryzysie działania koncentrują się na: korygowaniu sposobu myślenia jednostki (teorie poznawcze), rozwiązywaniu problemów (teorie poznawczo-behawioralne), znaczących relacjach jednostki uwzględniających czynniki i źródła pomocy (teorie ekologiczne), uwarunkowaniu kulturowym potrzeb w kryzysie (teorie wielokulturowe) (Okun 2002, s. 259). W praktyce możemy wyróżnić formę terapii krótkoterminowej, skoncentrowanej na problemie, oraz długoterminowej, polegającej na uzyskaniu trwałej zmiany w zachowaniu, myśleniu, relacjach, uczuciach, wartościach osobowości jednostki, sytuacji życiowej, potrzebach, środowisku. B.F. Okun (2002, s. 158) sugeruje, że powodem tak wielu podejść w pomocy psychologicznej jest zróżnicowanie ludzi i ich problemów, co wydaje się uzasadniać podejścia integrujące tradycyjne teorie i nowe podejścia w terapii osób niepełnosprawnych. Terapia osób, które mają specjalne potrzeby, wymaga działań kompleksowych, w których uwzględnia się wszystkie sfery życia, w tym różne formy adaptacji społecznej i aktywności życiowej: samoobsługa, komunikowanie się, funkcje poznawcze, usprawnianie motoryczne, zachowania społeczne (Puszczałowska-Lizis, Biała 2013, s. 12-20). Biorąc pod uwagę psychologiczną podstawę działań wspierających, zwracamy uwagę na zdolność współodczuwania stanów i sytuacji innych ludzi, rozumienia motywów ich postępowania, podejmowanych decyzji i postaw (Wlazło 2009, s. 331). Można również przyjąć, że celem oddziaływań terapeutycznych jest dążenie do integracji stanów poznawczo-emocjonalnych i dążeń jednostki z jej stanem fizycznym i procesami energetycznymi, czyli stopień zintegrowania, zgrania psychiki z ciałem. Dobrostan psychiczny lub psychologiczne funkcjonowanie osiągnane w drodze integracji wyznaczają: rozwój osobisty, autonomia, kompetencje, pozytywne nastawienie do siebie, pozytywne stosunki interpersonalne (Dołęga 2010, s. 45-46).

W procesie adaptacji społecznej osoby niepełnosprawne napotykać na różne przejawy stygmatyzacji w interakcjach ze zdrowymi. Jej stopień i konsekwencje są zróżnicowane w zależności od rodzaju niepełnosprawności (Kondracka-Szala 2015, s. 76). Można zatem stwierdzić, że jakość życia jednostki niepełnosprawnej jest nie tylko wypadkową obszarów jej funkcjonowania uwzględniających zdolności intelektualne, zachowania przystosowawcze, interakcje, role społeczne, zdrowie czy kontekst, ale zależne jest od jakości udzielonego jej możliwego, ale i potrzebnego wsparcia. W ujęciu ekologicznym kluczowe stają się pojęcia: „jednostka”, „środowisko”, „wsparcie”, „interakcja” (Zawiślak 2011, s. 21-23). Rozważania i koncepcje psychologiczne skupiają się na kontekście indywidualnym i społecznym oraz

postawach społeczeństwa wobec osób niepełnosprawnych. Te elementy mogą potencjalnie wpływać na kształtowanie się wewnętrznych standardów oceniających jakość życia jednostki. Powołując się na koncepcje R. Schalocka, możemy założyć, że o wysokiej jakości życia jednostki niepełnosprawnej decyduje gwarancja otrzymania wsparcia, pomocy, zabezpieczenia (Schalock 2000, za: Zawislak 2011, s. 55-56). Tym samym pewność możemy uznać za element stabilizujący poczucie bezpieczeństwa w wymiarze jednostkowym. Do podstawowych obszarów wsparcia, ale i aktywności jednostki możemy zaliczyć: zdrowie i bezpieczeństwo, zatrudnienie, ochrona osobista i ochrona praw, kontakty społeczne, zachowanie (Smith 2008, s. 229).

Poczucie bezpieczeństwa jednostki

W literaturze problemu rozważa się problem bezpieczeństwa w ujęciu podmiotowym (bezpieczeństwo miękkie), które dotyczy człowieka, oraz przedmiotowym, czyli militarnym (bezpieczeństwo twarde) (Żukrowska 2006, s. 19-20; Leszczyński i in. (red.) 2016, s. 11). Bezpieczeństwo jest opisywane jako:

- Stan – odczuwanie i ocena stanu bezpieczeństwa ma charakter subiektywny i obiektywny i jest zależne od indywidualnych doświadczeń, wiedzy, postrzegania i oceny zagrożeń.
- Proces, standard – organizacja bezpieczeństwa i jego stan podlega zmianom zależnie od uwarunkowań. Jednostki, grupy, społeczności i państwa współtworzą stan bezpieczeństwa.
- Pierwotna wartość – gwarantuje jednostce przetrwanie i swobodny autonomiczny rozwój.
- Potrzeba każdej jednostki – rozumiana jest jako bezpieczeństwo rozwoju.

W ujęciu podmiotowym koncentrujemy się zatem na indywidualnych doświadczeniach i możliwościach osoby dotkniętej niepełnosprawnością. W praktyce ocena indywidualnego poczucia bezpieczeństwa oraz rozpoznanie czynników zapewniających jednostce równowagę i stabilizację w własnej sytuacji życiowej wpłynie nie tylko na proces analizy i rozumienia sytuacji, ale także na dobór sposobu oraz mechanizmu radzenia sobie z utrzymaniem i powrotem do stanu równowagi. Problem podmiotowości jednostki podnosi w swoich rozważaniach A. Bałandynowicz (2016, s. 14-15) i wymienia przesłanki świadczące o podejściu podmiotowym do jednostki niepełnosprawnej: podejmowanie działań budujących wspólne uzgodnione i negocjowane cele, osoba jako cel sama w sobie, nie sprowadzamy jednostki do roli społecznej i pełnionej funkcji, jednostka nie może podlegać manipulacji, przymusowi, tresurze. Wyznacznikami autonomii osobistej są: osoba jako wartość bezwzględna; rezygnacja z relatywizmu wobec ocen podmiotu, zamiast tego pokazanie, co akceptujemy, a czego nie; jednostka nigdy nie jest wypadkową swoich czynów, oceniamy ją poprzez pryzmat osoby (Bałandynowicz 2016, s. 17-18).

Zdaniem B. Hołysta (2014, s. 231) bezpieczeństwo jest ciągłym procesem społecznym, w obrębie którego podmioty (jednostki) stosują mechanizmy mające warunkować budowanie i utrzymanie poczucie bezpieczeństwa. Rozumienie bezpieczeństwa jako procesu pozwala dostrzec, że jest ono budowane, tworzone w określonej czasoprzestrzeni, dzięki czemu człowiek nie tylko pełni różne funkcje

społeczne, ale buduje własną tożsamość społeczną. Brak bezpieczeństwa prowadzi do destabilizacji funkcjonowania jednostki, wpływa na efektywność działania, która może przejawiać się w postaci niechęci, oporu, wycofania, a w skrajnych przypadkach samoizolacji.

Analizując w badaniach kwestie piętna, wymienia się obszar niebezpieczeństwa, czyli potencjalnego zagrożenia. Choroba i inność są postrzegane jako zagrożenie, budzą lęk, strach, rodzą dystans, a w konsekwencji odrzucenie osób niepełnosprawnych (Szczupał 2013, s. 21; Hołyst 2014, s. 300). Ten obszar uważa się za najistotniejszy w procesie stygmatyzacji (Hołyst 2014, s. 299). Izolacja jest najbardziej widocznym przejawem dyskryminacji i znajduje odzwierciedlenie w procesie instytucjonalizacji poprzez tworzenie placówek specjalnych. Zasadnicze znaczenie ma także problem marginalizacji, któremu towarzyszy stygmatyzacja, a raczej pewna tendencja do bagatelizowania problemów życiowych osób niepełnosprawnych. Zagrożeniem dla zrównoważonego rozwoju społecznego są realne mechanizmy, które mogą doprowadzić do wykluczenia jednostek, grup społecznych (Jaglarz 2018, s. 192).

Podsumowanie

1. Wsparcie psychologiczne udzielane osobom niepełnosprawnym wpływa na kształtowanie ich postawy i nastawień wobec własnej niepełnosprawności. Pozwala w perspektywie na rozwój samoakceptacji i samorealizację poprzez zrozumienie i dystans do własnej sytuacji życiowej. Jest czynnikiem stabilizującym sytuację życiową jednostki. Ten rodzaj wsparcia wymaga jednak specjalistycznych umiejętności ze strony osoby podejmującej się organizacji i udzielania takiej pomocy.
2. Nieumiejętnie prowadzone wsparcie psychologiczne może pogłębiać frustracje wynikające z niepełnosprawności, być przyczyną utrzymania samoograniczeń w sferze świadomości zarówno osób sprawnych, jak i niepełnosprawnych.
3. Prowadzenie terapii pozwala osobom niepełnosprawnym podtrzymać jakość życia poprzez wypracowanie mechanizmów radzenia sobie z kryzysami wynikającymi z przyczyn niepełnosprawności, przejawów choroby, niekorzystnych rokowań. Nie bez znaczenia jest umiejętność radzenia sobie ze stresem i jego przejawami. Dostępność i organizowanie terapii indywidualnej dla osób z różnymi rodzajami deficytów ma ogromne znaczenie dla rozwijania podejścia podmiotowego w stosunku do osób niepełnosprawnych oraz utrzymania indywidualnej równowagi biopsychicznej jednostki. Ta z kolei warunkuje budowanie i utrzymanie poczucia bezpieczeństwa w życiu każdej osoby. Zrozumienie siebie i akceptacja wymiaru swojego człowieczeństwa wydają się kluczowe w osiągnięciu każdej zmiany.
4. Samoakceptacja i adekwatna samoocena są czynnikami ułatwiającymi poradzenie sobie z trudnościami, przeciążeniami psychicznymi, wezwaniami i nowymi sytuacjami wynikającymi z niepełnosprawności. Pozwalają na podjęcie ról i – co istotne – gotowość do ponoszenia odpowiedzialności (konfrontacji z rzeczywistością), podtrzymują aktywność jednostki i jej zaangażowanie w proces usprawniania.

5. Proces adaptacji społecznej jest warunkiem utrzymania jakości życia osoby niepełnosprawnej na każdym etapie, również wtedy, kiedy człowiek mimo wysiłków traci wcześniej wypracowane sprawności.
6. Terapia i wsparcie psychologiczne to kluczowe aktywności przeciwdziałające wykluczeniu, marginalizacji i dyskryminacji osób niepełnosprawnych w wymiarze społecznym poprzez wsparcie własnego rozwoju.
7. Każda osoba niepełnosprawna odpowiednio wspierana jest w stanie utrzymać względną równowagę i zadbać o swoje bezpieczeństwo.

Literatura

1. Bałandynowicz A. (2016), *Transracjonalizm koroną inkluzji i bezpieczeństwa dla osób z niepełnosprawnością*, [w:] Bębas S., Jagielska K., Koziół R., *Integracja społeczna i bezpieczeństwo osób niepełnosprawnych*, s. 7-20, Biblioteka Instytutu Pracy Socjalnej, Kraków.
2. Ćwirynkało K., Żywanowska A. (2004), *Wieloaspektowość wsparcia społecznego rodzin wychowujących dziecko niepełnosprawne*, [w:] Kwaśniewska G., Wojnarowska A. (red.), *Aktualne problemy wsparcia społecznego osób niepełnosprawnych*, s. 75-82, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin.
3. Dołęga Z. (2010), *Psychologiczne podstawy i społeczny aspekt wychowania integrującego*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków.
4. Hetherington A. (2004), *Wsparcie psychologiczne w służbach ratowniczych*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk.
5. Hołyst B. (2014), *Bezpieczeństwo jednostki*, Wydawnictwo Naukowe PWN, Warszawa.
6. Hołyst B. (2015), *Bezpieczeństwo społeczeństwa*, Wydawnictwo Naukowe PWN, Warszawa.
7. Jaglarz E. (2018), *Warunki środowiska pracowniczego sprzyjające integracji osób zagrożonych wykluczeniem społecznym*, [w:] Frydrychowicz S. (red.) *Wyzwania integracji społecznej w Polsce*, s. 193-219, Wydawnictwo Naukowe Ignatianum w Krakowie, Kraków.
8. Kawula S. (1996), *Studia z pedagogiki specjalnej*, Wydawnictwo Wyższej Szkoły Pedagogicznej, Olsztyn.
9. Kondracka-Szała M. (2015), *Wsparcie społeczne osób stygmatyzowanych*, Difin, Warszawa.
10. Kwaśniewska G., Wojnarowska A. (red.) (2004), *Aktualne problemy wsparcia społecznego osób niepełnosprawnych*, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin.
11. Leszczyński M. i in. (red.) (2013), *Bezpieczeństwo w wymiarze lokalnym. Wybrane obszary*, Difin, Warszawa.
12. Modrzewski J. (2010), *Wsparcie społeczne jako czynnik wzorujący współczesne scenariusze biograficzne*, [w:] Piorunek M. (red.), *Pomoc – wsparcie społeczne – poradnictwo. Od teorii do praktyki*, s. 15-49, Wydawnictwo Adam Marszałek, Toruń.
13. Okun B.F. (2002), *Skuteczna pomoc psychologiczna*, Instytut Psychologii Zdrowia, Warszawa.
14. Płonka-Syroka B., Szyszka M., Wójcik W. (2016), *Niepełnosprawność i choroba przewlekła w perspektywie terapeutycznej, zawodowej i społeczno-opiekuńczej*, Wyższa Szkoła Pedagogiczna im. Janusza Korczaka, Warszawa.
15. Puszczalowska-Lizis E., Biała A. (2013), *Terapia osób o specjalnych potrzebach*, Wydawnictwo Fraszka Edukacyjna, Warszawa.
16. Schalock R.L. (2000), *Three Decades of Quality of Life*, „Focus on Autism and Other Developmental Disabilities”, 15, 2, s. 116-127.
17. Smith D.D. (2008), *Pedagogika specjalna. Podręcznik akademicki*, t. 1, tłum. Hołówka T., Zakrzewska A.P., Wydawnictwo Akademii Pedagogiki Specjalnej, Wydawnictwo Naukowe PWN, Warszawa.
18. Szczupał B. (2013), *Piętno społeczne związane z niepełnosprawnością i chorobą przewlekłą*, [w:] Klinik A. (red.), *Racjonalność oraz uwarunkowania procesów terapeutycznych osób*

- niepełnosprawnych. Problemy edukacji, rehabilitacji i socjalizacji osób niepełnosprawnych*, t. 16, s. 15-26, Oficyna Wydawnicza Impuls, Kraków.
19. Walter N. (2016), *Internetowe wsparcie społeczne. Studium socjopedagogiczne*, Wydawnictwo Naukowe Uniwersytetu Adama Mickiewicza, Poznań.
 20. Wiliński M. (2010), *Modele niepełnosprawności: indywidualny – funkcjonalny – społeczny*, [w:] Brzezińska A., Kaczan R., Smoczyńska K. (red.), *Diagnoza potrzeb i modele pomocy dla osób z ograniczoną sprawnością*, Wydawnictwo Naukowe Scholar, Warszawa.
 21. Wlazło M. (2009), *O znaczeniu i kontekstach wsparcia w pedagogice osób z niepełnosprawnością intelektualną*, [w:] Baczała D., Bleszyński J.J., Zaorska M. (red.), *Osoba z niepełnosprawnością – opieka, terapia, wsparcie*, s. 329-338, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń.
 22. Zawisłak A. (2011), *Jakość życia osób dorosłych z niepełnosprawnością intelektualną*, Difin, Warszawa.
 23. Żukrowska K., Grącik M. (red.) (2006), *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, Oficyna Wydawnicza SGH, Warszawa.

THE ROLE OF PSYCHOLOGICAL SUPPORT AND THERAPY IN SOCIAL ADAPTATION OF PEOPLE WITH DISABILITIES

Abstract: This chapter evaluates the essence and significance of psychological support, including individual therapy, in shaping the social safety of people with disabilities who have a disability degree certificate. The need to organise such efforts institutionally is an important factor for reinforcing individual social adjustment and adaptation mechanisms of people with disabilities (especially during a pandemic). The objective of this chapter is to analyse the issue of support understood as available and highly specialised efforts adjusted to the needs and expectations of a person with disabilities, counteracting their functional disorders. These efforts aim at building and sustaining social relations, instilling individual independence and personal autonomy, and preventing social exclusion and isolation.

Keywords: disability, disorders, psychological support, therapy



Bezpieczeństwo w dobie COVID-19

Rozdział 4

ZAUFANIE SPOŁECZNE JAKO CZYNNIK WPŁYWAJĄCY NA SZCZEPIENIA PRZECIW COVID-19

Felicjan Byłok⁴

Streszczenie: W rozważaniach na temat podejmowanych działań na rzecz walki z pandemią COVID-19 istotne jest określenie czynników sprzyjających ograniczeniu jej rozprzestrzeniania się. Jednym z nich jest zaufanie społeczne, które wspomaga działania instytucji ochrony zdrowia na rzecz propagowania szczepień przeciw COVID-19. Przyjęcie założenia, że zaufanie do rządu, instytucji publicznych i do innych ludzi w istotny sposób determinuje decyzje ludzi o przyjęciu szczepionki, ułatwiło sformułowanie celu badań, którym było poszukiwanie odpowiedzi na pytania badawcze: W jakim zakresie zaufanie społeczne wspiera działania na rzecz ograniczania rozwoju pandemii? Czy i w jakim zakresie zaufanie społeczne wpływa na przyjmowanie szczepionek w układzie przestrzennym? Do badań zastosowano metodę dedukcyjną i Desk Research, za pomocą której przeprowadzono krytyczną analizę danych wtórnych i metody dedukcyjnej. W wyniku badań stwierdzono istotne związki między zaufaniem społecznym a poziomem zachorowań na COVID-19 i liczbą zaszczepionych mieszkańców w województwach w Polsce. Uzyskane wyniki badań mogą być przydatne w planowaniu działań propagujących szczepienia przeciw COVID-19.

Słowa kluczowe: zaufanie społeczne, COVID-19, szczepienia, bezpieczeństwo zdrowotne

Wprowadzenie

Chociaż obecna pandemia COVID-19 występuje w wymiarze niespotykanym w XXI wieku pod względem zasięgu geograficznego i wpływu na życie codzienne, to jej przebieg wydaje się podobny do poprzednich pandemii. Warto zatem prześledzić ich przebieg. Najbardziej dotkliwa była pandemia grypy A/H1N1, którą WHO ogłosiła w czerwcu 2009 roku. We wczesnej fazie tej grypy nie było dostępnej szczepionki i nie było pewności, czy zostanie wyprodukowana. Zalecenia dotyczące zdrowia publicznego obejmowały przede wszystkim częste mycie rąk, unikanie chorych, trzymanie się z dala od tłumu i praktykowanie właściwych zachowań higienicznych.

⁴ Politechnika Częstochowska, Wydział Zarządzania

Z doświadczeń płynących z zachowań ludzi podczas wcześniejszych pandemii wynika, że na przeszkodzie jej zapobieganiu stoją trzy grupy czynników (Bavel i in. 2020):

- 1) Ludzie nie doceniają ryzyka, na jakie się narażają.
- 2) Ludzie są przekonani, że zamykanie się w ścisłej izolacji w celu ochrony innych jest sprzeczne z naturą ludzką.
- 3) Ludzie często nieświadomie w swoich działaniach stanowią zagrożenie dla siebie i innych.

W przeciwdziałaniu pandemii główną rolę odgrywają władze państwowe i instytucje ochrony zdrowia, których zadaniem jest stwarzanie oraz gwarantowanie ochrony bez względu na wiek, płeć, miejsce zamieszkania, dochód i zamożność. Obecnie jednym z kluczowych zadań władz jest zapewnienie dostępności szczepionek przeciw COVID-19 i podejmowanie działań informacyjnych, mających na celu przekonanie obywateli do szczepienia się. Akceptacja szczepionek i zbudowanie przekonania, że są one najważniejszym środkiem chroniącym przed infekcją, jest niezbędna do przezwyciężenia pandemii. Pomocne w działaniach społecznych na rzecz propagowania szczepień może stać się promowanie zaufania społecznego, które oznacza, zgodnie z rozumieniem R. Putmana (2000), uogólnione zaufanie okazywane innym ludziom. Oparte jest ono na zasadzie wzajemności, w myśl której należy zrobić coś dla kogoś innego, nie oczekując natychmiastowej rekompensaty, ale mając nadzieję, że w przyszłości on lub ktoś inny odda przysługę. Z kolei L.S. Wrightsman (1996) ujmuje je jako cechę osobowości, która znajduje odzwierciedlenie w ogólnych oczekiwaniach co do intencji innych osób. Natomiast dla J.S. Colemana (1990) zaufanie jest relacją wzajemnych kalkulacji między jednostką pokładającą zaufanie a jednostką tym zaufaniem obdarzoną. W tym podejściu zakłada się, że osoby będą sobie ufać wtedy, gdy przyniesie to im obopólną korzyść. Koncepcje zaufania społecznego rozwinął P. Sztompka (2012), który uważa, że jest ono swego rodzaju zakładem podejmowanym na temat niepewnych przyszłych działań innych ludzi. Można powiedzieć, że „zaufanie [...] to prawidłowe przewidywanie działań innych ludzi, które mają wpływ na działania jednostki w sytuacji, gdy wybór działania musi zostać dokonany, zanim możliwe będzie zaobserwowanie działań innych osób” (Dasgupta 1988, s. 51). Z kolei T. Yamagishi (2002, s. 36) ujmuje zaufanie „jako oczekiwanie korzystnego zachowania ze strony kogoś w społecznie niepewnej sytuacji, oparte na wiedzy o jego skłonnościach (w tym uczuciach wobec partnera)”. Rozwinięte zaufanie społeczne staje się normą kulturową, tworząc kulturę zaufania. Występuje to w sytuacji, kiedy „uogólnione zaufanie przenika całą zbiorowość i traktowane jest jako obowiązująca reguła postępowania” (Sztompka 2002, s. 314). Wspólnym elementem wszystkich podejść są działania ukierunkowane na innych ludzi. Źródłem zaufania w działaniach ludzi może być zażyłość wynikająca z powtarzalności interakcji między stronami, kalkulacyjność skorelowana z szacowaniem przewagi korzyści nad kosztami związanymi z relacjami albo wartości odnoszące się do uczciwości i dobrej woli (Byłok 2020).

Celem rozdziału jest poszukiwanie związków między zaufaniem społecznym a rozprzestrzenianiem się pandemii i szczepieniami przeciw COVID-19. Autor szuka odpowiedzi na pytania: W jakim zakresie zaufanie społeczne wspiera

działania na rzecz ograniczania rozwoju pandemii? Czy i w jakim zakresie zaufanie społeczne wpływa na przyjmowanie szczepionek w układzie przestrzennym? Do badań zastosowano metodę dedukcyjną i Desk Research, za pomocą której przeprowadzono krytyczną analizę danych wtórnych i metody dedukcyjnej.

Zaufanie społeczne a bezpieczeństwo zdrowotne w okresie pandemii COVID-19

Kluczowym elementem wspomagającym przeciwdziałanie rozprzestrzenianiu się wirusa SARS-CoV-2 jest zaufanie, w szczególności do instytucji zdrowia publicznego. Podczas pandemii urzędnicy ochrony zdrowia często muszą przekonać ludzi, aby wprowadzili zmiany w swoim zachowaniu, np. powstrzymać się od kontaktów społecznych, przestrzegać kwarantanny lub dobrowolnie zgłosić się na badania medyczne. Ze względu na charakter i wielkość populacji objętej takimi działaniami pozytywne zachowania mogą być trudne do wyegzekwowania, w związku z tym potrzebne jest zaangażowanie liderów społeczności lokalnych, którzy mogą wzmocnić te komunikaty i pomóc zbudować zaufanie potrzebne do wywołania zmian behawioralnych. Badania przebiegu epidemii Eboli w Afryce Zachodniej w latach 2014-2015 sugerują, że pozyskanie lokalnych aktorów w celu budowania zaangażowania i zaufania do urzędników służby zdrowia może zwiększyć skuteczność działań w obszarze zdrowia publicznego. Na przykład wyspecjalizowane ośrodki leczenia Eboli, które zatrudniały łączników i mobilizatorów społecznych do podnoszenia świadomości i rozwiązywania nieporozumień oraz do akwizycji „od drzwi do drzwi”, były skutecznymi metodami zachęcania ludzi do przestrzegania zasad zarządzania kryzysowego, takich jak zakaz zgromadzeń, utrzymywanie dystansu społecznego, częste mycie rąk itd. (Bavel i in. 2020).

Niezwykle ważne jest, aby przekazywanie informacji o ryzyku związanym z zachorowaniem przekonało społeczeństwo do przestrzegania zaleceń służb medycznych na wczesnych etapach kryzysu, w celu ograniczenia rozprzestrzeniania się wirusa. Społeczeństwo musi najpierw zaufać ekspertom i przedstawicielom ochrony zdrowia, zanim zacznie wypełniać ich zalecenia. Liczne badania poświęcone pandemii grypy A/H1N1 z 2009 roku wskazują na dużą rolę zaufania jako predyktora zachowań społecznych. V.S. Freimuth i in. (2014) skoncentrowali się na ustaleniu związku między zaufaniem a rozwojem tej pandemii. Badacze odkryli, że przedstawiciele rządu i instytucje medyczne są obdarzeni zaufaniem wtedy, gdy opinia publiczna uzna, że są kompetentnymi ekspertami w obszarze zdrowia i cechuje ich otwartość, szczerłość i opiekuńczość.

Wpływ na zaufanie ma jakość komunikacji między przedstawicielami rządu a obywatelami. Ludzie, którzy mieli wyższy poziom wiedzy na temat wirusa i uważniej śledzili wiadomości o tej pandemii, mieli większe zaufanie do działań rządu. Ustalenia te wskazują, że wzrost wiedzy na temat kryzysu powinien mieć pozytywny wpływ na zaufanie do rządu. Kluczem w tej komunikacji jest zwrócenie uwagi na tych, którzy nie są zainteresowani lub unikają informacji na temat pandemii. Jednym z wniosków, jaki wynika z badań, jest ustalenie, że uczciwość i spójność informacji płynących z instytucji rządowych są niezbędne do budowania zaufania, co następnie

wpływa na przestrzeganie zalecanych procedur reagowania na pandemię (Freimuth i in. 2014).

Zakłócenie tej komunikacji sprzyja pojawianiu się fałszywych, nieprawdziwych i błędnych informacji na temat COVID-19 (fake newsów) w mediach społecznościowych, co podważa zaufanie do rządów i instytucji medycznych. Pojawiają się informacje o nowych, magicznych lekach, terapiach leczenia, o teoriach spiskowych. Pomimo wysiłków właścicieli mediów społecznościowych, aby powstrzymać tę falę dezinformacji, na całym świecie rozprzestrzeniają się fałszywe informacje o koronawirusie (Frenkel, Alba, Zhong 2020). Aby przeciwdziałać temu zjawisku, badacze wskazują na konieczność zrozumienia istoty fake newsów i ich konstrukcji. Sugerują, że źródła publicznej dezinformacji i polaryzacji są bardziej prawdopodobne w treści zwykłych wiadomości lub w ich unikaniu, ponieważ są jawnie fałszywe (Allen i in. 2020). Jednym ze sposobów przeciwdziałania jest demaskowanie fałszywych informacji za pomocą podawania prawdziwych faktów. Niezbędna do walki z dezinformacją jest wiedza fachowa, pochodząca ze źródła cechującego się bezstronnością, i ujawnianie zaprzeczeń, które opierają się na wyjaśnieniach przyczynowych. B. Swire-Thomson i U.H.B. Ecker (2018), bazując na wynikach badań, przedstawili sześć rekomendacji służących przeciwdziałaniu dezinformacji. Po pierwsze, najbardziej skuteczną metodą korygowania błędnych informacji jest podanie alternatywnej faktycznej przyczyny lub wyjaśnienia, aby ułatwić „wyłączenie” niedokładnych informacji w modelu sytuacji początkowej danej osoby. Po drugie, warto ostrzegać odbiorców przed błędnymi informacjami, co wpłynie na uznanie dezinformacji za szkodliwą. Po trzecie, sposobem walki z nieprawdziwymi informacjami mogą być subtelne podpowiedzi, które skłaniają ludzi do refleksji nad prawdziwością informacji. Platformy społecznościowe mogą zachęcać użytkowników do myślenia o prawdziwości informacji, na przykład okresowo prosząc użytkowników o ocenę prawdziwości losowo wybranych postów. Po czwarte, można pobudzać aktywność w poszukiwaniu niedokładnej wiedzy i nowo zakodowanych informacji faktycznych, która zwiększa prawdopodobieństwo, że poszczególne osoby zauważą rozbieżności między pierwotnie uznanymi błędnymi przekonaniem a dowodami faktycznymi oraz że odpowiednio zaktualizują swoją wiedzę. Po piąte, skuteczną metodą jest odrzucenie błędnych informacji, które obejmuje nie tylko stwierdzenie, że błędne przekonanie jest fałszywe, ale podanie wyczerpującego wyjaśnienia, dlaczego jest ono nieprawidłowe. Poprawki są najbardziej skuteczne, jeśli zawierają wystarczające wyjaśnienie, dlaczego błędne przekonanie jest fałszywe (i dlaczego podane fakty są prawdziwe). Po szóste, metodą zwalczającą fałszywe informacje jest budowanie wiarygodności, która skutecznie koryguje nieprawdziwe wiadomości. Polega ona bardziej na postrzeganej uczciwości i rzetelności źródła niż na jego wiedzy specjalistycznej. Oznacza to, że media społecznościowe mogą być skutecznym narzędziem wpływania na innych, a posty na Facebooku lub Twitterze mogą mieć większy wpływ na opinie znajomych niż porady ekspertów. Ostatnią metodą jest budowanie postaw sceptycznych wśród odbieranych informacji. Sceptycyzm to świadomość potencjalnych ukrytych sensów i chęć dokładnego zrozumienia dostępnych dowodów. Może ograniczyć skutki dezinformacji, ponieważ wykorzystuje większą ilość zasobów poznawczych do oceny prawdziwości dezinformacji.

Z analizy badań nad przebiegiem pandemii wynika, że zaufanie jest kluczowym czynnikiem sprzyjającym walce z wirusem. L.S. Meredith i in. (2007), opierając się na doświadczeniach wynikających z badań nad przebiegiem pandemii w grupie Afroamerykanów, opracowali konkretne zalecenia dotyczące budowania zaufania w obszarze zdrowia:

- Należy wykorzystywać źródła „wiarygodne” w materiałach pisemnych i ustnych komunikacji, np. takimi źródłami mogą być niezależni specjaliści medyczni (lekarze, urzędnicy Ministerstwa Zdrowia), krajowe media i obywatele z tej społeczności.
- Trzeba podawać pełne i dokładne informacje dotyczące pandemii.
- Warto wzmacniać przekazy informacji o chorobie dowodami wskazującymi na niebezpieczeństwo wynikające z zakażenia się i komplikacje zdrowotne z nim związane.
- Ważne jest, aby we wczesnym etapie zaangażować opinię publiczną jako partnera w procesie komunikacji ze społeczeństwem.

Konkludując, należy podkreślić, że w celu zmniejszenia lęku ludzi przed COVID-19, a także ograniczenia wiary w fałszywe informacje o niej, rządy, instytucje medyczne, urzędnicy ds. zdrowia i platformy społecznościowe powinny prowadzić kampanie informujące o skuteczności metod leczenia tej choroby, w tym przede wszystkim o skuteczności szczepionek.

Zaufanie a postawy wobec szczepienia przeciw grypie

Jedną ze skutecznych metod przeciwdziałania rozprzestrzenianiu się pandemii jest stosowanie szczepionek. Podczas pandemii grypy A/H1N1 w latach 2009-2010 jej dalsze rozprzestrzenianie się powstrzymały masowe szczepienia przeciw tej chorobie. Badania nad związkami między zaufaniem a szczepieniem przeciw grypie wskazały na istotne powiązania między nimi. Zaufanie społeczne może stać się czynnikiem sprzyjającym podejmowaniu decyzji o zaszczepieniu się. Dotyczy to w szczególności instytucjonalnego i publicznego zaufania. B. Rönnerstrand (2013) ustalił występowanie związku między zaufaniem a gotowością do zaszczepienia się przeciwko chorobom zakaźnym. Zaufanie do opieki zdrowotnej jest powiązane z zamiarem szczepienia, ponieważ czyni ludzi bardziej podatnymi na zalecenia opieki zdrowotnej. Może także zwiększyć liczbę ludzi skłonnych wierzyć, że mogą wpływać na swoje zdrowie za pomocą środków ochronnych. Inną przesłanką związaną z zaufaniem społecznym jest poczucie moralnej odpowiedzialności wobec innych ludzi, w której dbałość o indywidualne uodpornienie jest sposobem ich ochrony. Istotne jest zaufanie do źródła informacji zdrowotnych, które osoby pozyskują ze swoich sieci interpersonalnych, mediów lub rządów. Osoby podejmują decyzje o zaszczepieniu się pod wpływem informacji zdrowotnych wtedy, gdy ufają konkretnemu źródłu informacji.

Istotnym czynnikiem sprzyjającym poddaniu się szczepieniom jest zaufanie instytucjonalne do rządu. W. van der Weerd i in. (2011), śledząc wpływ zaufania do rządu na zachowania ludzi podczas pandemii grypy A/H1N1 w Holandii w 2009 roku, ustalili kilka ważnych kwestii. W pierwszym okresie rozwoju pandemii

zaufanie do rządu było wysokie, ale z czasem zmniejszało się. W trakcie pandemii wzrosła wrażliwość na sprawy związane z chorobą i chęć stosowania środków ochronnych, przy czym zaufanie i wrażliwość były związane z intencją stosowania środków ochronnych tylko w pierwszym okresie. Wyższe poziomy zamiaru szczepienia się były związane ze zwiększonym zaufaniem do rządu, obawą przed zachorowaniem i postrzeganą podatnością na zagrożenia. W drugim i trzecim okresie trwania pandemii wzrosło poszukiwanie informacji o chorobie. Większość respondentów chciała otrzymywać informacje na temat zapobiegania infekcjom od miejskich służb zdrowia, podmiotów świadczących opiekę zdrowotną i mediów. Natomiast zaufanie do rządu spadło.

Podobne wyniki uzyskano w badaniu wpływu zaufania do działań rządu i administracji państwowej na stosunek do szczepień przeciwko wirusowi i poziom ich przyjmowania w USA. Z badań wynika, że ogólna populacja USA wyraziła względnie duże zamiary otrzymania szczepionki przeciwko grypie A/H1N1 w pierwszym okresie pandemii, faktyczne szacunki zasięgu szczepionki były znacznie niższe. We wrześniu 2009 roku 50% dorosłych miało otrzymać szczepionkę, ale do końca stycznia 2010 roku tylko 24% populacji USA zgłosiło chęć otrzymania szczepionki. Od końca stycznia do końca czerwca 2010 roku tylko 3% zostało zaszczepionych, w sumie 27% dorosłych zostało zaszczepionych w całym kraju (Quinn i in. 2013). Jedną z przyczyn tego stanu rzeczy było niskie zaufanie do rządu. Inną przyczyną był duży odstęp czasu między pierwszymi informacjami o szczepionce ze źródeł rządowych a dostępnością szczepionki, co utrudniło utrzymanie zaangażowania i intencji behawioralnych wobec szczepienia.

Na decyzję o przyjęciu szczepionki wpływ mają również inne czynniki. Badania M. Junga, L. Lin i K. Viswanatha (2013) wykazały, że na zamiar wzięcia szczepionki przeciw grypie A/H1N1 wywarły takie czynniki jak zmartwienie, wrażliwość lub spisek, przy czym zmartwienie i wrażliwość mają również wpływ na postrzeganą skuteczność zaleceń zdrowotnych. Na wzrost zaufania do szczepionki wywierają wpływ również „wiarygodne źródła”, którymi są m.in. znane osoby. S.C. Quinn i in. (2013) przeanalizowali reakcję na ujawnienie przez prezydenta Obamę szczepień jego córek w USA. Badacze ustalili, że ujawnienie tej informacji miało ogromny wpływ na decyzje dotyczące szczepień, niezależnie od przynależności do partii, nawet jeśli poziom zaufania do działań rządu, a zwłaszcza do prezydenta, był różny. Zatem osoby stanowiące wzór do naśladowania mogą być wykorzystane w strategii komunikacji ze społeczeństwem w sytuacji, kiedy cechuje ich odpowiedzialność powiernicza i uczciwość jako kluczowe elementy zaufania do skuteczności szczepień.

Zaufanie społeczne a szczepienia przeciw COVID-19 w Polsce

Badanie relacji między zaufaniem społecznym a zachorowaniami na COVID-19 przeprowadzono na podstawie danych dotyczących liczby zachorowań na 10 tys. mieszkańców województw i wskaźnik zaufania społecznego zbudowany z deklaracji osób zdecydowanie lub raczej mających zaufanie do policji, władz lokalnych miasta/gminy i – ogólnie rzecz biorąc – ludzi. Badania związku między zaufaniem społecznym a przyjmowaniem szczepionki przeprowadzono na podstawie danych

z 14 sierpnia 2021 roku i wskaźnika zaufania społecznego z raportu badań Głównego Urzędu Statystycznego (2020). Jednostkami analizy uczyniono regiony w obszarze województw. Z analizy danych zawartych w tabeli 4.1 wynika, że poziom zaufania społecznego w Polsce jest na średnim poziomie (71,3), przy czym występują regionalne różnice w jego występowaniu. Najwyższy ma miejsce w województwie zachodniopomorskim, w dalszej kolejności w województwach lubuskim i świętokrzyskim.

Tabela 4.1. Wskaźniki zaufania społecznego i wskaźniki zachorowań w Polsce w okresie od 25 marca 2020 r. do 14 września 2021 r.

Województwo	WZS	SWZ 24.07.2020	SWZ 20.10.2020	SWZ 21.01.2021	SWZ 14.09.2021
dolnośląskie	66,1	10,24	35,8	333,3	740,6
kujawsko- pomorskie	64,8	3,35	42,7	483,0	880,5
lubelskie	72,8	3,67	36,1	345,4	611,2
lubuskie	70,2	0,88	28,8	168,5	737,5
łódzkie	64,8	36,05	58,3	385,8	742,4
małopolskie	71,3	5,9	104,7	337,3	657,5
mazowieckie	68,2	9,9	49,0	327,8	734,8
opolskie	70,9	10,2	56,3	405,6	717,9
podkarpackie	76,2	3,99	50,7	303,1	600,9
podlaskie	68,6	7,62	40,2	329,2	601,8
pomorskie	69,7	3,01	50,0	414,7	823,3
śląskie	65,6	30,43	69,9	372,0	809,5
świętokrzyskie	72,1	6,92	46,4	305,2	599,0
warmińsko- mazurskie	66,9	1,98	28,7	449,0	863,7
wielkopolskie	73,1	8,96	48,2	423,9	819,6
zachodnio- pomorskie	68,6	3,74	29,3	443,7	770,4

Legenda: WZS – wskaźnik zaufania społecznego, SWZ – skumulowany wskaźnik zachorowań na 10 tys. mieszkańców województwa

Źródło: opracowanie własne na podstawie (Serwis Rzeczypospolitej... 2020; *Koronawirus w Polsce...* 2021)

Niektórzy badacze uważają, iż wysoki poziom zaufania społecznego jest czynnikiem ograniczającym rozprzestrzenianie się pandemii COVID-19 (Jalan, Sen 2020). Również w analizie związków między zaufaniem społecznym a poziomem zachorowania w Polsce odkryto częściowe zależności potwierdzające te ustalenia badawcze (tab. 4.1). Czynnikiem różnicującym te zależności był etap w rozwoju pandemii. W początkowych etapach jej rozwoju ta zależność była silna. W pierwszym pomiarze, tj. 24 lipca 2020 roku (koniec pierwszej fali zachorowań), niski poziom

zachorowań na COVID-19 wystąpił w województwach o najwyższym poziomie zaufania, tj. w województwach lubuskim, warmińsko-mazurskim, lubelskim, świętokrzyskim i podkarpackim. W kolejnym etapie badania, tj. 20 października 2020 roku (początek drugiej fali zachorowań), wysoki poziom zaufania wpływał na niski poziom zachorowań w przypadku województw: lubuskiego, lubelskiego, świętokrzyskiego i wielkopolskiego. Podczas badań w fazie największego rozwoju trzeciej fali zachorowań (21 stycznia 2021 r.) związek między silnym zaufaniem społecznym a infekcjami na COVID-19 wystąpił w przypadku województw: lubuskiego, lubuskiego, małopolskiego, świętokrzyskiego i podkarpackiego. W ostatnim badaniu przeprowadzonym 14 września 2021 roku (początek czwartej fali zachorowań) zaobserwowano, iż wysoki poziom zaufania miał wpływ na niski poziom infekcji w województwach: lubuskim, małopolskim, podkarpackim i świętokrzyskim. Reasumując, należy stwierdzić, że jedynie stały silny wpływ na niski poziom zachorowań miało wysokie zaufanie społeczne w województwach lubelskim, podkarpackim i świętokrzyskim. W pozostałych województwach związek między wysokim zaufaniem społecznym a niskim poziomem zachorowań wystąpił w ograniczonym zakresie.

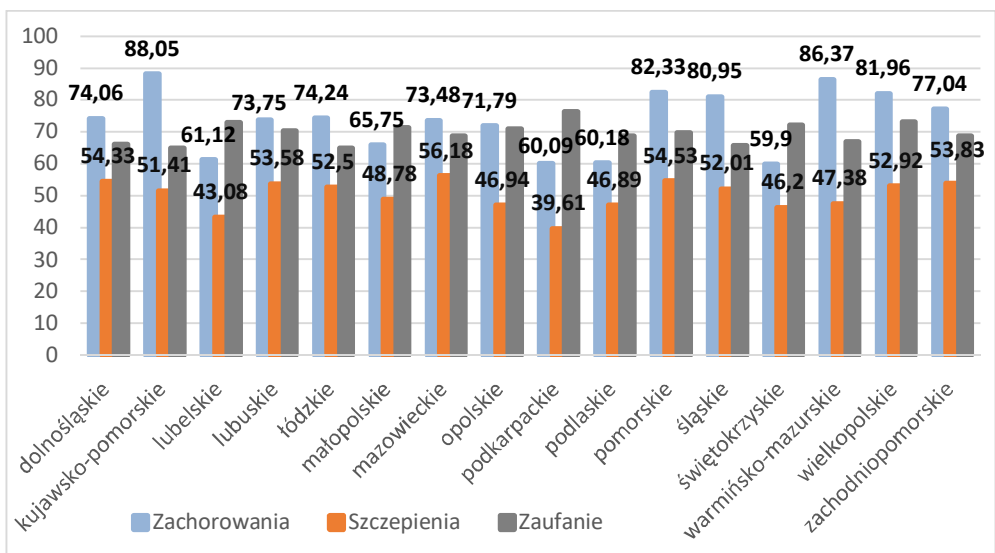
Najskuteczniejszą metodą przeciwdziałania pandemii COVID-19 są szczepienia. W Polsce dopuszczone są do użytku cztery szczepionki, które obejmują szczepionki z fragmentem materiału genetycznego (mRNA), szczepionki z wektorami wirusowymi, szczepionki z inaktywowanym wirusem, żywe szczepionki atenuowane oraz szczepionki z podjednostkami białkowymi lub peptydowymi. Dwie szczepionki wykorzystują platformę mRNA, tj. szczepionka Comirnaty (Pfizer – BioNTech) i szczepionka Spikevax (Moderna BIOTECH Spain, S.L.), oraz dwie wykorzystujące wektor adenowirusowy – szczepionka Vaxzevria (AstraZeneca) i szczepionka COVID-19 Vaccine Janssen (Augustynowicz, Jackowska 2021). Szczepionki cechuje wysoka efektywność wynosząca 80-90% w ochronie przed objawami COVID-19 oraz wysoka efektywność w ochronie przed zakażeniami bezobjawowymi. Z analizy tabeli 4.2 wynika, że występują regionalne różnicowania przyjmowania wymienionych wyżej szczepionek. Najwięcej mieszkańców przyjęło podwójną dawkę szczepionek Pfizer – BioNTech, Moderna BIOTECH i AstraZeneca oraz pojedynczą Vaccine Janssen w województwach dolnośląskim, lubuskim, mazowieckim, pomorskim i zachodniopomorskim, w których więcej niż połowa mieszkańców w pełni się zaszczepiła. Natomiast najmniej osób przyjęło szczepionki w województwach podkarpackim, lubelskim, świętokrzyskim i opolskim.

Jednym z celów badawczych było zbadanie wpływu zaufania społecznego na liczbę zaszczepionych mieszkańców poszczególnych województw. Z analizy tabeli 4.2 wynika, że w województwach o najwyższym poziomie zaufania zaobserwowano stosunkowo niski poziom zaszczepienia. Dotyczy to województw: podkarpackiego, lubelskiego, opolskiego, świętokrzyskiego i małopolskiego, w których mniej niż połowa mieszkańców jest w pełni zaszczepiona. W pozostałych województwach o wysokim poziomie zaufania społecznego, tj. wielkopolskim i lubuskim, zaobserwowano wysoki poziom zaszczepienia mieszkańców. Zatem wyniki badań wskazują na niejednoznaczny związek między zaufaniem społecznym a liczbą zaszczepionych mieszkańców.

Tabela 4.2. Wskaźnik zaufania społecznego i wskaźnik szczepienia przeciw COVID-19 w województwach (w procentach)

Województwa	Wskaźnik zaufania społecznego	Wskaźnik szczepienia 2 dawką	Wskaźnik szczepienia 1 i 2 dawką
dolnośląskie	66,1	47,61	54,33
kujawsko-pomorskie	64,8	44,76	51,41
lubelskie	72,8	37,74	43,08
lubuskie	70,2	46,58	53,58
łódzkie	64,8	46,69	52,50
małopolskie	71,3	42,92	48,78
mazowieckie	68,2	49,72	56,18
opolskie	70,9	41,71	46,94
podkarpackie	76,2	34,78	39,61
podlaskie	68,6	42,01	46,89
pomorskie	69,7	48,36	54,53
śląskie	65,6	45,71	52,01
świętokrzyskie	72,1	40,28	46,20
warmińsko-mazurskie	66,9	41,53	47,38
wielkopolskie	73,1	47,47	52,92
zachodniopomorskie	68,6	46,70	53,83

Źródło: opracowanie własne na podstawie (GUS 2020; *Raport szczepień...*)



Rysunek 4.1. Wskaźniki zachorowań na COVID-19, szczepień na COVID-19 i zaufania społecznego w województwach w Polsce w 2021 roku

Legenda: Zachorowania – skumulowany wskaźnik zachorowań na 10 tys. mieszkańców województwa; Szczepienia – wskaźnik wyszczepienia populacji mieszkańców województw w procentach

Źródło: opracowanie własne

W Polsce obserwuje się znaczne zróżnicowanie liczby osób zaszczepionych. Występują regiony, w których mieszkańcy z rezerwą podchodzą do szczepienia i nie szczepią się w dużej liczbie. Dane przedstawione na rysunku 4.1 pozwalają obserwować związki między wielkością zachorowań a liczbą szczepień i poziomem zaufania. W województwach o relatywnie niskim poziomie zachorowań w stosunku do średniej w Polsce mieszkańcy rzadziej się szczepią. Dotyczy to województw: lubelskiego, małopolskiego, podlaskiego, podkarpackiego i świętokrzyskiego. Jednym z możliwych wyjaśnień tego związku jest hipoteza, iż w województwach, w których liczba zachorowań była mniejsza niż w pozostałych, mieszkańcy w mniejszym stopniu osobiście odczuli skutki pandemii, stąd nie odczuwają potrzeby szczepienia, które wiąże się z pewnym ryzykiem zdrowotnym.

Podsumowanie

Jednym z pytań badawczych była identyfikacja związków między zaufaniem społecznym a liczbą zachorowań w układzie przestrzennym. Wyniki badań przestrzennych związków między zaufaniem a wielkością zachorowań na COVID-19 w Polsce wskazują na jego wpływ na zakres rozprzestrzeniania się pandemii, przy czym znaczenie ma liczba infekcji. W celu wykrycia zależności między zaufaniem i liczbą zachorowań poddano analizie cztery okresy, tj. lipiec i październik 2020 roku oraz styczeń i wrzesień 2021 roku. Wybór okresów był związany z przebiegiem pandemii w Polsce. W lipcu miała miejsce pierwsza fala zachorowań, w październiku rozpoczęła się druga fala pandemii, w styczniu miał miejsce początek trzeciej fali, a we wrześniu rozpoczęła się czwarta fala. W badanych okresach zanotowano istotne zmiany w relacjach między zmiennymi. W okresie pierwszej i drugiej fali wykazano dodatni wpływ zaufania społecznego na liczbę infekcji, natomiast w trzecim okresie zaobserwowano, że duża liczba infekcji osłabiła wpływ zaufania społecznego. Zatem wpływ zaufania na liczbę zachorowań jest zależny od poziomu infekcji w społeczeństwie. Im większa liczba zachorowań, tym słabszy wpływ zaufania na rozprzestrzenianie się wirusa.

Kolejnym pytaniem badawczym było poszukiwanie związków między liczbą zachorowań a liczbą osób zaszczepionych dopuszczonymi do użycia szczepionkami w układzie przestrzennym. Podobnie jak w przypadku związków między zaufaniem a liczbą infekcji, także w relacjach między liczbą zaszczepionych osób a liczbą infekcji wykazano związek, przy czym miał on charakter ujemny, mianowicie w przypadku regionów o najwyższym poziomie zaufania zaobserwowano najniższy poziom zaszczepienia. Nie przesądza to jednak o znaczeniu zaufania w stymulowaniu potrzeby zaszczepienia się ludzi dopuszczonymi szczepionkami. Największą rolę ma do odegrania zaufanie do rządu jako istotnego pośrednika między człowiekiem a chorobą. W tym celu rząd powinien budować zaufanie, zapewniając społeczeństwu pełną informację o pandemii przez cały czas jej trwania, nawet wtedy, gdy wiedza jest ograniczona. Rząd musi dostarczyć informacji o ryzykach związanych z zachorowaniem, istnieniu i skuteczności działań oraz środków zapobiegawczych, a także o bezpieczeństwie i skuteczności szczepień. Według W. van der Weerd i in. (2011) informacje o szczepionkach powinny być gromadzone i prezentowane w ścisłej

współpracy z gminnymi służbami zdrowia, placówkami opieki zdrowotnej i mediami, aby skutecznie dotrzeć do społeczeństwa. Pozwoli to zbudować i utrzymać zaufanie do proponowanych szczepionek, które mogą przeciwdziałać rozprzestrzenianiu się choroby. N. Pitas i C. Ehmer (2020) proponują posłużyć się w tym celu narzędziami komunikacji cyfrowej – w większym stopniu niż dotychczas. Cyfrowe formy komunikacji warto wykorzystać jako środek tworzenia zaufania do szczepionek poprzez rozpowszechnianie szczegółowych informacji o pandemii, skutkach choroby, o szczepionkach oraz ich bezpieczeństwie. Istotne jest również aktywne usuwanie potencjalnie szkodliwych dezinformacji.

Literatura

1. Allen J. i in. (2020), *Evaluating the Fake News Problem at the Scale of the Information Ecosystem*, „Science Advances”, 6, 14, s. 1-6.
2. Augustynowicz E., Jackowska T. (2021), *COVID-19 – Szczepionki i szczepienia*, „Przegląd Pediatryczny”, 50, 28, s. 16-26.
3. Bavel J.J.V. i in. (2020), *Using Social and Behavioural Science to Support COVID-19 Pandemic Response*, „Nature Human Behaviour”, 4, s. 460-471.
4. Byłok F. (2020), *Organizacyjny kapitał społeczny w przedsiębiorstwach. Aspekty teoretyczne i empiryczne*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa.
5. Coleman J.S. (1990), *Foundation of Social Theory*, The Belknap Press, Cambridge, London.
6. Dasgupta P. (1988), *Trust as Commodity*, [w:] Gambetta D. (red.), *Trust: Making and Breaking Cooperative Relations*, s. 49-72, Basil Blackwell, Oxford.
7. Freimuth V.S. i in. (2014), *Trust During the Early Stages of the 2009 H1N1 Pandemic*, „Journal of Health Communication”, 19, 3, s. 321-339.
8. Frenkel S., Alba D., Zhong R. (2020), *Surge of Virus Misinformation Stumps Facebook and Twitter*, „The New York Times”, 8th March.
9. GUS (2020), *Jakość życia i kapitał społeczny w Polsce. Wyniki badania spójności społecznej*, GUS, Warszawa.
10. Jalan J., Sen A. (2020), *Containing a Pandemic with Public Actions and Public Trust: The Kerala Story*, „Indian Economy Review”, <https://link.springer.com/article/10.1007/s41775-020-00087-1> (dostęp: 04.09.2021).
11. Jung M., Lin L., Viswanath K. (2013), *Associations between Health Communication Behaviors, Neighborhood Social Capital, Vaccine Knowledge, and Parents' H1N1 Vaccination of Their Children*, „Vaccine”, 31, 42, s. 4860-4866.
12. *Koronawirus w Polsce. Mapa zakażeń* (2021), <https://tvn24.pl/polska/koronawirus-w-polsce-mapa-zakazen-ile-szczepien-ile-nowych-przypadkow-wykryto-16-wrzesnia-2021-4344739> (dostęp: 16.09.2021).
13. Meredith L.S. i in. (2007), *Trust Influences Response to Public Health Messages During a Bioterrorist Event*, „Journal of Health Communication”, 12, 3, s. 217-232.
14. Pitas N., Ehmer C. (2020), *Social Capital in the Response to COVID-19*, „American Journal of Health Promotion”, <https://journals.sagepub.com/doi/pdf/10.1177/0890117120924531> (dostęp: 06.09.2021).
15. Putman R.D. (2000), *Bowling Alone. The Collapse and Survival of American Community*, Simon and Schuster, New York.
16. Quinn S.C. i in. (2013), *Exploring Communication, Trust in Government, and Vaccination Intention Later in the 2009 H1N1 Pandemic: Results of a National Survey*, „Biosecurity and Biodefense”, 11, 2, s. 96-106.
17. Rönnerstrand B. (2013), *Social Capital and Immunisation Against the 2009 A(H1N1) Pandemic in Sweden*, „Scandinavian Journal of Public Health”, 41, 8, s. 853-859.

18. Serwis Rzeczypospolitej Polskiej (2020), *Mapa zarażeń koronawirusem SARS-CoV-2 w Polsce*, <https://www.gov.pl/web/koronawirus/wykaz-zarazen-koronawirusem-sars-cov-2> (dostęp: 14.09.2021).
19. *Raport szczepień przeciwko COVID-19*, <https://www.gov.pl/web/szczepimysie/raport-szczepien-przeciwko-covid-19> (dostęp: 14.09.2021).
20. Swire-Thomson B., Ecker U.H.B. (2018), *Misinformation and Its Correction: Cognitive Mechanisms and Recommendations for Mass Communication*, [w:] Southwell B.G., Thorson E.A., Sheble L. (red.), *Misinformation and Mass Audiences*, s. 195-211, University of Texas Press, Austin.
21. Sztompka P. (2007), *Zaufanie. Fundament społeczeństwa*, Znak, Kraków.
22. Sztompka P. (2012), *Socjologia. Analiza społeczeństwa*, Znak, Kraków.
23. Yamagishi T. (2002), *The Structure of Trust: An Evolutionary Game of Mind and Society*, Hokkaido University Press, Hokkaido.
24. Wrightsman L.S. (1966), *Personality and Attitudinal Correlates of Trusting and Trustworthy Behaviors in a Two-Person Game*, „Journal of Personality and Social Psychology”, 4, s. 328-332.
25. van der Weerd W. i in. (2011), *Monitoring the Level of Government Trust, Risk Perception and Intention of the General Public to Adopt Protective Measures During the Influenza A(H1N1) Pandemic in the Netherlands*, „BMC Public Health”, 11, 575, <https://doi.org/10.1186/1471-2458-11-575>.

PUBLIC TRUST AS A FACTOR INFLUENCING COVID-19 VACCINATION

Abstract: In the consideration of the actions taken to combat the COVID-19 pandemic, it is important to determine the factors conducive to limiting its spread. One of them is public trust, which supports the activities of health care institutions to promote vaccination against COVID-19. The assumption that trust in government, public institutions, and other people significantly determines people's decisions to adopt the vaccine has made it easier to formulate the purpose of the research, which was to seek answers to research questions: To what extent does public trust support efforts to curb the development of pandemics? Does and to what extent does public trust affect the intake of vaccines in the spatial system? The Desk Research were used for the research, with the help of which a critical analysis of secondary data and the deductive method was carried out. As a result of the research, significant links were found between public trust and the level of COVID-19 cases and the number of vaccinated residents in voivodeships in Poland. The obtained research results may be useful in planning activities promoting vaccination against COVID-19.

Keywords: COVID-19, health safety, public trust, vaccination

Rozdział 5

ROZWIĄZANIA SMART CITY SŁUŻĄCE ZARZĄDZANIU MIASTEM W OKRESIE PANDEMII COVID-19

Katarzyna Zadros⁵

Streszczenie: Pandemia COVID-19 spowodowała głębokie zmiany w sposobach zarządzania przestrzenią publiczną w miastach. Podstawowym celem tych zmian było ograniczenie rozwoju pandemii i przenoszenia wirusa między ludźmi. W warunkach pandemicznych w zupełnie nowy sposób musiały także zacząć działać władze miast, by nie tylko przystosować się do wprowadzanych przepisów krajowych, ale również by uwzględnić lokalną specyfikę funkcjonowania społeczeństwa. W rozdziale zostanie przeprowadzona analiza działań typowych dla inteligentnego miasta, wdrażanych w celu zarządzania przestrzenią publiczną w sposób umożliwiający ograniczanie emisji wirusa, a tym samym zmniejszenie liczby zakażeń i zachorowań na COVID-19.

Słowa kluczowe: miasto, pandemia COVID-19, Smart City, zarządzanie

Wprowadzenie

Spółeczeństwa państw wysokorozwiniętych na przestrzeni XX i początku XXI wieku zapomniały o zagrożeniach, jakimi były zarazy dziesiątkujące ludność i paraliżujące funkcjonowanie państw oraz gospodarek. Dlatego wybuch pandemii COVID-19 był całkowitym zaskoczeniem, a zarazem wydarzeniem szokującym, na które w „cywilizowanym świecie” nie było już miejsca. Wprawdzie zdarzały się doniesienia o lokalnych lub regionalnych epidemiach, ale dotyczyły one kraje biedne, zaniedbane gospodarczo, w odległych zakątkach świata, natomiast wydawało się, że Europa, Ameryka Północna, Australia czy bogate kraje Azji czas walki z pandemią miały już za sobą. Z tego względu doniesienia z Chin o wybuchu i szybkim rozprzestrzenianiu się nowej choroby zakaźnej wywołanej nieznanym dotychczas rodzajem koronawirusa pod koniec 2019 roku nie budziły większych obaw. Jednak już kilka miesięcy później okazało się, że wirus nie tylko atakuje mieszkańców niektórych regionów Chin, ale błyskawicznie rozprzestrzenił się w pozostałych częściach świata i pod koniec zimy 2020 roku konieczne było podjęcie z nim walki w skali globalnej. Na ustach mieszkańców całego świata pojawiło się magiczne słowo „lockdown” oznaczające maksymalne zamknięcie gospodarek i wszystkich

⁵ Politechnika Częstochowska, Wydział Zarządzania

obszarów aktywności społecznej ludzi w celu zapobieżenia rozprzestrzenianiu się wirusa oraz powodowanej przez niego choroby COVID-19.

W ciągu kilku tygodni świat przypominał sobie, czym jest pandemia i jakie niesie ze sobą zagrożenia, a także co zrobić, by ograniczyć jej rozprzestrzenianie się. Jednak, mimo że od tego okresu szoku i niedowierzania minęło już kilkanaście miesięcy, ciągle jeszcze utrzymuje się stan powszechnego zagrożenia zdrowia i życia, gdyż choroby nie udało się opanować. Jednocześnie ludzie zaczęli się stopniowo przyzwyczajać do funkcjonowania w pandemicznych warunkach, zaś władze państw oraz zarządzający miastami z różnym skutkiem wprowadzali rozwiązania mające ograniczać emisję wirusa.

Szczególne miejsce w walce z rozprzestrzenianiem się pandemii odegrały nowoczesne technologie cyfrowej komunikacji stosowane w inteligentnych miastach, pozwalające zarządzać miastami i ich częściami tak, by czuwać nad bezpieczeństwem pandemicznym mieszkańców i do minimum ograniczać obostrzenia w przemieszczaniu się i zaspokajaniu potrzeb społecznych. W prezentowanym rozdziale zostanie przedstawione, w jaki sposób wybrane miasta w Polsce i na świecie wykorzystwały nowoczesne technologie do walki z zagrożeniem COVID-19.

Przyczyny zamknięcia społeczeństw i gospodarek z powodu pandemii COVID-19

Zanim poruszony będzie zasadniczy temat, konieczne jest krótkie wyjaśnienie, dlaczego pandemia wywołana przez wirusa SARS-CoV-2 okazała się tak niebezpieczna i wprowadziła zbiorowy strach przed wywoływaną przez niego chorobą COVID-19. Czym zakażenie tym wirusem różni się od innych infekcji wirusowych? Każdego roku w niektórych okresach ludzie chorują na łatwo rozprzestrzeniające się choroby zakaźne wywołane przez wirusy. Najpopularniejszymi od wielu lat wśród tego typu infekcji są choroby grypowe i przeziębienia. Czym różni się od nich COVID-19? Zazwyczaj jego przebieg jest łagodny lub całkowicie bezobjawowy, jednak w niektórych przypadkach ma przebieg ciężki, a około 30% infekcji prowadzi do śmierci osoby zakażonej, spowodowanej ostrym zespołem oddechowym (Krawczyk 2020, s. 28). Ponadto SARS-CoV-2 jest wirusem, który szybko mutuje, a jego kolejne mutacje są coraz bardziej zjadliwe (Welz, Breś-Targowska 2020, s. 263; Drulis-Kawa 2021).

Zakażenie wirusem następuje drogą kropelkową, przez co ma on dużą łatwość rozprzestrzeniania się. Kolejnym problemem jest to, iż do chwili obecnej nie ma skutecznych środków farmaceutycznych, które hamowałyby jego rozwój i tym samym umożliwiały skuteczne leczenie. Poza tym dopiero pod koniec 2020 roku udało się wprowadzić do powszechnego użycia szczepionki, które skutecznie chronią człowieka przed wirusem i jego mutacjami, ale na razie nie można stwierdzić, jak długo ta ochrona będzie się utrzymywała (*Stanowisko...* 2020). Charakterystyka wirusa i zakażenia nim sprawia, że jest on szczególnie groźnym zagrożeniem dla osób starszych, chorych przewlekle, a także pracowników systemu ochrony zdrowia i innych instytucji, którzy mają kontakt z dużą liczbą osób. Dlatego funkcjonowanie instytucji publicznych: urzędów, szkół, uczelni wyższych czy podmiotów leczniczych zostały istotnie zmodyfikowane oraz znacznie ograniczono dostęp do nich obywateli.

Wysokie prawdopodobieństwo infekcji spowodowało, że wprowadzone zostały obostrzenia dostępu do środków komunikacji publicznej, sklepów, kawiarni, restauracji oraz zasad korzystania z przestrzeni publicznej, wprowadzono także zakaz zgromadzeń. Przyjęcie na poziomie państwa tych obostrzeń oraz obowiązek ich egzekwowania w przestrzeni lokalnej spowodowały, że miasta musiały wprowadzić pełną reorganizację funkcjonowania podległych im instytucji oraz przestrzeni publicznej oraz zorganizować kontrolę przestrzegania tych obostrzeń (Allam, Jones 2020). Szybko okazało się, że idealnie nadają się do tego rozwiązania typowe dla inteligentnych miast (ang. *Smart Cities*). Pod tym pojęciem należy rozumieć miasto, „które wykorzystuje technologie informacyjno-komunikacyjne w celu zwiększenia interaktywności i wydajności infrastruktury miejskiej i jej komponentów składowych, a także do podniesienia świadomości mieszkańców” (Albino, Berardi, Dangelico 2015, s. 6). Oznacza to, że inteligentne miasto charakteryzuje się konkurencyjną i wydajną gospodarką, inteligentnymi sieciami transportowymi, zrównoważonym wykorzystaniem zasobów, wysoką jakością życia oraz wysokiej jakości kapitałem ludzkim, a także inteligentnym zarządzaniem miastem (Czupich, Ignasiak-Szulc, Kola-Bezka 2016, s. 225). Dzięki realizacji koncepcji Smart City miasta są w stanie zapewnić swoim mieszkańcom (Masik, Studzińska 2018, s. 564):

- powszechny dostęp do informacji o mieście i jego infrastrukturze,
- sprawne załatwianie spraw urzędowych,
- efektywnie funkcjonujące służby miejskie,
- korzystne warunki inwestowania w mieście,
- sprawną i powszechnie dostępną komunikację,
- bezpieczne środowisko naturalne i społeczne,
- szerokie możliwości spędzania wolnego czasu,
- aktywną partycypację mieszkańców w podnoszeniu jakości życia w mieście.

Specjaliści podkreślają przy tym konieczność uczestniczenia we wprowadzaniu i realizacji cyfrowych rozwiązań mieszkańców miasta, wręcz postrzegają aktywność obywatelską jako kluczowy czynnik powodzenia realizacji w praktyce tej koncepcji. Można więc sądzić, że także w trakcie pandemii COVID-19 mieszkańcy ze zrozumieniem podejść do wprowadzanych zamian w sposobach organizacji życia miast i funkcjonowaniu ich instytucji. Poza tym aktywnie i z pełnym zrozumieniem sytuacji zagrożenia będą współuczestniczyć w życiu swoich miast, opartym na nowych zasadach i rozwiązaniach. W kolejnej części rozdziału zostanie przedstawione to, co zmieniło się w miastach, i jaki jest stosunek mieszkańców do tych zmian.

Inteligentne rozwiązania stosowane przez miasta w zapobieganiu i zwalczaniu zakażeń SARS-CoV-2

Zmiany w organizacji życia miast i ich obywateli łatwo można było zaobserwować, śledząc ruch uliczny, liczbę osób w sklepach czy komunikacji publicznej. Dążenie do zachowania dystansu społecznego, noszenie maseczek i rękawiczek stało się dla wielu osób standardowym zachowaniem. Bardzo szybko większość mieszkańców nauczyła się także korzystać z rozwiązań teleinformatycznych przy załatwianiu spraw urzędowych. Wielu z nich także zmieniło swoje nawyki zakupowe,

korzystając z elektronicznych płatności i zamawiania różnego rodzaju dóbr przez Internet. Takie zmiany zachowań mieszkańców powinny być stymulatorami dla władz lokalnych do wprowadzania zintegrowanej struktury Internetu rzeczy (ang. *Intenet of Things* – IoT), która przyczynia się do wzrostu efektywności działania służb i spółek miejskich, a tym samym poprawiania warunków życia mieszkańców. Wydaje się, że wiele miast dość sprawnie z tym wyzwaniem sobie poradziło.

Najszerzej dostrzegalnymi zmianami w funkcjonowaniu instytucji publicznych było pojawienie się obsługi zdalnej klientów oraz systemu elektronicznej komunikacji z klientem. Co ciekawe – to, co przez wiele lat wydawało się niemożliwe do wykonania, w okresie pandemii udało się praktycznie wszystkim miastom wprowadzić w ciągu kilku dni. Okazało się także, że jest to znacznie szybsza, skuteczniejsza i tańsza forma załatwiania spraw w instytucjach użyteczności publicznej (Szyja 2020, s. 271). Wielu urzędników oraz mieszkańców miast obecnie nie umie sobie wyobrazić, by w urzędzie można było nie stosować takich narzędzi informatycznych, jak e-skrzynka nadawcza, e-PUAP czy elektroniczny urząd, których przydatność od kilku lat wskazywali badacze (Papińska-Kacperek, Polańska 2017, s. 216-225). Zdalna praca pojawiła się także w placówkach ochrony zdrowia, zwłaszcza podstawowej opieki zdrowotnej (POZ), a w ślad za nią rozwiązania informatyczne określane jako pakiet e-zdrowie, w skład którego wchodzi e-recepty, e-zwolnienia, e-skierowania itp. Prawie wszystkie placówki POZ zaczęły także stosować teleporady medyczne jako dominującą formę usług zdrowotnych. Niestety obecnie jest to oceniane jako jeden z kluczowych czynników, które przyczyniły się do nadumieralności Polaków w 2020 roku (Mikołajewska 2021). W podobny sposób działały placówki edukacyjne na wszystkich poziomach szkolnictwa oraz uczelnie wyższe. Zdaniem autorki to, czy taka organizacja kształcenia wpłynęła negatywnie na jego efekty, będzie można w pełni ocenić dopiero za 2-3 lata, przy weryfikowaniu wiedzy i umiejętności, jakie młodzi ludzie zdobywali w trakcie nauki zdalnej.

W wielu miastach rewolucją objęty został system komunikacji publicznej, zaczęły pojawiać się solarne przystanki autobusowe wyposażone w kamery i system analizy tłumu, pozwalający na monitorowanie odległości i liczby pasażerów. Nieliczne miasta, np. Gdynia, zaczęły wykorzystywać algorytmy samouczące się w ramach funkcjonowania monitoringu miejskiego, dzięki czemu możliwe stało się śledzenie skupisk ludzkich i sprawdzanie, czy mieszkańcy stosują się do zakazu gromadzenia się w miejscach publicznych. W tym celu wykorzystano tzw. wyzwalacz detekcji tłumu, odpowiedzialny za wzbudzenie alarmu w razie pojawienia się w określonym miejscu grupy ludzi (Dajerling 2020, s. 42).

W instytucjach publicznych pojawiły się skanery temperatury ludzkiego ciała, działające w podobny sposób jak kamery termowizyjne lub mające postać bramek, przez które każdy wchodzący do danego obiektu musiał przejść. Tego typu urządzenia szczególnie przydatne okazały się w podmiotach leczniczych i na lotniskach, mogły być także stosowane na dworcach kolejowych i autobusowych, a także przez podmioty komercyjne, w wejściach do przedsiębiorstw, biur, restauracji itp. Ich montaż nie był jednak nadzorowany przez instytucje publiczne, ale wynikał z decyzji zarządzających tymi podmiotami (Ostaszewski 2020, s. 52-53). Podobnie wygląda sytuacja z korzystaniem z tzw. stacji dezynfekcji rąk, działającymi na podczerwień i dozującymi środków odkażający bezpośrednio na dłonie. Stacje te wręcz

powszechnie są stosowane w wejściach do budynków użyteczności publicznej, zakładach pracy, a także w wejściach do pomieszczeń sklepowych w galeriach handlowych i wielu innych miejscach charakteryzujących się dużą przepustowością ludzi.

Analizując przyjmowane w Polsce rozwiązania informatyczne, należy także wspomnieć o działaniach realizowanych na poziomie ogólnopolskim. Tu przede wszystkim można wymienić aplikację Kwarantanna Domowa opracowaną przez Ministerstwo Cyfryzacji, która pozwala nadzorować osoby objęte kwarantanną. Na szeroką skalę zaczęto także wykorzystywać Alert Rządowego Centrum Bezpieczeństwa (RCB), czyli informację SMS-ową o zagrożeniach na danym obszarze kraju oraz informującą wjeżdżających do Polski o konieczności poddania się kwarantannie. Jeszcze innym stosowanym na terenie całego kraju rozwiązaniem jest aplikacja ProteGO. Jej celem jest monitorowanie stanu zdrowia jej użytkownika poprzez wypełnienie testu oceny ryzyka i prowadzenie dziennika zdrowia, który, jeśli zajdzie taka konieczność, może być udostępniony personelowi medycznemu (Dajering 2020, s. 43).

Wielu polskich i zagranicznych badaczy problematyki wykorzystania inteligentnych technologii w walce z SARS-CoV-2 zwraca także uwagę na kwestie dotyczące roli informacji w zarządzaniu miastami w okresie pandemii (Lai, Yeung, Celi 2020), która umożliwia jej kontrolę oraz kształtowanie wiedzy obywateli na temat czynników ryzyka zakażenia, postępowania w razie podejrzenia u siebie lub swoich bliskich choroby oraz zasad zapobiegania rozprzestrzenianiu się wirusa, a także prowadzenie kampanii na rzecz szczepienia się. Badacze zwracają również uwagę na konieczność standaryzacji stosowanych w walce z pandemią procedur oraz protokołów komunikacji między miastami, gdyż stosowane dotychczas mają zazwyczaj autorskie rozwiązania, zrozumiałe głównie dla usługodawców. To powoduje niepotrzebną fragmentaryzację informacji i nie pozwala na tworzenie zintegrowanego obrazu rozwoju pandemii, a tym samym zmniejsza skuteczność decyzji umożliwiających jej powstrzymanie (Allam, Jones 2020). Wydaje się jednak, że ten obszar działań w większości polskich miast, podobnie jak na poziomie ogólnopolskim, od początku pandemii był i jest zdecydowanie zaniedbywany. Świadczyć o tym może m.in. liczba osób w pełni zaszczepionych, a także łamanie zasad bezpieczeństwa w okresach zmniejszania się liczby zachorowań i szybki wzrost liczby osób zakażonych oraz chorych na COVID-19 w okresach zwiększonej emisji wirusa.

Problematyka wykorzystania inteligentnych rozwiązań w zarządzaniu miastami w okresie pandemii stała się także przedmiotem zainteresowań badawczych. Odzwierciedleniem tego są podejmowane badania społeczne, w których sprawdza się opinie mieszkańców na temat stosowania inteligentnych rozwiązań w ograniczaniu pandemii COVID-19. Jak wynika z tych badań, Polacy powszechnie akceptują wykorzystanie technologii do walki z SARS-CoV-2, są także gotowi sami wykorzystywać wybrane rozwiązania informatyczne kontrolujące ludzi i ich stan zdrowia w celu eliminowania z miejsc publicznych osób, które mogą stanowić zagrożenie epidemiczne (Duszczyk 2020; Wyrwa, Zarsaś, Wolak 2021).

Analizując podejmowane w ramach inteligentnego miasta inicjatywy na rzecz walki z pandemią, należy także zwrócić uwagę na zagrożenia dla prywatności czy wręcz intymności mieszkańców miast, jakie niesie ze sobą stosowanie przez władze rozwiązań i narzędzi śledzących oraz monitorujących obywateli, a także

przetwarzających i magazynujących pozyskane w ten sposób dane. Umożliwia to naruszanie prywatności obywateli i ich inwigilację. Można wręcz zastanawiać się, czy ich stosowanie nie wiąże się z naruszaniem praw człowieka. Ponadto zgromadzone tak duże ilości danych o dużej liczbie osób stanowią atrakcyjny cel dla ataków hakerów. Jednak jeśli dane te są gromadzone, przechowywane i udostępniane w bezpieczny sposób, technologia wykorzystana do ich zdobycia może być niezwykle skuteczna w ograniczaniu rozmiarów obecnej pandemii, jak i podobnych zdarzeń (Sooryaa Muruga Thambiran 2020), które, jak przewidują epidemiolodzy, będą pojawiały się w przyszłości.

Podsumowanie

Pandemia COVID-19 pozwoliła skutecznie przetestować stosowane w miastach inteligentne technologie oraz zweryfikować ich przydatność w warunkach kryzysowych. Jednocześnie stała się źródłem nowych rozwiązań oraz szybkiego wdrażania rozwiązań teleinformatycznych, które w normalnych warunkach implementowane byłyby przez kilka, a może nawet kilkanaście lat. Stała się także swoistym narzędziem weryfikacji stosowanych w ramach Smart City rozwiązań organizacyjnych i wymiany doświadczeń między zarządzającymi miastami w celu stworzenia dla mieszkańców jak najbezpieczniejszych warunków życia oraz możliwości zaspokajania potrzeb indywidualnych i społecznych.

Czy przyjmowane rozwiązania w dłuższym okresie się sprawdzą i czy władze miast będą chciały z nich korzystać także po opanowaniu sytuacji pandemicznej, dzisiaj trudno wyrokować. Wydaje się jednak, że wiele z nich zostanie już na stałe, znacznie ułatwiając życie mieszkańcom oraz upraszczając im dostęp do usług społecznych oraz administracji publicznej. Natomiast długoterminowa reakcja mieszkańców miast na wprowadzane kryzysowe rozwiązania „smart” będzie prawdopodobnie zależała od oceny, w jakim stopniu władze miast poradziły sobie z zaspokajaniem podstawowych, a jednocześnie sprzecznych potrzeb obywateli, a mianowicie: wolności i bezpieczeństwa oraz z jednej strony prywatności, z drugiej zaś pozyskiwania i korzystania z dostępu do dużej ilości danych o obywatelach.

Literatura

1. Albino V., Berardi U., Dangelico R.M. (2015), *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, „Journal of Urban Technology”, 22, 1, s. 3-21.
2. Allam Z., Jones D.S., *On the Coronavirus (COVID-19) Outbreak and the Smart City Network: Universal Data Sharing Standards Coupled with Artificial Intelligence (AI) to Benefit Urban Health Monitoring and Management*, „Healthcare”, 8, <https://pubmed.ncbi.nlm.nih.gov/32120822/> (dostęp: 21.09.2021).
3. Czupich M., Ignasiak-Szulc A., Kola-Bezka M. (2016), *Czynniki i bariery wdrażania koncepcji Smart City w Polsce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach”, 276, s. 223-235.
4. Dajerling L. (2020), *Wykorzystanie technologii w walce z epidemią koronawirusa SARS-CoV-2. Przegląd rozwiązań stosowanych w wybranych państwach*, „Nowiny Nauki o Bezpieczeństwie”, 1, s. 31-44.

5. Drulis-Kawa Z. (2021), *Koronawirus SARS-CoV-2 – biologia, wykrywanie i zwalczanie*, „Przegląd Uniwersytecki On-Line”, <https://uni.wroc.pl/koronawirus-sars-cov-2-biologia-wykrywanie-i-zwalczanie/> (dostęp: 10.08.2021).
6. Duszczyk M. (2020), *Pandemia otworzyła Polaków na nowe technologie. Ale nie na długo*, <https://cyfrowa.rp.pl/it/art18144741-pandemia-otworzyla-polakow-na-nowe-technologie-ale-nie-na-dlugo> (dostęp: 20.09.2021).
7. *Inteligentne miasta. Czy nowe technologie przyczyniają się do zwalczania pandemii?* (2020), <https://lodz.tvp.pl/48226911/inteligentne-miasta-czy-nowe-technologie-przyczyniaja-sie-do-zwalczania-pandemii> (dostęp: 25.09.2021).
8. Krawczyk K. (2020), *Psychiczne koszty pandemii*, „Medycyna Praktyczna dla Ratowników”, 20.04., s. 28.
9. Lai Y., Yeung W., Celi L.A. (2020), *Urban Intelligence for Pandemic Response: Viewpoint*, „JMIR Public Health Surveill”, 6, 2, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7159057/> (dostęp: 21.09.2021).
10. Masik G., Studzińska D. (2018), *Ewolucja koncepcji i badania miasta inteligentnego*, „Przegląd Geograficzny”, 90, 4, s. 557-571.
11. Mikołajewska M. (2021), *RAPORT: nadmiarowe zgony w 2020 r. Polska w ścisłej czołówce*, <https://www.medonet.pl/koronawirus/koronawirus-w-polsce,nadmiarowe-zgony-w-2020-roku--raport--polska-w-scislej-czolowce,artykul,49396199.html> (dostęp: 28.09.2021).
12. Ostaszewski W. (2020), *Bezpieczeństwo i higiena pracy w czasach pandemii*, „Praca i Zabezpieczenie Społeczne”, 5, s. 51-55.
13. Papińska-Kacperek J., Polańska K. (2017), *E-administracja idea Open Government w administracji lokalnej w Polsce*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu”, 475, s. 215-225.
14. Sooryaa Muruga Thambiran S. (2020), *How COVID Accelerated Smart City Development*, „GCN”, <https://gcn.com/articles/2020/10/15/smart-cities-post-covid.aspx> (dostęp: 27.09.2021).
15. *Stanowisko naukowców dotyczące szczepień przeciwko SARS-CoV-2* (2020), <https://www.uw.edu.pl/stanowisko-naukowcow-dotyczace-szczepien-przeciwko-covid-19/> (dostęp: 05.08.2021).
16. Szyja P. (2020), *Funkcjonowanie administracji publicznej w sytuacji kryzysu spowodowanego czynnikami zewnętrznymi – studium przypadku COVID-19*, „Rocznik Administracji Publicznej”, 6, s. 267-281.
17. Welz A., Breś-Targowska A. (2020), *Koronawirus – aktualny problem medyczny i społeczny*, „Terapia i Leki”, 76, 5, s. 263.
18. Wyrwa J., Zaraś M., Wolak K. (2021), *Smart Solutions in Cities during the COVID-19 Pandemic*, „Virtual Economics”, 4, 2, s. 88-103.

SMART CITY SOLUTIONS FOR CITY MANAGEMENT DURING THE COVID-19 PANDEMIC

Abstract: The COVID-19 pandemic has caused profound changes in the ways of managing public space in cities. The primary goal of these changes was to limit development of the pandemic and transmission of the virus between people. In pandemic conditions, city authorities had to start operating in a completely new way: adapt to the introduced national regulations, and also to take into account the local society and its specificity. The chapter will analyze the typical measures for a smart city implemented to manage public space in a way that allows reducing the virus emission, and thus reducing number of infections and cases of COVID-19 disease.

Keywords: city, management, COVID-19 pandemic, Smart City

Rozdział 6

WPŁYW KOMUNIKACJI INTERPERSONALNEJ NA POCZUCIE BEZPIECZEŃSTWA PRACOWNIKÓW W DOBIE PANDEMII

Agata Przewoźna-Krzemińska⁶

Streszczenie: Wybuch globalnej pandemii spowodował szereg zmian w każdym aspekcie życia, nie tylko gospodarczego, społecznego, zdrowotnego czy naukowego, ale także w komunikacji międzyludzkiej. Komunikacja interpersonalna z wykorzystaniem nowoczesnych technologii, szczególnie w tym trudnym dla społeczeństwa okresie, ma za zadanie zapewnić poczucie bezpieczeństwa fizycznego, ale przede wszystkim psychicznego pracowników. Właściwa i otwarta komunikacja oraz skuteczne informowanie o aktualnej sytuacji ma kluczowe znaczenie dla bezpieczeństwa i poprawy jakości życia w warunkach kryzysu. Celem rozdziału jest próba odpowiedzi na pytanie, jak komunikować się z pracownikami i informować o zmianach w czasie pandemii, aby zapewnić ich bezpieczeństwo.

Słowa kluczowe: bezpieczeństwo, komunikacja interpersonalna, organizacja, pandemia

Wprowadzenie

Pandemia spowodowała zmiany w życiu na całym świecie. Interakcje (społeczne, zawodowe, naukowe, gospodarcze) oraz komunikacja interpersonalna zostały w większości branż zawodowych przeniesione do sieci (nastąpiła izolacja domowa), uzależnione od nowych technologii i inteligentnego otoczenia. Problemem w sytuacji kryzysu zdrowotnego stała się komunikacja z otoczeniem – jak należy informować o zaistniałej sytuacji, szczególnie, że większość firm z różnych branż i sektorów stanęło przed wyzwaniem „jak przetrwać”, „czy zwolnić pracowników”, „jak zabezpieczyć pracowników przed zakażeniem koronawirusem”. Pandemia doprowadziła do zmian w sposobie funkcjonowania organizacji, przede wszystkim nastąpiło ograniczenie kontaktów między pracownikami, zmieniła się komunikacja wewnętrzna, która okazała się jednym z kluczowych obszarów, na którym musiało się skupić wiele firm, starając się ograniczyć negatywny wpływ pandemii na swoją działalność. Z dnia na dzień zaczęło się tworzyć społeczeństwo cyfrowe i informacyjne.

⁶ Politechnika Częstochowska, Wydział Zarządzania

Przedstawione w rozdziale uwagi i wnioski stanowią punkt wyjścia do dalszych analiz i badań dotyczących procesu komunikacji w trakcie trwania pandemii. Hipoteza, jaką postawiono dla zrealizowania celów rozdziału, brzmiała następująco: *W dobie pandemii informacja (komunikacja, manipulacja) odgrywa kluczową rolę w bezpieczeństwie pracowników.*

Koronawirus a komunikacja w organizacjach

Jednym z podstawowych obszarów związanych z zarządzaniem, na którym musiały się skupić przedsiębiorstwa, okazała się komunikacja wewnętrzna, pozwalająca na ograniczenie negatywnego wpływu pandemii na działalność gospodarczą. Dzięki sprawnej komunikacji wewnętrznej przedsiębiorcy z każdego sektora gospodarczego mieli szansę ograniczyć skutki nieprzewidywalnej sytuacji związanej z pandemią. W każdej branży znaczenie i wpływ komunikacji bywa różny, ale istotne jest, że rzutuje ona nie tylko na samopoczucie, ale także na zachowanie pracowników i pracodawców, które w czasie pandemii mogło się przyczynić do poprawy bezpieczeństwa.

Przedmiotem analizy prezentowanego rozdziału jest zagadnienie wpływu komunikacji i informacji na poczucie bezpieczeństwa pracowników w dobie pandemii. W opracowaniu zostały zdefiniowane przykładowe pojęcia, np. „komunikacja interpersonalna”, „bezpieczeństwo” i „pandemia”. Z uwagi na to, że w 2021 roku brak było aktualnych oraz spójnych badań, które by obrazowały, jak komunikacja może wpływać na poczucie bezpieczeństwa w warunkach pandemii, kryzysu, czyli zmiany, w części empirycznej zostały wykorzystane i przeanalizowane fragmenty wybranych badań (nawiązujących do komunikacji w organizacji) zapożyczone z raportu *Bezpieczeństwo w pracy w Polsce 2020* (Raport 2021). W związku z wybuchem pandemii COVID-19 w 2020 roku organizacje (firmy, spółki, firmy produkcyjne, sieci handlowe, banki, zakłady opieki zdrowotnej, placówki oświatowe, finansowe itd.) stanęły przed wyzwaniem szybkiego (natychmiastowego) wdrożenia procedur bezpieczeństwa, a także przed koniecznością błyskawicznego i skutecznego poinformowania (przekonania) swoich pracowników o obligatoryjnych zasadach i obowiązku ich przestrzegania. Całkowicie nowe obowiązujące zasady dotyczyły zmienionej organizacji pracy, obostrzeń dotyczących odstępów między pracownikami oraz reżimu sanitarnego (mycie, dezynfekowanie rąk, noszenie ubrań i masek ochronnych). Każdy zatrudniony pracownik z dnia na dzień był zobowiązany do przyswojenia nowych, niezwykle odpowiedzialnych zasad, aby zachować bezpieczeństwo w pracy. Było to związane nie tylko z własnym zdrowiem, ale także ze zdrowiem współpracowników, a w konsekwencji rodziny i całego otoczenia (zarówno wewnętrznego, jak i zewnętrznego). I tu kluczowa stała się rola komunikacji wewnętrznej, której wykorzystywanie miało na celu utrzymanie zdrowia (fizycznego, psychicznego) pracowników, a w konsekwencji płynnego funkcjonowania firmy. W przypadku wielu firm komunikacja z pracownikami miała duże znaczenie, szczególnie w sytuacji globalnych, medialnych informacji dotyczących nadchodzącego kryzysu gospodarczego i zwolnień pracowniczych. To właśnie dzięki komunikacji pracownicy czuli się pewniej w organizacji, co z kolei wiązało się z ich wydajnością w pracy i pozytywnie wpływało na funkcjonowanie przedsiębiorstwa.

Uwarunkowania teoretyczne komunikacji interpersonalnej

Temat komunikacji interpersonalnej podejmowany jest od lat przez badaczy tego zjawiska. Pojęcie „komunikacja” zostało zdefiniowane przez teoretyków przedmiotu. Termin ten ma swoje korzenie w łacińskim słowie „comunico” lub „comunicare”, które oznacza „łączyć wspólnie”. Na uwagę zasługuje definicja M. Niecia, który określa komunikowanie jako „rodzaj kontaktu nawiązanego za pomocą zmysłów, bądź także specjalnie do tego przystosowanych narzędzi (środków komunikowania), między co najmniej dwiema osobami, z których jedna (nadawca) przekazuje drugiej (odbiorcy) za pomocą zrozumiałych dla nich znaków pewne treści pojęciowe lub emocje z zamiarem wywołania u odbiorcy określonych reakcji” (Nieć 2010, s. 19). Ważna jest także definicja B. Dobek-Ostrowskiej, która określa komunikowanie jako „proces porozumiewania się jednostek, grup lub instytucji, którego celem jest wymiana myśli, dzielenie się wiedzą, informacjami i ideami. Proces ten odbywa się na różnych poziomach, przy użyciu zróżnicowanych środków i wywołuje określone skutki” (Dobek-Ostrowska 2004, s. 13). Z. Nęcki zwraca natomiast uwagę na niewerbalne aspekty komunikacji interpersonalnej, określając ją jako „wymianę werbalnych, wokalnych i niewerbalnych sygnałów (symboli), w celu osiągnięcia lepszego poziomu współdziałania” (Nęcki 2000, s. 109). W każdej organizacji komunikacja ma priorytetowe znaczenie dla jej efektywności i składa się z szeregu komponentów, a „każdy opis komunikowania musi opierać się na schemacie pojęciowym, obejmującym trzy podstawowe elementy: nadawcę, przekaz (komunikat, kanał), odbiorcę” (Nieć 2010, s. 14). Aby wystąpił proces komunikacji, muszą wystąpić te trzy elementy. Zdaniem D. Stewart „jakość przekazywanej komunikacji wpływa znacząco na zachowanie się ludzi, na ich wydajność, zaangażowanie, motywację czy nawet energię” (Stewart 1996, s. 323). W każdej firmie nadawcą jest zwykle jednostka posiadająca wiedzę, kompetencje, informację, potrzebę, cel, a także chęć przekazania informacji innym osobom. Jeżeli przekaz nie dociera do odbiorcy, to „komunikowanie nie nastąpiło, i sytuacji nie poprawi nawet fakt, że przekaz dotrze do odbiorcy, ale będzie dla niego niezrozumiały” (Stoner 1996, s. 511). Literatura przedmiotu wymienia komponenty w procesie komunikowania, czyli „ludzi (źródło, nadawca, odbiorca), wiadomość, kanał, szum, sprzężenie zwrotne oraz kontekst sytuacyjny” (Stankiewicz 2006, s. 51). Odpowiedź to informacja zwrotna określana jako sprzężenie zwrotne (Morozowski 2012, s. 24). Komunikacja interpersonalna pełni szereg funkcji, a młode pokolenia (szczególnie w okresie pandemii, nauki i pracy zdalnej) wykorzystują przede wszystkim nowoczesne technologie i zmodernizowane narzędzia do komunikacji typu social media, aplikacje itd.). Komunikacja interpersonalna dzieli się na komunikację werbalną, niewerbalną, formalną, nieformalną, pionową, poziomą, jednostronną, dwustronną. W ostatnim „pandemicznym” okresie te klasyczne podziały zostały wzbogacone o komunikację zdalną, która wyparła komunikację niewerbalną. Literatura wyróżnia także komunikację skierowaną do wewnątrz i na zewnątrz organizacji (komunikacja wewnętrzna i komunikacja zewnętrzna). Komunikacja interpersonalna pełni bardzo wiele funkcji w firmach. Przykładowo T. Listwan wyróżnia funkcje: informacyjną, instruktażową, kontrolną, integracyjną, ekspresyjną i motywacyjną (Listwan 2004, s. 289). W literaturze przedstawia się także trzy modele komunikacji

interpersonalnej: agresywny, uległy i asertywny. W celu poprawnego asertywnego komunikowania nadawca powinien potrafić słuchać, aby poznać potrzeby rozmówcy i w odpowiedni sposób prowadzić z nim dialog. Zasada komunikacji asertywnej brzmi: „Dwa monologi nie czynią dialogu” (Jeff Daly). Ważne jest, aby w trakcie procesu komunikowania słuchać nadawcy oraz mieć szacunek do swojego rozmówcy, nie przerywać komunikatu i zachowywać się etycznie. Korzystając z komunikatorów internetowych, w większości przypadków nie widzimy naszego odbiorcy, co może przełożyć się na błędną interpretację komunikatów. Aktualnie pojawiły się nowe bariery komunikacyjne, np. filtrowanie, różnice w percepcji, chaos informacyjny, emocje, wybiórcze postrzeganie, płec i dysonans kształtujący się między przekazem werbalnym a niewerbalnym. Podsumowując, należy stwierdzić, że „komunikacja interpersonalna” to „proces werbalnego i niewerbalnego dzielenia się informacjami i emocjami z inną osobą, określana jest także jako proces porozumiewania się jednostek, grup czy też instytucji, których celem jest dzielenie się informacjami, myślami i ideami” (Wilsz 2009, s. 404). Natomiast „komunikowanie” jest często określane w literaturze przedmiotu jako interakcja oraz oddziaływanie społeczne przy pomocy komunikatów. W wielu przypadkach (zazwyczaj zamierzonych, ale niekoniecznie) w komunikacji wykorzystywana jest manipulacja, która definiowana jest jako „forma wywierania wpływu na osobę lub grupę, w taki sposób, aby nieświadomie i z własnej woli realizowała cele manipulatora. Jest to umiejętność rządzenia innymi, znajomość zasad dowodzenia, prowadzenia negocjacji, aby skłonić partnera do zmiany zdania” (Cialdini 2016, s. 186). Ludźmi można manipulować w przeróżny sposób (za pomocą słów, gestów, znaków). Pojawia się coraz więcej nowatorskich sposobów manipulacji. Coraz trudniej jest też odróżnić, czy to jeszcze komunikacja, czy już manipulacja. Przykładem zastosowania komunikacji (z przewagą komunikacji niewerbalnej) z elementami manipulacji są tzw. „mowy motywacyjne” (rodzaj przemówienia, wystąpienia bardzo ekspresyjnego i emocjonalnego, wzbogaconego elementami niewerbalnymi, np. mimiką, gestykulacją). Celem mowy motywacyjnej jest pobudzenie do realizacji założonych celów (w przypadku pracowników pobudzenie do zaangażowania w realizację planów, zespołowe pobudzenie do działania itp.). Nowym, niezwykle ważnym aspektem komunikacji jest zarządzanie przez komunikację, które polega na „budowie i doskonaleniu systemu ciągłego informowania zespołów pracowniczych o głównych celach, problemach i kryzysach w organizacji, zamierzeniach kierownictwa oraz aktualnej i docelowej pozycji na rynku. Nadrzędnym celem zarządzania przez komunikację jest stworzenie dobrych stosunków pomiędzy pracownikami a kierownikami, co wpływa na zaangażowanie, zapobiega kryzysom” (Przewoźna-Krzemińska 2017, s. 25).

Bezpieczeństwo w sytuacji pandemii

Bezpieczeństwo zawsze było priorytetem każdego człowieka i organizacji przez niego tworzonych, ale dopiero na początku XXI wieku naukowcy poświęcili więcej uwagi temu zjawisku. W 2011 roku bezpieczeństwo uznano za dyscyplinę naukową. Termin „bezpieczeństwo” jest definiowany niezwykle szeroko, najczęściej określany jest jako „stan, w którym jednostka, grupa społeczna, organizacja, państwo nie odczuwa zagrożenia swego istnienia lub podstawowych interesów;

sytuacja, w której występują formalne, instytucjonalne i praktyczne gwarancje ochrony”. Bezpieczeństwo to naczelna potrzeba człowieka i instytucji przez niego tworzonych, ponieważ związane jest ono z rozwojem społecznym i cywilizacyjnym. Pewność tej tezy wynika z analizy uwarunkowań rozwoju cywilizacyjnego człowieka w różnych okresach historycznych i uwarunkowań kulturowych, w których podmiot bezpieczeństwa funkcjonował. Znaczenie bezpieczeństwa dla jego podmiotu warunkowane było rozwojem cywilizacyjnym oraz kulturowym (Czupryński 2008, s. 139). „Bezpieczeństwo” jest antonimem „zagrożenia”, które może pozbawić człowieka stanu stabilności. Literatura wyróżnia na przykład następujące rodzaje bezpieczeństwa: polityczne, militarne, ekonomiczne, społeczne, kulturowe, ideologiczne, religijne, morskie, ekologiczne, zewnętrzne i wewnętrzne. Wybuch pandemii COVID-19, której nikt na świecie się nie spodziewał, stał się zagrożeniem bezpieczeństwa dla wszystkich. Pojawił się wcześniej niezdefiniowany kryzys w obszarze bezpieczeństwa zdrowotnego (w konsekwencji także w obszarze bezpieczeństwa społecznego, gospodarczego, politycznego i naukowego). W związku z epidemią COVID-19 w środkach masowego przekazu powstał natłok informacji na temat sytuacji pandemicznej na świecie. Informacje te jednak nie zawsze były rzetelne i prawdziwe, a często miały charakter wręcz dezinformujący. Media od zawsze miały wpływ na kształtowanie nastrojów społecznych, ale w chwili wybuchu globalnej pandemii zalew informacji dotyczących zakażeń czy zgonów każdego dnia od marca 2020 roku spowodował uczucie lęku i duże poczucie zagrożenia bezpieczeństwa nie tylko zdrowotnego, ale społecznego, gospodarczego itd. Dodatkowo praca i nauka zdalna naruszyły wszelkie normy bezpiecznego funkcjonowania jednostki, zaburzone zostały podstawowe potrzeby bezpieczeństwa z piramidy Masłowa. Brak relacji i kontaktów interpersonalnych, powszechna cyfryzacja i związane z nią problemy technologiczne, nadmierna inwigilacja, kontrola, a w rezultacie znużenie i zmęczenie oraz wszelkie zagrożenia (cyberzagrożenia, cyberprzestępczość) i nadmiar informacji medialnych stały się zagrożeniem bezpieczeństwa psychicznego. W dobie pandemii dysfunkcje i problemy natury psychicznej dotknęły znaczną część społeczeństwa, szczególnie młodych ludzi. Komunikacja w trakcie pandemii była prowadzona dynamicznie. Oczywiście jest, że w sytuacji zagrożenia należy komunikować szybko, systematycznie, otwarcie i odpowiedzialnie. Dotknięte kryzysem firmy bardzo często poprzez swoją postawę uspakajały nastroje w zespołach pracowniczych, przedstawiając realną sytuację i swoje priorytety. Skuteczna komunikacja w kryzysie wymagała zwykle podjęcia działań przez sztaby kryzysowe, w których skład wchodziły kluczowe osoby w firmie (zarząd, menedżerowie) odpowiedzialne za przepływ informacji. W organizacjach nastąpiło wzmocnienie działań komunikacyjnych skierowanych do pracowników w czasie pandemii.

Analiza raportu

Jak wskazuje Barometr Zaufania Edelmiana, 63% społeczeństwa ufa komunikacji prowadzonej przez firmy. Pracodawca powinien przejąć inicjatywę i stać się najważniejszym źródłem informacji w kontekście sytuacji organizacji i jej planów (Edelman... 2021). Opóźnienie zwiększa ryzyko, że zespół zacznie bazować na

nieoficjalnych, często nieprawdziwych doniesieniach, co dodatkowo zwiększy jego niepewność. Człowiek od chwili urodzenia jest pod wpływem oddziaływania innych osób, na które sam także oddziałuje. Problem manipulacji dotyczy każdej jednostki. W momencie zagrożenia pandemią COVID-19 wybuchła globalna wojna informacyjna i nastąpiła wszechobecna manipulacja informacją. Społeczeństwo jest atakowane tzw. fake newsami, czyli fałszywymi, celowymi informacjami, które mają wprowadzić w błąd odbiorcę. Na bieżąco powstają tendencyjne teorie spiskowe, podawane są fałszywe wiadomości, następuje dezinformacja. W tej sytuacji społeczeństwu trudno jest odróżnić dowody naukowe i fakty od mniej wiarygodnych źródeł informacji, które dominują w mediach, szczególnie w mediach społecznościowych. Dla celów rozdziału zaprezentowano 7. edycję raportu *Bezpieczeństwo pracy w Polsce 2020* (Raport 2021), który stanowi odpowiedź na nieoczekiwane wyzwania, przed jakimi stanęły firmy na całym świecie. Raport jest cykliczną publikacją Koalicji Bezpieczni w Pracy, która powstała w 2014 roku w celu promocji kultury bezpieczeństwa w miejscu pracy. Obecnie zrzesza 5 niezależnych firm: CWS Polska, PW Krystian, Tencate Protective Fabrics, SEKA SA i DHL, w Polsce reprezentowany przez dwie dywizje: DHL Parcel i DHL Supply Chain. Koalicja prowadzi dynamiczną działalność edukacyjną w zakresie obowiązujących norm i procedur bhp, wspierając pracodawców we wdrażaniu wysokich standardów bezpieczeństwa i wskazując realne korzyści płynące z ich przestrzegania. Pandemia COVID-19 miała wpływ na spowolnienie gospodarcze i kondycję finansową polskich firm. Dotyka to głównie zmian w postrzeganiu bhp, organizacji pracy, optymalizacji kosztów działania, gotowości do zmian i reorganizacji w firmie. I tu kluczowa okazała się rola komunikacji wewnętrznej, a polskie firmy zmuszone były reagować szybciej niż ustawodawca. Celem prezentowanego projektu było kompleksowe zbadanie zakresu wpływu pandemii COVID-19 na bezpieczeństwo i organizację pracy polskich firm. Badanie składało się z dwóch części:

- I część: „Pracodawcy” – obejmowała zbadanie opinii pracowników odpowiadających za bezpieczeństwo i organizację pracy (w tym działania związane z pandemią). Pomiar został zrealizowany metodą wywiadu telefonicznego (CATI) na próbie 200 osób.
- II część: „Pracownicy” – obejmowała zbadanie opinii pracowników. Pomiar został zrealizowany metodą wywiadu online (CAWI) z wykorzystaniem panelu internetowego SW Panel na próbie 1517 osób.

Próby badawcze w obu częściach projektu zostały dobrane w taki sposób, aby reprezentować struktury branż obecnych w polskiej gospodarce. Badanie zostało przeprowadzone w dniach 21 lipca – 17 sierpnia 2020 roku. W kontekście przygotowania do pracy zdalnej ankietowani przyznali, że firmy powinny zadbać o edukację pracowników dostosowaną do nowych realiów świadczenia pracy, np. w formie dodatkowych szkoleń dotyczących obsługi sprzętu firmowego (93% odpowiedzi), bezpieczeństwa danych (87%) oraz szkoleń bhp dostosowanych do sytuacji pracy zdalnej. Niewielu pracodawców (niecałe 14%) było zdania, że firmy powinny zapewniać pracownikom dodatkowe ergonomiczne przyrządy do przygotowania miejsca pracy. Pytania dotyczyły wdrożonych działań i poczucia bezpieczeństwa. Na pytanie: „Jakie działania z zakresu bezpieczeństwa i higieny pracy wdrożyła Pani/Pana

firma w związku z pandemią COVID-19?” (próba 200 pracowników) – 89% badanych pracowników odpowiedziało, że nastąpiła intensyfikacja komunikacji wewnętrznej w firmie. Inne pytanie brzmiało: „Czy działania z zakresu bezpieczeństwa i higieny pracy zostały wdrożone przez Państwa firmę z własnej inicjatywy, jeszcze przed oficjalnym zamrożeniem gospodarki?” (próba 199 pracowników) – 21% badanych pracowników odpowiedziało, że nastąpiła intensyfikacja komunikacji wewnętrznej w firmie. Pracodawcy także pozytywnie ocenili wpływ wdrożonych przez siebie działań na zabezpieczenie pracowników przed zagrożeniami psychofizycznymi. Najlepiej ocenianymi działaniami w tym zakresie były: system pracy rotacyjnej (81% pozytywnych ocen), dostosowanie zakładu pracy do nowych wymogów sanitarnych (77%) oraz intensyfikacja komunikacji wewnętrznej w firmie (76%). Najgorzej oceniana przez pracodawców była decyzja o wysłaniu pracowników na obowiązkowe urlopy (59%). Dodatkowe działania z zakresu bhp częściej zauważane były przez pracowników większych firm. Wszystkie wymieniane zjawiska były częściej odnotowywane przez osoby pracujące w zakładach pracy zatrudniających powyżej 250 pracowników niż w firmach o małej lub średniej wielkości.

Podsumowanie

Analizując wyniki badań, należy zauważyć, że wprowadzenie pracy zdalnej w trakcie pandemii spowodowało negatywne skutki psychofizyczne, w tym problemy z komunikacją interpersonalną, a w konsekwencji poczucie wyizolowania. Podsumowując rozważania dotyczące wpływu chaosu informacyjnego i cyberzagrożeń na psychikę ludzką w czasie pandemii, warto podkreślić, że kluczowe jest ze strony właściwych organizacji (przede wszystkim państwa) zapewnienie bezpieczeństwa online, opracowanie net-etykiety, a w sytuacji codziennego korzystania ze zdalnej formy komunikacji (pracy, nauki) priorytetem powinno być zagwarantowanie najwyższych standardów bezpieczeństwa w celu zniwelowania stresu, aby ograniczyć i zapobiec powstawaniu dysfunkcji psychicznych oraz fizycznych, szczególnie młodego pokolenia. Zdrowi, racjonalnie myślący młodzi ludzie są gwarancją bezpieczeństwa dla wszystkich pokoleń. Ważne jest, że badane firmy zwracały uwagę na jakość i formę komunikacji w celu zapewnienia bezpieczeństwa swoim pracownikom.

Literatura

1. Armstrong M. (2005), *Zarządzanie zasobami ludzkimi*, Oficyna Ekonomiczna, Kraków.
2. Cialdini R. (2016), *Teoria wywierania wpływu*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk.
3. Czubasiewicz H., Wróbel P. (2012), *Komunikacja społeczna – wpływ na zachowania w organizacji*, [w:] Rutka R., Wróbel P. (red.), *Organizacja zachowań zespołowych*, s. 82-111, PWE, Warszawa.
4. Czupryński A. (2008), *Metodologia nauk*, Aureus, Kraków.
5. Dobek-Ostrowska B. (2004), *Podstawy komunikowania społecznego*, Wydawnictwo Astrum, Wrocław.

6. Dobek-Ostrowska B. (2007), *Komunikowanie polityczne i publiczne*, Wydawnictwo Naukowe PWN, Warszawa.
7. Edelman Trust Barometr (2021), *Wyniki corocznego badania zaufania Edelman Trust Barometer 2021 – spadek zaufania do źródeł informacji i rosnąca rola biznesu*, <https://lhse.pl/wyniki-corocznego-badania-zaufania-edelman-trust-barometer-2021-spadek-zaufania-do-zrodel-informacji-i-rosnaca-rola-biznesu/> (dostęp: 10.09.2021).
8. Głodowski W. (2006), *Komunikowanie interpersonalne*, Hansa Communication, Warszawa.
9. Listwan T. (2004), *Zarządzanie kadrami*, C.H. Beck, Warszawa.
10. Morozowski M. (2012), *Media masowe. Władza, rozrywka i biznes*, Oficyna Wydawnicza ASPRA-JR, Warszawa.
11. Necki Z. (2000), *Komunikacja międzyludzka*, Oficyna Wydawnicza Antykwa, Kraków.
12. Nieć M. (2010), *Komunikowanie społeczne i media. Perspektywa politologiczna*, Wolters Kluwer, Warszawa.
13. Przewoźna-Krzemińska A. (2017), *Komunikacja interpersonalna w relacjach przełożony – podwładny na przykładzie instytucji samorządowej*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie”, 25, 1, s. 21-29.
14. Przewoźna-Krzemińska A., (2013), *Wpływ komunikacji interpersonalnej na relacje zespołów pracowniczych w sytuacjach konfliktowych*, [w:] Bsoul M., Bylok F. (red.), *Związki zawodowe w procesie przemian społeczno-gospodarczych w Polsce i wybranych krajach Unii Europejskiej*, s. 278-291, Wydawnictwo Naukowe Śląsk, Katowice.
15. Raport (2021), *Bezpieczeństwo w pracy w Polsce 2020*, <https://www.seka.pl/raport-bezpieczenstwo-pracy-polsce-2020/> (dostęp: 10.09.2021).
16. Stankiewicz J. (2006), *Komunikowanie się w organizacji*, Astrum, Wrocław.
17. Stewart D.M. (red.) (1996), *Praktyka kierowania. Jak kierować sobą, innymi i firmą*, PWE, Warszawa.
18. Stoner J. (1996), *Kierowanie*, PWE, Warszawa.
19. Wilsz J. (2009), *Teoria pracy*, Oficyna Wydawnicza Impuls, Kraków.
20. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. nr 179 poz. 1065).

THE IMPACT OF INTERPERSONAL COMMUNICATION ON THE SENSE OF SECURITY IN THE PANDEMIC ERA

Abstract: The outbreak of the global pandemic caused numerous changes in every aspect of our life, not only economic, social, health, or scientific, but also in interpersonal communication. Interpersonal communication with the use of modern technologies, especially in this difficult period for the society, has the aim to ensure a sense of security not only physical, but above all mental security. A proper and open communication, as well as effective information on the present circumstances, is essential for the safety and improvement of the quality of life in crisis conditions. The aim of the chapter is to try to answer the question of how to communicate with the employees and inform them about the changes during the pandemic in order to ensure their safety.

Keywords: interpersonal communication, organization, pandemic, security



Bezpieczeństwo informacyjne

Rozdział 7

ZARZĄDZANIE BEZPIECZEŃSTWEM CYFROWYM W SMART CITY

Konrad Głębocki⁷

Streszczenie: Celem niniejszego rozdziału jest systematyzacja zagadnień związanych z bezpieczeństwem cyfrowym w Smart City oraz sformułowanie rekomendacji dla miast w tym obszarze. Autor, dokonując przeglądu literatury, usystematyzował przedmiotową problematykę w następujące elementy: bezpieczeństwo cyfrowe i pojęcia bliskoznaczne, Smart City a bezpieczeństwo cyfrowe, klasyfikacja zagrożeń cyfrowych w Smart City, Internet rzeczy jako szczególnie narażony element Smart City oraz system zarządzania bezpieczeństwem cyfrowym. W relacji do tego ostatniego elementu autor sformułował rekomendacje dla miast aspirujących do miana Smart City.

Słowa kluczowe: bezpieczeństwo cyfrowe, Smart City, zarządzanie miastem

Wprowadzenie

Smart City staje się koncepcją istotną nie tylko dla miast globalnych, ale w coraz większym stopniu dla miast średniej wielkości. Coraz to większe i „sprytniejsze” wykorzystanie technologii ICT i w ogóle nowoczesnych technologii w połączeniu z inteligentnym społeczeństwem stanowi dużą szansę na podniesienie jakości życia. Jednak pojawiają się także zagrożenia dotyczące bezpieczeństwa cyfrowego. Mieszkańcy miast będą bardziej skłonni do korzystania z nowoczesnych aplikacji i rozwiązań ułatwiających życie, jeśli będzie to dla nich bezpieczne, a ich prywatność będzie odpowiednio zabezpieczona. Celem niniejszego rozdziału jest systematyzacja zagadnień związanych z bezpieczeństwem cyfrowym w Smart City. Podstawową wykorzystaną metodą badawczą jest przegląd literatury zagranicznej i polskiej. Ponadto przywołane zostały przypadki zagrożeń, które wystąpiły w odniesieniu do miast oraz jednego z urzędów marszałkowskich.

Bezpieczeństwo cyfrowe i pojęcia bliskoznaczne

Bezpieczeństwo cyfrowe (ang. *digital security*) stanowi wg niektórych badaczy obszar o olbrzymim potencjale rozwojowym dla tych, którzy chcieliby się poświęcić

⁷ Politechnika Częstochowska, Wydział Zarządzania

pracy nad nim (Schneier 2015, s. XXV). Wydaje się, że bezpieczeństwo cyfrowe w całości polega obecnie na ochronie, tj. na szyfrowaniu, zaporach itd. Zasadniczo nie prowadzi się wykrywania, odpowiedzi i audytowania (Schneier 2015, s. 9). Poza tym przy budowaniu systemów informatycznych zapomina się o bezpieczeństwie fizycznym – np. laptopy z poufnymi informacjami są często kradzione (Schneier 2015, s. 284).

W analizie aspektów związanych z problematyką bezpieczeństwa cyfrowego bardzo istotne jest zdefiniowanie samego pojęcia. Po pierwsze termin „bezpieczeństwo cyfrowe” używany jest zamiennie z innymi terminami, takimi jak: „bezpieczeństwo komputerowe”, „bezpieczeństwo sieci i systemów”, a także „inżynieria bezpieczeństwa” oraz „bezpieczeństwo informacyjne” i „bezpieczeństwo informatyczne”. Pojęcia te wpisują się w ogólnie definiowane bezpieczeństwo informacji (Mosiądz, Sobiech, Wójcik 2019, s. 40). Bezpieczeństwo informacji ma szerszy zakres znaczeniowy niż bezpieczeństwo cyfrowe – obejmuje także informacje utwalone na innych niż cyfrowe nośnikach – np. na papierze. Do tego można byłoby dodać jeszcze termin „cyberbezpieczeństwo”, który jednak jest tożsamy z pojęciem „bezpieczeństwo sieci”.

Z punktu widzenia nauki bezpieczeństwo cyfrowe jest niewątpliwie zagadnieniem interdyscyplinarnym, wchodzącym w zakres nauk związanych z informatyką, socjologią, zarządzaniem, naukami o bezpieczeństwie. Ponadto, z punktu widzenia kontekstu Smart City, zagadnienie bezpieczeństwa cyfrowego wchodzi także w zakres subdyscypliny, jaką jest zarządzanie publiczne. Stąd też problematyczne jest klasyfikowanie bezpieczeństwa cyfrowego wyłącznie jako subdyscypliny nauk o bezpieczeństwie.

W zagranicznych opracowaniach w kontekście bezpieczeństwa cyfrowego bardzo często występuje termin „cyberbezpieczeństwo”. Jego definicje są bardzo zróżnicowane, subiektywne i często zawierają niewiele treści. Brak powszechnie akceptowanej definicji, która obejmowałaby jej wielowymiarowość, jest niejako blokowany przez koncentrację na aspektach technologicznych z jednoczesnym pomijaniem aspektów z innych obszarów. Dla szerszego ujęcia zaproponowana została następująca definicja: cyberbezpieczeństwo stanowi organizowanie i zbieranie zasobów, procesów i struktur wykorzystywanych do ochrony cyberprzestrzeni i powiązanych systemów dla ochrony przed zdarzeniami naruszającymi prawa własności (Craigen, Diakun-Thibault, Purse 2014, s. 13). Wydaje się, że ta kanadyjska definicja również nie może być rozważana jako bardziej uniwersalna, ponieważ koncentruje się na naruszeniu praw własności, a konieczna jest ochrona dóbr z dużo szerszego ich katalogu.

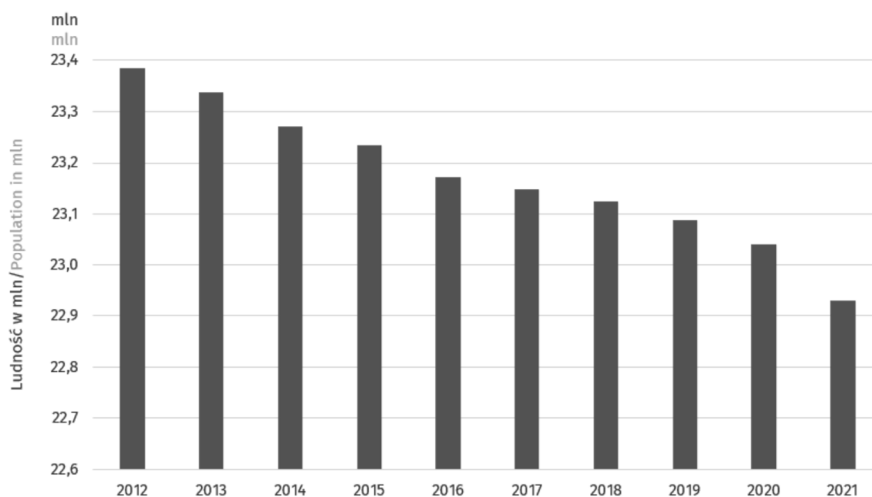
W definicji bezpieczeństwa cyfrowego OECD, która jest umieszczona pod tytułem: *Why “digital security” instead of “cybersecurity”?* (*Dlaczego bezpieczeństwo cyfrowe zamiast cyberbezpieczeństwa?*), akcent kładzie się na wątek, że bezpieczeństwo cyfrowe odnosi się do gospodarczych i społecznych aspektów cyberbezpieczeństwa, w przeciwieństwie do czysto technicznych aspektów i tych odnoszących się do przestrzegania prawa karnego oraz aspektów bezpieczeństwa narodowego i międzynarodowego. Ponadto w nawiązaniu do tej definicji wskazuje się, że termin „cyfrowy” jest zgodny z wyrażeniami takimi jak „gospodarka cyfrowa” (ang. *digital economy*), „transformacja cyfrowa” (ang. *digital transformation*) czy też „technologie cyfrowe” (ang. *digital technologies*). Powyższe tworzy podstawę do

konstruktywnego międzynarodowego dialogu pomiędzy interesariuszami wykazującymi wolę wzmocnienia zaufania i zmaksymalizowania szans wynikających z technologii informacyjno-komunikacyjnych (OECD 2021).

Bardziej przedmiotowa definicja bezpieczeństwa cyfrowego o charakterze pojęcia kolektywnego obejmuje zasoby zaangażowane do ochrony: tożsamości osób w Internecie, danych dotyczących tych osób i ich aktywów dostępnych przez Internet. Narzędzia służące tej ochronie zawierają: usługi web, oprogramowanie antywirusowe, karty SIM do smartfonów i zabezpieczone urządzenia osobiste. Różnica pomiędzy bezpieczeństwem cyfrowym a cyberbezpieczeństwem polega na tym, że to pierwsze dotyczy ochrony dóbr osób w Internecie (dane, tożsamość i aktywa), natomiast to drugie dotyczy ochrony całych sieci, systemów komputerowych. Można uznać, że bezpieczeństwo cyfrowe jest podtypem cyberbezpieczeństwa (choć wielu praktyków używa tych pojęć zamiennie) – bezpieczeństwo cyfrowe chroni zatem informacje, a cyberbezpieczeństwo chroni infrastrukturę, całe sieci, systemy oraz informacje (Simplilearn 2021).

Smart City a bezpieczeństwo cyfrowe

Mimo że miasta pokrywają zaledwie 3% powierzchni ziemi, to jednak są głównym motorem rozwoju gospodarczego, konsumując przy tym 75% energii wytwarzanej na planecie. Ludność miast na świecie dynamicznie rośnie. W Polsce nie obserwuje się tego ogólnoswiatowego trendu. Liczba ludności w miastach z roku na rok maleje. Tempo spadku nieco osłabło w latach 2016-2019, by niestety przyspieszyć w ostatnim okresie (rys. 7.1).



Rysunek 7.1. Liczba ludności polskich miast ogółem w latach 2012-2021

Źródło: (GUS 2021, s. 15)

Trudno dzisiaj przewidzieć, czy trend ten zmieni się w Polsce. Nie oznacza to jednak, że liczba ludności maleje w każdym polskim mieście. W niektórych miastach liczba ludności rośnie, w innych zaś maleje. Różne jest także tempo tych zmian. Niezależnie od powyższych danych i trendów występuje konieczność transformacji sposobów, w jaki miasta są zarządzane, oraz transformacji kwalifikacji, jakie posiadają pracownicy zatrudnieni w jednostkach miejskich. Dzisiaj w dużej mierze zarządzanie miastami skupione jest na elementach fizycznych, takich jak drogi, kanalizacja, przestrzenie zielone, budownictwo, transport czy gospodarka odpadami. Po raz pierwszy jednak pojawia się możliwość zbierania i procesowania olbrzymiej ilości danych (Wilson 2019, s. 19). Umożliwia to realizację koncepcji Smart City, polegającej na wykorzystaniu nowoczesnych technologii przy akceptacji i partycypacji społecznej dla poprawy warunków życia mieszkańców miasta. Niektóre miasta próbują stworzyć w pierwszym rzędzie popyt na technologie Smart City, by następnie wdrażać samą koncepcję, inne zaś tworzą strategie oraz projekty i realizują koncepcję Smart City. Niezależnie od sposobu realizacji tej koncepcji jednym z głównych czynników akceptacji mieszkańców dla wdrażania koncepcji Smart City i chęci używania technologii Smart City jest kwestia bezpieczeństwa cyfrowego i zabezpieczenia prywatności (Habib, Alsmadi, Prybutok 2020, s. 610). Bezpieczeństwo przechowywania danych cyfrowych w budowaniu, przebudowywaniu lub zakupie systemów cyfrowych staje się ważne dla polskich gmin, także tych, które w zakresie cyfrowym współdziałają ze sobą, jak w przypadku konsorcjum gmin dla realizacji projektu „Gmina bliżej mieszkańców”, dotyczącego budowy innowacyjnej platformy e-usług publicznych dla mieszkańców kilku gmin: Moszczenicy, Ujazdu i Będkowa (Komorowski 2020, s. 45-46).

Technologie związane ze Smart Cities są promowane jako środek do efektywniejszego dostarczania usług, lecz paradoksalnie przy ich wdrażaniu pojawiają się nowe zagrożenia, w tym powodowanie, że usługi i miejska infrastruktura stają się mniej zabezpieczone i bardziej narażone na czyny przestępcze (Kitchin, Dodge 2019, s. 47). Niezależnie od zabezpieczenia technologii, które w Smart City powinno być jak najlepsze, potrzebne jest upowszechnianie wiedzy o zagrożeniach w urzędzie miasta, a także w jednostkach miejskich, np. w szkołach. Wiedza zarówno uczniów, jak i nauczycieli i rodziców na temat zagrożeń cyfrowych jest w dużym stopniu niewystarczająca, dlatego postuluje się wdrożenie procedur zwiększających bezpieczeństwo cyfrowe (Tomczyk, Srokowski 2016, s. 102).

Klasyfikacje zagrożeń cyfrowych w Smart City

Najczęściej stosowany podział bazuje na kryterium lokalizacji: zagrożenie może wystąpić wewnątrz organizacji, do której należy system informatyczny (przykłady tych zagrożeń to: kradzież danych dokonana przez użytkownika systemu, wystąpienie awarii urządzenia, błąd oprogramowania), lub może pochodzić z zewnątrz tej organizacji (przykłady to: wyłączenie sieci energetycznej, włamanie do pomieszczenia biura). Inny podział opiera się na kryterium przypadkowości zagrożenia: zagrożenie może być celowe (np. umyślne skasowanie danych czy też kradzież

komputera) lub przypadkowe (przypadkowe wyłączenie komputera w czasie pracy (Madej 2010, s. 81).

Podział zagrożeń związanych z bezpieczeństwem cyfrowym można zatem podzielić na pochodzące z wewnątrz instytucji (kiedy osoby uprawnione wykorzystują w sposób nieuprawniony zgromadzone w systemie informatycznym dane) lub z zewnątrz instytucji (kiedy osoby nieuprawnione uzyskują dostęp do danych, np. wskutek włamania). Egzemplifikacją tego pierwszego przypadku jest zdarzenie związane z Miejskim Ośrodkiem Pomocy Społecznej w Częstochowie, gdzie miało dojść do kradzieży danych osobowych kilkudziesięciu pracowników MOPS-u celem ich wykorzystania do głosowania w ramach budżetu obywatelskiego (Romanek 2021). Natomiast przykładem drugiej sytuacji jest atak hakerski na urząd miasta w Kołobrzegu, a ściślej na jego serwisy informacyjne, na których hakerzy zamieścili fake news, polegając na informacjach, z których miało wynikać, że ksiądz został zamordowany na Litwie przez imigrantów (Stech 2021). Kolejny przykład, tym razem z innego poziomu samorządu terytorialnego, to zdarzenie z urzędu marszałkowskiego województwa małopolskiego, gdzie w lutym 2021 roku doszło do ataku hakerskiego, skutkiem którego przez około 2 miesiące (od lutego do kwietnia) nie działały systemy informatyczne urzędu (m.in. nie były dostępne dane osobowe, głównie klientów urzędu). Przestępcy zaszyfrowali serwery i żądali milionów okupu w kryptowalutach (Dybała 2021).

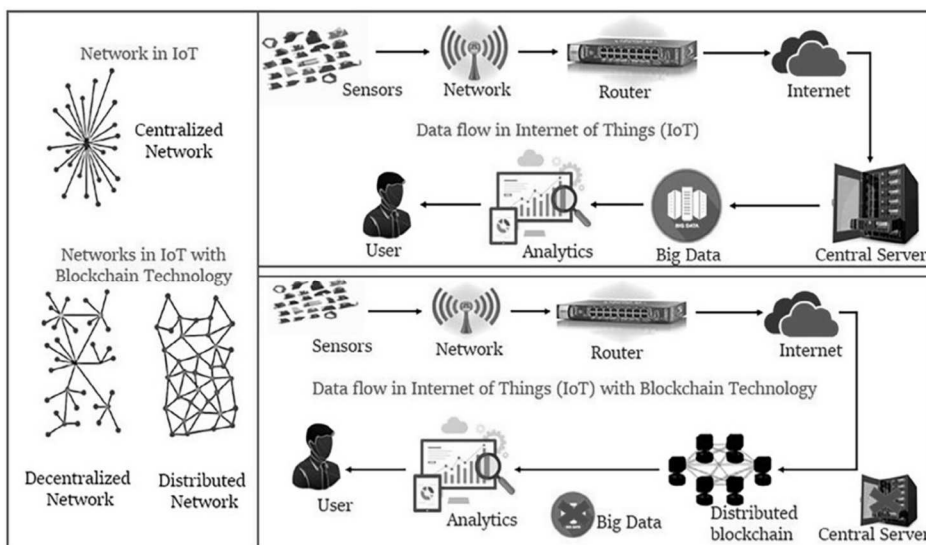
Można mówić nie tylko o rodzajach i grupach rodzajowych zagrożeń cyfrowych, ale także o wymiarach bezpieczeństwa cyfrowego. Różne mogą być wymiary bezpieczeństwa cyfrowego, w tym bezpieczeństwo w kontakcie z innymi użytkownikami sieci czy też bezpieczeństwo wizerunku (Tomczyk, Srokowski 2016, s. 58).

Internet rzeczy jako szczególnie narażony element Smart City

Niezwykle dynamiczny rozwój technologii ICT przejawia się m.in. w rozwoju Internetu rzeczy (IoT), co przyczynia się do tworzenia gigantycznej ilości danych. IoT stanowi ważny element Smart City. Wykorzystanie IoT powoduje zachowanie coraz większej ilości cyfrowych śladów działalności i życia ludzi we wszystkich kontekstach, co tworzy niespotykaną do tej pory skalę możliwych potencjalnych ryzyk dla bezpieczeństwa i praw obywateli. Wspomniane cyfrowe ślady i różnego rodzaju dane są bardzo użyteczne w zwalczaniu przestępczości, jednocześnie jednak zbieranie takich danych i ich procesowanie i archiwizowanie zderza się z potrzebą prywatności i autonomii osobistej (Losavio i in. 2018, s. 1). Konsekwencje istnienia tej olbrzymiej nowej przestrzeni danych mogą być znaczące nie tylko dla kwestii bezpieczeństwa osób, ale także prywatności, praw jednostki oraz osobistej autonomii (Losavio i in. 2018, s. 9).

Poszukuje się nowych sposobów zwiększania bezpieczeństwa źródłowych danych IoT w aplikacjach Smart City. W aplikacjach tych w zakresie danych replikowanych oraz niereplikowanych dotyka się kwestii chmury, sieci bazowych, ramy IoT i sieci rozproszonych czujników. Źródła niereplikowanych danych (ang. *non-replicated resources*) są zarządzane z użyciem natychmiastowo odwołalnych środków bezpieczeństwa, by chronić przed niepotrzebnymi zagrożeniami śledzenia,

grożącymi pierwotnemu dostarczycielowi źródłowych danych (Al-Solami 2021, s. 2). Potrzebę bezpieczeństwa przy IoT określa się czasem jako najważniejszy aspekt jego funkcjonowania. W tym zakresie wskazuje się na istnienie trzech głównych obszarów: Smart City, zarządzanie danymi i informacją oraz architektura i ramy. W zapewnieniu bezpieczeństwa IoT pomocne może być odpowiednie wykorzystanie łańcucha bloków (ang. *blockchain*), dzięki któremu można w sieci IoT pominąć centralny serwer oraz big data. Urządzenia IoT są łatwo dostępne, a *blockchain* może pomóc w certyfikowaniu dostępu do informacji zgromadzonych na urządzeniach (Ye, Cao, Chen 2021, s. 1).



Rysunek 7.2. Typy sieci w Internecie rzeczy

Źródło: (Kumar, Mallick 2018, za: Ye, Cao, Chen 2021, s. 6)

W ramach Smart City pojawia się także kwestia integracji pomiędzy IoT i technologiami związanymi z mediami społecznościowymi. W tym zakresie obserwowane są duże możliwości, a jednocześnie również i tutaj zwraca się uwagę na problem bezpieczeństwa informacji i prywatności (Mendhurwar, Mishra 2021, s. 565).

System zarządzania bezpieczeństwem cyfrowym w Smart City

Polityka bezpieczeństwa to system zarządzania nie tylko systemami informatycznymi, ale także organizacją i postępowaniem pracowników. To zapewnianie bezpieczeństwa informacji poprzez jasne zakomunikowanie i przedstawienie pracownikom obowiązujących zasad i reguł (Beskosty 2017). Zjawisko zagrożeń dla bezpieczeństwa cyfrowego jest w dużym stopniu ignorowane i niedoceniane przez zarządzających miastami. Podejście do rozwiązywania tego problemu powinno być dużo bardziej systemowe, polegające na (Kitchin, Dodge 2019, s. 47):

- szerszym projektowaniu bezpieczeństwa (ang. *security-by-design*);
- tworzeniu zespołów bezpieczeństwa cyfrowego;
- tworzeniu zespołów ratownictwa cyfrowego;
- zmian w procedurach zamówień publicznych;
- ciągłego rozwoju zawodowego.

Także w MŚP w Polsce postuluje się systemowe podejście menedżerów do cyberbezpieczeństwa, co wiąże się z planowaniem ich rozwoju i od strony formalnej z wypełnieniem wymogów prawnych ochrony danych osobowych (Matuska 2018, s. 75). Z punktu widzenia wdrażania koncepcji Smart City postuluje się zapewnienie bezpieczeństwa cyfrowego miasta poprzez:

- tworzenie strategii miejskiego bezpieczeństwa cyfrowego;
- tworzenie programów operacyjnych bezpieczeństwa cyfrowego w różnych jego aspektach;
- stworzenie miejskiego zespołu bezpieczeństwa cyfrowego;
- stworzenie miejskiego zespołu ratownictwa cyfrowego;
- stworzenie regulaminu bezpieczeństwa cyfrowego dla pracowników urzędu miasta oraz wszystkich jednostek i podmiotów miejskich;
- realizowanie szkoleń pracowników w zakresie stosowania regulaminu bezpieczeństwa cyfrowego;
- stworzenie i stosowanie podręcznika zamówień publicznych związanych z bezpieczeństwem cyfrowym, który będzie brany pod uwagę zarówno w toku procedury zamówień publicznych, jak i przy ich realizacji.

Podsumowanie

Bezpieczeństwo cyfrowe dotyczy ochrony tożsamości osób w Internecie, danych związanych z tymi osobami oraz ich aktywów dostępnych przez Internet. Z kolei narzędzia wykorzystywane do tej ochrony to: usługi web, oprogramowanie antywirusowe, karty SIM do smartfonów i zabezpieczone urządzenia osobiste. Tak rozumiane bezpieczeństwo cyfrowe ściśle wiąże się z koncepcją Smart City, która polega na wykorzystaniu nowoczesnych technologii, w tym ICT, przy akceptacji i przy udziale mieszkańców miasta do podniesienia jakości życia mieszkańców. Jednym z głównych czynników akceptacji mieszkańców dla wdrażania koncepcji Smart City i chęci używania technologii Smart City jest właśnie kwestia bezpieczeństwa cyfrowego i zabezpieczenia prywatności.

Najczęstszym podziałem zagrożeń cyfrowych, który można zastosować także do Smart City, jest podział bazujący na kryterium lokalizacji: zagrożenie może wystąpić wewnątrz urzędu miasta i jednostek miejskich lub pochodzić z zewnątrz tych instytucji. Dynamiczny rozwój technologii ICT przejawia się m.in. w rozwoju Internetu rzeczy (IoT), co przyczynia się do tworzenia gigantycznej ilości danych. IoT stanowi ważny element Smart City. Poszukuje się nowych sposobów zwiększania bezpieczeństwa źródłowych danych IoT w aplikacjach Smart City. Przy wdrażaniu koncepcji Smart City postuluje się zapewnienie bezpieczeństwa cyfrowego miasta poprzez właściwe planowanie na każdym poziomie tego procesu, zmiany

strukturalne, zmiany w zarządzaniu zasobami ludzkimi oraz zmiany w zamówieniach publicznych.

Literatura

1. Al-Solami E. (2021), *Replication-Aware Secure Resource Administration Scheme for Internet of Things – Smart City Applications*, „Transactions on Emerging Telecommunications Technologies”, 32, 3, <https://doi.org/10.1002/ett.4200> (dostęp: 25.09.2021).
2. Beskosty M. (2017), *Zarządzanie bezpieczeństwem informacji*, „Studia nad Bezpieczeństwem”, 2, s. 163-173.
3. Craigen D., Diakun-Thibault N., Purse R. (2014), *Defining Cybersecurity*, „Technology Innovation Management Review”, 4, 10, s. 13-21.
4. Dybała B. (2021), *Atak hakerski na urząd marszałkowski. Śledczy nadal nie wie, kto za tym stoi. Ekspert komentuje*, <https://gazetakrakowska.pl/atak-hakerski-na-urzed-marszalkowski-sledczy-nadal-nie-wiedza-kto-za-nim-stoi-ekspert-komentuje/ar/c1-15675832> (dostęp: 22.09.2021).
5. GUS (2021), *Powierzchnia i ludność w przekroju terytorialnym w 2021 r.*, <https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/powierzchnia-i-ludnosc-w-przekroju-terytorialnym-w-2021-roku,7,18.html> (dostęp: 23.09.2021).
6. Habib A., Alsmadi D., Prybutok V. (2020), *Factors that Determine Residents' Acceptance of Smart City Technologies*, „Behaviour and Information Technology”, 39, 4, s. 1-14.
7. Kitchin R., Dodge M. (2019), *The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention*, „Journal of Urban Technology”, 26, 2, s. 47-65.
8. Kumar N.M., Mallick P.K. (2018), *Blockchain Technology for Security Issues and Challenges in IoT*, „Procedia Computer Science”, 132, s. 1815-1823.
9. Komorowski T.M. (2020), *Modele współpracy samorządowej w zakresie rozwoju i utrzymania infrastruktury informatycznej i cyfrowych usług publicznych*, [w:] Krok E., Swacha J. (2020), *Innowacje i zarządzanie*, s. 39-50, Wydawnictwo SiZ, Łódź.
10. Losavio M.M. i in. (2018), *The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy and Security*, „Security Privacy”, 1, 23, s. 1-11.
11. Madej J. (2010), *Klasyfikacja zagrożeń systemu bezpieczeństwa informatycznego*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie”, 814, s. 77-86.
12. Matuska E. (2018), *Zarządzanie bezpieczeństwem cyfrowym w sektorze małych i średnich przedsiębiorstw – aspekty personalne*, „Studia nad Bezpieczeństwem”, 3, s. 65-76.
13. Mendhurwar S., Mishra R. (2021), *Integration of Social and IoT Technologies: Architectural Framework for Social Transformation and Cyber Security Challenges*, „Enterprise Information Systems”, 15, 4, s. 565-584.
14. Mosiądz M., Sobiech J., Wójcik J. (2019), *Bezpieczeństwo cyfrowe a rzetelność pomiaru*, „Metrologia i Probiernictwo. Biuletyn Głównego Urzędu Miar”, 22, 1, s. 38-47.
15. OECD (2021), *Digital security*, <https://www.oecd.org/sti/ieconomy/digital-security> (dostęp: 25.09.2021).
16. Romanek B. (2021), *Kradzież danych osobowych pracowników częstochowskiego MOPS-u, Radna Monika Pohorecka interweniuje u Prezydenta, MOPS wydaje oświadczenie*, <https://czestochowa.naszemiasto.pl/kradziez-danych-osobowych-pracownikow-czestochowskiego-mops/ar/c1-8150221> (dostęp: 22.09.2021).
17. Schneier B. (2015), *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, Indianapolis.
18. Simplilearn (2021), *What is Digital Security: Overview, Types, and Applications Explained*, https://www.simplilearn.com/what-is-digital-security-article#what_is_digital_security (dostęp: 25.09.2021).

19. Stech B. (2021), *Atak hakerów na strony urzędu miasta w Kolobrzegu i serwisy informacyjne. Fake news o morderstwie księdza*, <https://koszalin.wyborcza.pl/koszalin/7,179397,27465486,atak-hakerow-na-strone-urzedu-miasta-w-kolobrzegu-zamiescili.html> (dostęp: 22.09.2021).
20. Tomczyk Ł., Srokowski Ł. (2016), *Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole. Raport z badań*, https://depot.ceon.pl/bitstream/handle/123456789/13949/Tomczyk_Srokowski_Kompetencje_w_zakresie_bezpiecze%C5%84stwa_cyfrowego%20.pdf?sequence=1&isAllowed=y (dostęp: 23.09.2021).
21. Wilson P. (2019), *State of Smart Cities in UK and beyond* IET Smart Cities, „IET Journals – The Institution of Engineering and Technology”, 1, 1, s. 19-22.
22. Ye C., Cao W., Chen S. (2021), *Security Challenges of Blockchain in Internet of Things: Systematic Literature Review*, „Transactions on Emerging Telecommunications Technologies”, 32, 8, <https://doi.org/10.1002/ett.4177> (dostęp: 22.09.2021).

DIGITAL SECURITY MANAGEMENT IN SMART CITY

Abstract: Goal of the chapter is systematization of aspects related to digital security in Smart City and giving recommendations for cities in the field. The author in course of overview of literature divided the issue into the following elements: digital security and similar notions, Smart City and digital security, classification of digital threats to Smart City, Internet of Things as an element of Smart City specially exposed to threats and system of digital security management. In relation to the last element the author formulated recommendations for cities aspiring to being viewed as Smart Cities.

Keywords: city management, digital security, Smart City

Rozdział 8

NOWOCZESNE TECHNOLOGIE WSPOMAGAJĄCE ANALIZĘ ZAGROŻEŃ SYSTEMU PRZETWARZAJĄCEGO INFORMACJE NIEJAWNE

Ewelina Włodarczyk⁸, Aurelia Rybak⁹

Streszczenie: Ze względu na postęp technologiczny większość informacji przechowywanych jest obecnie w systemach informatycznych. Stąd częściej kładzie się nacisk na ochronę systemów informacyjnych i bezpiecznego przetwarzania zawartych w nich danych. Tym bardziej jest to istotne w sytuacji, gdy w systemie informatycznym przechowywane są informacje niejawne, w przypadku których organizację ochrony regulują przepisy prawne. Każde przedsiębiorstwo, które ma do czynienia z informacjami niejawnymi, jest m.in. zobowiązane do wyznaczenia poziomu zagrożeń w aspekcie utraty poufności, integralności oraz dostępności tych informacji. W tym celu można skorzystać z nowoczesnych technologii. Celem rozdziału jest pokazanie, jak ważne, a zarazem skompilowane jest zapewnienie ochrony informacji niejawnych, a także zaprezentowanie programu komputerowego, który umożliwia przeprowadzenie analizy zagrożeń metodą zgodną z zaleceniami Departamentu Bezpieczeństwa Teleinformatycznego ABW.

Słowa kluczowe: analiza zagrożeń, bezpieczeństwo informacji, informacje niejawne, program komputerowy

Wprowadzenie

Informacja zawsze miała ogromne znaczenie dla wielu dziedzin życia, natomiast postęp techniczny spowodował większe zainteresowanie informacją, a przede wszystkim sposobami i możliwościami jej przetwarzania. Stąd obecnie informacja to nie tylko dobro współczesnej cywilizacji, ale również i towar, który może być bardzo kosztowny w nabyciu. W literaturze dotyczącej zarządzania przedsiębiorstwem informację definiuje się jako odzwierciedlenie rzeczywistości wywołujące zmianę zachowania u odbiorcy lub jako fragment wiedzy o dziedzinie lub przedmiocie, którą przekazuje się innym ludziom (por. Jakubowska 2008, s. 95-105). Instytucje państwowe przetwarzają dodatkowo różnego rodzaju informacje, które mają ogromny wpływ na bezpieczeństwo narodowe – informacje niejawne.

⁸ Politechnika Śląska, Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

⁹ Politechnika Śląska, Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

Informacje te nie dotyczą tylko sfery militarnej i politycznej, ale również ekonomicznej, która zyskuje coraz większy wpływ zarówno na bieżące bezpieczeństwo kraju, jak i suwerenność państwa (por. Dela 2015, s. 22-50).

Podstawowym aktem prawnym dotyczącym ochrony informacji niejawnych jest Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Tym dokumentem zmieniono system ochrony informacji niejawnych, by dostosować krajowe akty normatywne do standardów NATO i Unii Europejskiej (por. Leciak 2011, s. 192). W ustawie określono zasady tej ochrony oraz zakres przedmiotowy oznaczany czterema rodzajami klauzul. Informacjom niejawnym powinna być nadawana klauzula tajności, stosownie do zagrożeń, które spowodowałyby jej nieuprawnione ujawnienie. Klauzulę tajności nadaje osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału (por. Szałowski 2013, s. 110). Ustawa precyzuje również okres ochrony przewidziany dla każdego rodzaju klauzul, sposób organizacji ochrony informacji niejawnych, kto, po spełnieniu jakich warunków i na jakich zasadach może mieć dostęp do informacji niejawnych, kancelarie tajne, środki bezpieczeństwa fizycznego, bezpieczeństwo teleinformatyczne oraz bezpieczeństwo przemysłowe.

Bezpieczeństwo fizyczne, którego podstawy prawne zawarto w rozdziale 7. ustawy, obejmuje kancelarie tajne oraz środki bezpieczeństwa fizycznego. Kancelaria tajna to wyodrębniona komórka organizacyjna w zakresie ochrony informacji niejawnych. Jest ona podległa pełnomocnikowi ochrony, obsługiwana przez pracowników pionu ochrony i odpowiedzialna za właściwe rejestrowanie, przechowywanie, obieg oraz wydawanie materiałów uprawnionym osobom (Ustawa 2010, art. 42.4). Dokładne wymagania dotyczące tworzenia i funkcjonowania kancelarii tajnych zawarto w akcie wykonawczym.

Stosowane środki bezpieczeństwa fizycznego mają za zadanie zabezpieczyć informacje niejawne przed nieuprawnionym dostępem. W szczególności są to następujące przypadki: sabotaż, zamach terrorystyczny, kradzież, zniszczenie, szpiegostwo, dostęp do danych o wyższej klauzuli niż dozwolone, nieuprawnione wejście do pomieszczeń, gdzie przetwarzane są informacje. Zakres stosowania środków bezpieczeństwa fizycznego uzależniono od poziomu zagrożeń. Zatem organizacje mające do czynienia z informacjami niejawnymi są zobowiązane do wyznaczenia poziomu zagrożeń w aspekcie utraty: dostępności, integralności i poufności (Rozporządzenie 2012, § 3.6).

Analiza zagrożeń w tym zakresie jest regulowana przez Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych. Są w tej sprawie odstępstwa od normy, to znaczy niektóre organizacje mogą samodzielnie regulować działalność w tym zakresie, tj. ministerstwa. Kryteria i sposób określania poziomu zagrożeń zawiera Załącznik 1 Rozporządzenia, a Załącznik 2 określa metodykę doboru środków bezpieczeństwa fizycznego. Wyznaczając poziom zagrożeń, należy uwzględnić klauzule tajności, liczbę informacji oraz rodzaje zagrożeń. Natomiast ustalając wymagany poziom zabezpieczenia informacji niejawnych, należy określić liczbę i poziom dostępu osób, które są zatrudnione lub pełnią służbę. Na podstawie wyliczonego poziomu zagrożeń oraz klauzuli tajności informacji niejawnych można

dokonać wyboru właściwych środków ochrony. Wyboru dokonuje się na podstawie tabeli wymagań bezpieczeństwa fizycznego. Należy przy tym pamiętać, że dobór środków ochrony fizycznej musi być oparty na zasadzie proporcjonalności. Oznacza to, iż środki ochrony fizycznej muszą być dobierane każdorazowo do panujących warunków oraz stosowne do wymaganego poziomu bezpieczeństwa, który jest postawiony chronionym materiałom. Stąd, aby uniemożliwić dostęp do informacji niejawnych osobom nieuprawnionym, wydziela się strefy ochronne dla informacji niejawnych o klauzuli „poufne” lub wyżej i stosuje się system kontroli wejść oraz wyjść ze stref ochronnych przez określenie uprawnień do przebywania w nich. Ponadto do ochrony informacji niejawnych powinno się stosować jedynie wyposażenie i urządzenia, które posiadają odpowiednie certyfikaty. W przepisach określono utworzenie trzech stref ochronnych, tj. strefy ochronnej I, strefy ochronnej II, strefy ochronnej III, oraz dodatkowo strefy ochronnej o statusie specjalnym, a także zasady ich organizowania (por. Mikowski 2016, s. 201-204). System środków bezpieczeństwa fizycznego obejmuje swoim zakresem rozwiązania organizacyjne, wyposażenie i urządzenia służące ochronie informacji niejawnych oraz elektroniczne systemy pomocnicze, które wspomagają ochronę tych informacji. Ustawodawca wymienia następujące grupy środków bezpieczeństwa fizycznego: personel bezpieczeństwa, bariery fizyczne, szafy i zamki, systemy kontroli dostępu, systemy sygnalizacji włamania i napadu, systemy dozoru wizyjnego, systemy kontroli osób i przedmiotów (por. Rozporządzenie 2012, § 4.3). Kolejnym elementem związanym z bezpieczeństwem fizycznym ujętym w ustawie, o którym należy wspomnieć, jest bezpieczeństwo systemów i sieci teleinformatycznych. Bezpieczeństwo w tym zakresie polega na akredytacji tych systemów przez służby ochrony państwa. Urządzenia i narzędzia kryptograficzne, które służą do ochrony niejawnych informacji, podlegają badaniom i certyfikacji (por. Mikowski 2016, s. 206). Bezpieczeństwo teleinformatyczne zapewnia się przez ochronę informacji przetwarzanych w systemach teleinformatycznych przed utratą właściwości, które gwarantują bezpieczeństwo. Zatem ochronę fizyczną systemu teleinformatycznego uzyskać można poprzez wprowadzenie spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych danych. Ustawodawca wskazał również, w jaki sposób ten cel osiągnąć, a mianowicie poprzez m.in. zarządzanie ryzykiem w systemie teleinformatycznym, ograniczenie zaufania, wprowadzenie wielopoziomowej ochrony systemu teleinformatycznego, wykonywanie okresowych testów bezpieczeństwa, ograniczanie uprawnień oraz minimalizację funkcjonalności (por. Rozporządzenie 2011, §5). Z kolei w rozporządzeniu w sprawie środków bezpieczeństwa zawarto wytyczne dotyczące zabezpieczeń fizycznych dla systemów teleinformatycznych, w którym są przetwarzane informacje niejawne. Dokładnie określono, w jakich strefach ma odbywać się przetwarzanie informacji teleinformatycznych o poszczególnych klauzulach.

Podsumowując, należy podkreślić, że system środków bezpieczeństwa fizycznego informacji niejawnych jest rozbudowany i zawiera rozwiązania prawne, organizacyjne i techniczne. Zatem w celu uzyskania odpowiedniej ochrony informacji niejawnych należy stosować odpowiednią kombinację dostępnych środków bezpieczeństwa fizycznego.

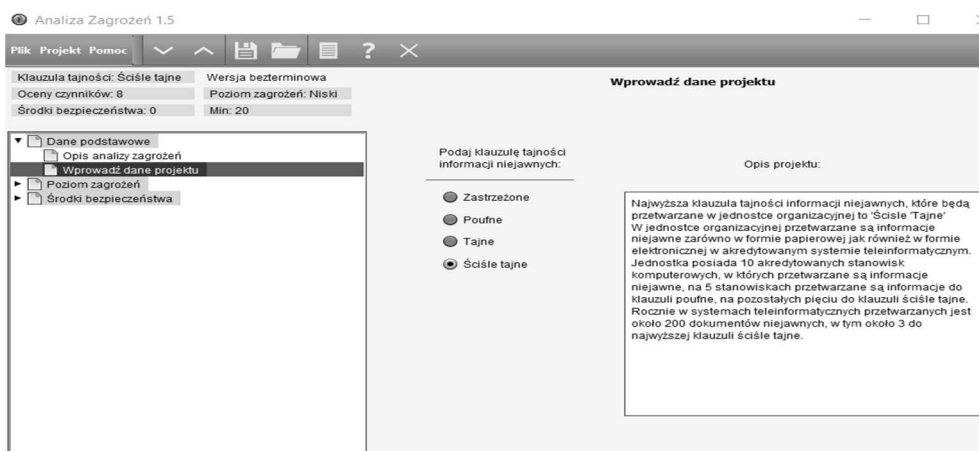
Analiza zagrożeń systemu przetwarzającego informacje niejawne

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego, określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych. Poziom zagrożeń wyznacza się dla pomieszczenia lub obszaru, gdzie przetwarza się informacje niejawne. Ponadto, określając poziom ryzyka, należy ocenić wpływ danego czynnika na bezpieczeństwo informacji niejawnych. Stąd poziom zagrożeń ustala się na podstawie wyboru oceny istotności czynnika. Czynnikiem są: postać informacji niejawnej, istotność klauzuli, liczba osób, liczba materiałów niejawnych, lokalizacja, dostęp osób do budynku oraz inne. Czynniki ocenia się w skali trójstopniowej: bardzo istotny (8 punktów), istotny (4 punkty) oraz mało istotny (1 punkt). Każdy z czynników należy indywidualnie ocenić pod kątem znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych w konkretnej jednostce organizacyjnej, według podanej skali, a wybór należy uzasadnić. Wyjątek stanowi czynnik „klauzula przetwarzanych informacji”, gdzie wskazano, że dla informacji o klauzuli „ściśle tajne” czynnik ten ma „bardzo istotne znaczenie”. W przypadku, gdyby w jednostce organizacyjnej wystąpiły czynniki nieujęte w pierwszych sześciu punktach, wówczas w rubryce „inne” należy je opisać i ocenić. W sytuacji, gdyby wstąpiło więcej czynników w tym zakresie, wybiera się najwyższy uznany stopień oceny.

Poziom zagrożeń trzeba ocenić, zanim rozpocznie się przetwarzanie informacji oraz po każdorazowej zmianie czynników branych pod uwagę podczas analizy zagrożeń. Suma punktów wszystkich czynników stanowi podstawę określenia poziomu zagrożenia. Istnieją trzy poziomy zagrożenia, a mianowicie: niski (do 16 pkt), średni (17 do 32 pkt) i wysoki (pow. 32 pkt) (por. Rozporządzenie 2012, Załącznik 1). Wyznaczenie poziomu zagrożenia jest niezbędne do zastosowania prawidłowych i skutecznych środków bezpieczeństwa. Proces doboru środków bezpieczeństwa fizycznego polega na jest odczytaniu z zawartej w załączniku tabeli „Podstawowe wymagania bezpieczeństwa fizycznego” minimalnej łącznej sumy punktów koniecznych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich kombinacji środków bezpieczeństwa fizycznego oraz minimalnej liczby punktów koniecznych do uzyskania w każdej z grup obejmujących kategorie wymaganych do zastosowania środków bezpieczeństwa fizycznego. Następnie na podstawie uzyskanych informacji należy dokonać wyboru określonych środków bezpieczeństwa fizycznego, ujętych w tabeli „Klasyfikacja środków bezpieczeństwa fizycznego”, w której wymieniono środki bezpieczeństwa oraz ich wagi punktowe możliwe do zastosowania. W przypadku niezastosowania danego środka, wpisuje się wartość 0. Dokonując wyboru, należy pamiętać o uwzględnieniu wymagań określonych zarówno w rozporządzeniu, jak i samej tabeli „Klasyfikacja środków bezpieczeństwa fizycznego”. Środki bezpieczeństwa podzielono na sześć kategorii: szafy, pomieszczenia, budynki, kontrola dostępu, personel bezpieczeństwa, systemy sygnalizacji napadu i włamania oraz granice (por. Rozporządzenie 2012, Załączniki 1 i 2).

Analiza zagrożeń, którą narzuca ustawodawca, jest bardzo pracochłonnym procesem, zatem warto skorzystać z postępu technicznego i wykorzystać do tego celu

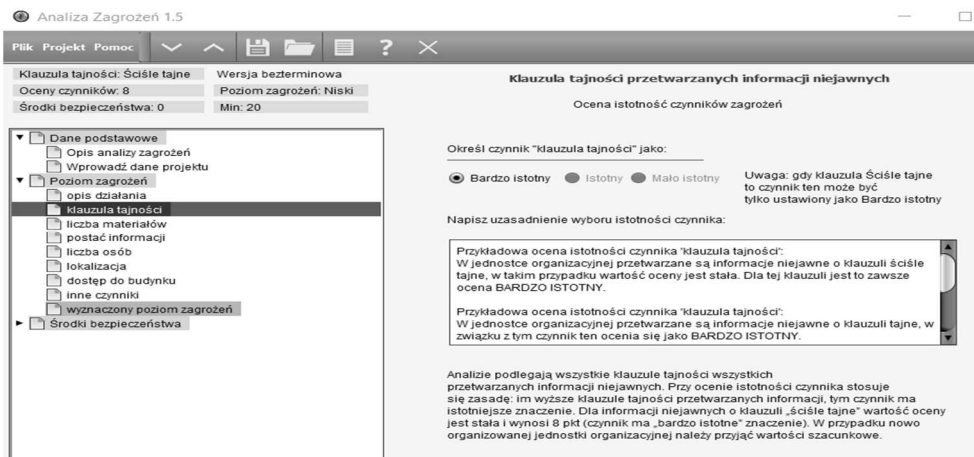
program komputerowy. Aby przedstawić działanie programu Analiza Zagrożeń firmy F-tec, dokonano analizy na przykładowym obiekcie przetwarzającym informacje niejawne. W celu przeprowadzenia analizy zagrożeń dla bezpieczeństwa informacji niejawnych w pierwszej kolejności należy opisać system, w którym przechowywane i przetwarzane są te informacje. W tym miejscu należy również wskazać, jaka jest najwyższa klauzula tajności informacji niejawnych przetwarzanych w jednostce organizacyjnej (rys. 8.1). Następnie należy dokonać wyliczenia poziomu zagrożeń i dobrać odpowiednie środki bezpieczeństwa. Aby ułatwić zachowanie narzuconych zasad analizy, program podzielono na dwie części. W pierwszej dokonuje się właśnie wyliczenia poziomu zagrożeń, w drugiej doboru środków bezpieczeństwa. Ponadto program na każdym etapie działania podpowiada wytyczne zawarte w rozporządzeniu.



Rysunek 8.1. Opis obiektu

Źródło: opracowanie własne

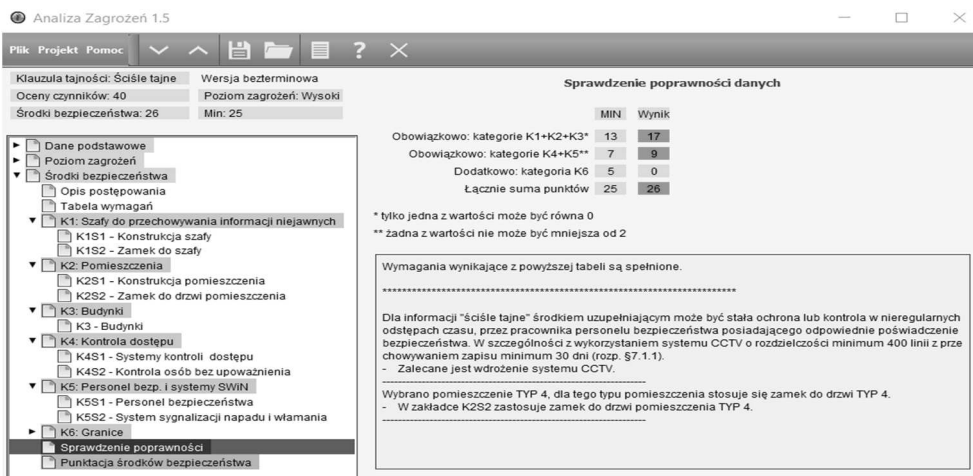
Pierwszym krokiem w części dotyczącej wyliczenia poziomu zagrożeń jest ocena istotności czynnika „klauzula tajności”, w której należy podać, jak istotne są czynniki, w zależności od nadanej klauzuli zgodnie z rozporządzeniem. Program podpowiada, że w przypadku klauzuli „ściśle tajne” czynnik musi być ustawiony jako bardzo istotny. Ponadto podpowiada, jak powinno wyglądać uzasadnienie wybranej istotności (rys. 8.2). Następnie dokonuje się oceny czynnika „liczba materiałów”, „postać informacji”, „liczba osób” i „lokalizacja”. Ostatnimi ocenianymi czynnikami są „dostęp do budynku” i „inne czynniki”. Na każdym etapie w oknie uzasadnienia wyboru program zawiera przykładowe oceny istotności oraz wyjaśnienia dotyczące poszczególnych czynników. Po dokonaniu oceny wszystkich czynników program automatycznie wylicza poziom zagrożeń oraz oblicza minimalne wymagania dla środków bezpieczeństwa. Zaimplementowano również moduł sprawdzania poprawności wprowadzonych danych, który umożliwia zapewnienie zgodności wyboru środków bezpieczeństwa z rozporządzeniem.



Rysunek 8.2. Ocena istotności czynnika klauzula tajności

Źródło: opracowanie własne

W drugiej części program umożliwia, posługując się metodyką zgodną z zawartą w rozporządzeniu, wybór środków bezpieczeństwa fizycznego, które będą spełniać wymagania zawarte w przepisach prawnych. Wymagania dla doboru środków bezpieczeństwa wynikają z wyliczonego poziomu zagrożeń, zatem aby dokonać wyboru środków ochrony, musi być ukończona część I programu. Im wyższy poziom zagrożeń, tym lepsze środki bezpieczeństwa muszą być wdrożone. Ponadto istotna jest także klauzula informacji niejawnych przetwarzanych w organizacji, ponieważ ma ona wpływ na wymagania dla środków bezpieczeństwa. Środki bezpieczeństwa w programie podzielono zgodnie z wytycznymi zawartymi w przepisach prawnych na: szafy do przechowywania informacji niejawnych, pomieszczenia, budynki, kontrolę dostępu, personel bezpieczeństwa i systemy sygnalizacji napadu i włamania oraz granice. Przy każdej grupie środków bezpieczeństwa wymienione są rodzaje zabezpieczeń, zgodne z przepisami prawa, wraz z ich dokładnym opisem i podpowiedziami, co należy wybrać, aby zestaw był prawidłowy. Przykładowo w grupie „szafy do przechowywania informacji niejawnych” są dwie kategorie, a mianowicie: „budowa szafy” i „zamki”. Jest to duże ułatwienie dla użytkownika. Ponadto program wskazuje nie tylko, ile punktów należy zdobyć, ale również jakie są obowiązkowe zabezpieczenia w przypadku danej klauzuli oraz zabezpieczenia dodatkowe. Dodatkowo dla ułatwienia jest okno sprawdzające poprawność wybranych środków, zgodnie z wytycznymi zawartymi w rozporządzeniu (rys. 8.3). Po wprowadzeniu wszystkich danych dotyczących środków ochrony można przejść do ostatniej zakładki. W tej części jest punktacja środków bezpieczeństwa. W zakładce przedstawione są dokonane przez program obliczenia, zgodnie z metodologią zawartą w rozporządzeniu, wybranych środków bezpieczeństwa. Program umożliwia także generowanie raportu, który zawiera wszystkie wprowadzone i wyliczone na tej podstawie elementy.



Rysunek 8.3. Sprawdzenie poprawności danych

Źródło: opracowanie własne

Podsumowanie

Bezpieczeństwo stanowi nieodzowny element życia. Postęp technologiczny, który obecnie ma miejsce, przekłada się również na sferę bezpieczeństwa. W dobie cyfryzacji każdego aspektu życia również elementy związane z zarządzaniem bezpieczeństwem zostają przenoszone do świata wirtualnego. Dzięki temu z jednej strony człowiek jest w stanie szybciej, wygodniej i dokładniej sprawować nadzór nad warunkami zapewniającymi stan bezpieczeństwa, z drugiej zaś niesie to za sobą nowe zagrożenia. W przypadku informacji niejawnych poziom zagrożeń jest związany z bezpieczeństwem fizycznym. Organizacje przetwarzające informacje niejawne są zobligowane do stosowania środków bezpieczeństwa fizycznego. Środki te z kolei muszą być odpowiednie dla poszczególnych poziomów zagrożeń w celu udaremnienia ewentualnych prób nieuprawnionego dostępu do informacji. Ustawodawca narzuca sposób wyznaczenia poziomu zagrożeń oraz rodzaje środków bezpieczeństwa. Taka analiza zagrożeń jest procesem bardzo pracochłonnym, zatem warto skorzystać z postępu technicznego i wykorzystać do tego celu program komputerowy.

Program Analiza Zagrożeń służy do przeprowadzenia takiej analizy zgodnie z wymaganiami prawnymi oraz wyboru środków bezpieczeństwa. Jest bardzo intuicyjny i pozwala na łatwe i bezproblemowe wyliczenie zagrożeń, a następnie, na podstawie przeprowadzonych obliczeń oraz wprowadzonej klauzuli informacji niejawnych, umożliwia wybór właściwych środków bezpieczeństwa fizycznego. Dodatkowo zawiera moduł, który sprawdza poprawność danych, dzięki czemu spełnione zostaną wymagania narzucone przez ustawodawcę. Użytkownik może nie tylko wygenerować raport zawierający wszystkie informacje w każdym kroku, ale również zapisać stan analizy zagrożeń do pliku w celu późniejszego wykorzystania tych danych do kolejnej analizy. Jest to baza danych z gotowymi bibliotekami, która

na każdym etapie pracy zawiera dodatkowo wyjaśnienia dotyczące wymagań prawnych oraz sposobu wypełniania danych. Przedstawiony program jest tylko przykładem gotowego rozwiązania. Oczywiście istnieje również wiele innych produktów tego typu na rynku. Ponadto można także stworzyć samodzielnie taką bazę danych, korzystając ze strukturalnego języka zapytań oraz języka programowania. Podsumowując, należy podkreślić, że podczas analizy zagrożeń systemu przetwarzającego informacje niejawne warto skorzystać z nowych technologii i użyć rozwiązania, które pozwala na automatyzację pracy.

Literatura

1. Dela M. (2015), *Bezpieczeństwo osobowe jako element ochrony informacji niejawnych*, „Woj-skowy Przegląd Prawniczy”, 1, s. 22-50.
2. Jakubowska M. (2008), *Ochrona informacji niejawnych. Wybrane zagadnienia*. „Bezpieczeń-stwo. Teoria i Praktyka”, 3-4, s. 95-105.
3. Leciak M. (2011), *Prawnokarne aspekty nowej ustawy o ochronie informacji niejawnej*, „Stu-dia Iuridica Toruniensia”, 9, 2, s. 192-214.
4. Mikowski R. (2016), *Bezpieczeństwo fizyczne informacji niejawnych*, „Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z Nauk Społecznych”, 9, s. 199-214.
5. Szałowski R. (2013), *Ochrona informacji niejawnych a prawo dostępu do informacji publicz-nej*, „Ius Novum”, 7, 1, s. 108-124.
6. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228, ze zm.).
7. Program do Analizy Zagrożeń, <https://f-tec.pl/analiza-zagrozen/> (dostęp: 15.09.2021).
8. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (DZ.U. 2012 poz. 683, ze zm.).
9. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 948, ze zm.).

MODERN TECHNOLOGIES SUPPORTING THE ANALYSIS OF THREATS TO SYSTEMS PROCESSING CLASSIFIED INFORMATION

Abstract: Due to technological progress, most of the information nowadays is stored in information systems. Hence, more emphasis has been put on protection of information systems and safe processing of their data. This is all the more important when classified information is stored in IT systems, in which case organization of the protection is regulated by legal provisions. Each company that deals with classified information is, inter alia, obliged to determine the level of threats in terms of loss of confidentiality, integrity and availability of such information. In order to do it, modern technologies might be used. The chapter shows how important and at the same time compiled it is to ensure the protection of classified information, and also presents a computer program that allows threat analysis to be carried out with the use of a method consistent with the recommendations of ABW (National Security Agency) IT Security Department.

Keywords: classified information, computer program, information security, threat analysis

Rozdział 9

NOWOCZESNE TECHNOLOGIE WSPOMAGAJĄCE ANALIZĘ RYZYKA DLA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Ewelina Włodarczyk¹⁰, Aurelia Rybak¹¹

Streszczenie: Poczucie bezpieczeństwa jest jedną z potrzeb, którą można zaspokoić dzięki dostępnym środkom i technikom. Obecnie wyróżnia się różne kategorie bezpieczeństwa, jedną z nich jest bezpieczeństwo informacyjne obejmujące swym zakresem bezpieczeństwo danych osobowych. Dane osobowe podlegają szczególnej ochronie regulowanej szeregiem przepisów prawnych, których przestrzeganie jest na pewno dużym wyzwaniem dla przetwarzających je organizacji. Tym bardziej, że obecne przepisy narzucają model opierający się na analizie ryzyka związanego z przetwarzaniem danych osobowych. Zatem organizacje, tworząc system ochrony danych osobowych, zmuszone są przeprowadzać taką analizę ryzyka. Do jej przeprowadzenia można wykorzystać nowe technologie wspomagające zarządzanie bezpieczeństwem. Rozdział ma na celu przedstawienie, jak ważne, a zarazem skompilowane jest zapewnienie ochrony danych osobowych, oraz pokazanie programu komputerowego, który wspomaga dokonanie analizy ryzyka związanego z przetwarzaniem tych danych.

Słowa kluczowe: analiza ryzyka, bezpieczeństwo danych osobowych, bezpieczeństwo informacji, program komputerowy

Wprowadzenie

Intensywny rozwój w obszarze nowych technologii oraz informatyki, w szczególności w zakresie technologii mobilnych i teleinformatyki, istotnie oddziałuje na każdą sferę życia ludzkiego. Gwałtowna ewolucja elektroniki i sieci teleinformatycznych oraz powszechność urządzeń elektronicznych pozwalających na korzystanie z Internetu bez wątpienia ułatwiają pozyskiwanie informacji, która jest współcześnie jednym z najważniejszych strategicznych zasobów zarówno państw, jak i organizacji (por. Polończyk 2017, s. 79-94). Stąd nieustanny wzrost wartości i znaczenia informacji, która jako jeden z elementów wpływających na przewagę, wiedzę, władzę, ale również decydujących o bezpieczeństwie obywateli, organizacji, a nawet całych państw, powoduje wzrost zagrożeń jej bezpieczeństwa. Zatem

¹⁰ Politechnika Śląska, Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

¹¹ Politechnika Śląska, Wydział Górnictwa, Inżynierii Bezpieczeństwa i Automatyki Przemysłowej

z uwagi na tę zależność (por. Liderman 2012, s. 11-12) coraz częściej kładzie się nacisk na bezpieczeństwo informacji, a także ochronę systemów informacyjnych i bezpiecznego przetwarzania zawartych w nich danych.

Ta problematyka jest o tyle istotna, iż obecnie praktycznie każda płaszczyzna bezpieczeństwa, również w odniesieniu do bezpieczeństwa narodowego, jest coraz bardziej uzależniona od bezpiecznego obiegu danych i niezawodności systemów opartych na ogromnych zasobach informacyjnych (por. Grzebiela 2018, s. 87-101). Zwłaszcza, że wśród przetwarzanych informacji bardzo często znajdują się dane osobowe, których ochrona jest dodatkowo uwarunkowana wieloma przepisami. Zagwarantowanie bezpieczeństwa informacyjnego to ogromnie złożony proces, którego powodzenie uzależnione jest od mnóstwa determinant, wśród których jest m.in. umiejętne zarządzanie bezpieczeństwem informacji, zastosowanie wielu procedur organizacyjnych oraz technicznych, a także poziom świadomości osób uprawnionych do dostępu do danych (por. Janczak, Nowak 2013, s. 7; por. Polończyk 2017, s. 79-94).

Bezpieczeństwo informacyjne i bezpieczeństwo danych osobowych

Patrząc ogólnie na bezpieczeństwo informacyjne, można zauważyć, że obejmuje ono ogół procesów technologicznych, czyli pozyskiwanie, transmisję, obróbkę oraz magazynowanie danych w systemach informacyjnych, i tworzy zespół działań zapewniających bezpieczeństwo środowiska informacyjnego (por. Janczak, Nowak 2013, s. 17). Zatem pojęcie to jest szerokie, dotyczy nie tylko bezpieczeństwa informacji we wszystkich postaciach, lecz również bezpieczeństwa systemów generujących, przetwarzających, magazynujących tę informację, a także środowiska działania tych systemów oraz personelu z nich korzystającego. Na podstawie tej definicji można więc stwierdzić, iż w pojęciu „bezpieczeństwo informacyjne” ujęte jest „bezpieczeństwo informacji”, oznaczające, jak już wcześniej wspomniano, ochronę wszelkiego rodzaju form przepływu, magazynowania i przetwarzania danych zapewniających bezpieczeństwo środowiska informacyjnego (por. Janczak, Nowak 2013, s. 20).

Ze względu na coraz to większy udział nowoczesnych technologii używanych do transmisji, przechowywania oraz przetwarzania danych bezpieczeństwo informacyjne jest narażone na nowe rodzaje zagrożeń, tj. cyberzagrożeń, które wynikają przede wszystkim z działań terrorystycznych (por. Liderman 2012). Z tego powodu coraz częściej pojęcie „bezpieczeństwo informacyjne” analizuje się jako część systemu informatycznego, używając go jako synonimu „bezpieczeństwa sieciowego”, które określa się również jako „bezpieczeństwo w sieci”, „bezpieczeństwo teleinformatyczne”, „bezpieczeństwo komputerowe” czy „bezpieczeństwo telekomunikacyjne”. Jest to oczywiście błąd i nie powinno się bezpieczeństwa informacyjnego odnosić tylko do obszaru cyberprzestrzeni oraz teleinformatyki ani utożsamiać go z bezpieczeństwem teleinformatycznym.

Bezpieczeństwo systemów i sieci teleinformatycznych to działania mające na celu uniemożliwienie nieuprawnionym osobom dostępu do ważnych danych, które można przechwycić emisją radiową i analizą ruchu w sieciach radiowych, albo

poprzez wprowadzenie w błąd osób prowadzących taką analizę. Bezpieczeństwo systemów łączności zawiera „systemy łączności, bezpieczeństwo środków utrudniających oraz środków mających na celu fizyczną ochronę systemów łączności, materiałów niejawnych i informacji związanych z systemami łączności” (Herman 2002, s. 170).

Bezpieczeństwo teleinformatyczne dotyczy zatem pozyskiwania, gromadzenia i przetwarzania danych w formie elektronicznej przez sieci i systemy teleinformatyczne. Nie obejmuje ono danych występujących w innych formach niż cyfrowa, więc podobnie jak „bezpieczeństwo informacji” jest węższym pojęciem od „bezpieczeństwa informacyjnego” (por. Ura, Pieprzny 2015).

Rozważając z kolei temat problematyki zagrożeń bezpieczeństwa informacyjnego, można stwierdzić, że lista zagrożeń jest bardzo obszerna i bez wątpienia cały czas będzie ulegała rozszerzeniu o kolejne zagrożenia, zwłaszcza wynikające z postępu technologicznego. Dlatego niezmiernie ważne jest ciągle monitorowanie zagrożeń. Jest to szczególnie istotne w sytuacji, gdy w organizacjach coraz chętniej wykorzystuje się nowe technologie. Stąd identyfikacja zagrożeń w przypadku korzystania z nowego programu lub narzędzia informatycznego będącego w początkowej fazie użytkowania pozwoli na ich modyfikację i usprawnienie.

Jak wiadomo, w obecnych organizacjach jednym z najważniejszych zagrożeń bezpieczeństwa informacyjnego jest potencjalny niekontrolowany dostęp i ujawnienie informacji, która stanowi tajemnicę przedsiębiorstwa. Warto w tym miejscu wspomnieć o ochronie danych osobowych, które również podlegają szczególnej ochronie, regulowanej szeregiem przepisów prawnych. Tym bardziej, że 25 maja 2018 roku wprowadzono w życie Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (tzw. RODO), które zwraca szczególną uwagę na bezpieczeństwo indywidulane człowieka z uwagi na przetwarzanie jego danych osobowych (Rysz 2020, s. 205-220).

RODO definiuje pojęcie „danych osobowych” oraz wprowadza nakaz zastosowania odpowiednich środków technicznych i organizacyjnych w ich przetwarzaniu, żeby zapewnić bezpieczeństwo przy równoczesnym uwzględnieniu istniejącego ryzyka straty tych informacji lub ich nieuprawnionego przetwarzania. Rozporządzenie RODO zastąpiło w Polsce Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, która była pierwszym aktem prawnym regulującym zasady przetwarzania i ochrony danych osobowych (Odlanicka-Poczobutt, Szyszka-Schuppik 2018, s. 419-432). Ponadto wprowadzenie w życie RODO spowodowało, że przepisy prawne w Polsce musiały zapewnić skuteczne stosowanie przepisów rozporządzenia, nie dublując przy tym jego rozwiązań oraz nie będąc z nim sprzecznymi. Stąd w ramach zmian dostosowujących do RODO uchwalono nowe przepisy oraz dokonano nowelizacji wielu aktów prawnych. Przede wszystkim uchwalono Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tzw. UODO) oraz wprowadzono zmiany w przepisach sektorowych.

Podsumowując, należy dodatkowo pamiętać, że równie ważne są przepisy sektorowe, które regulują przetwarzanie danych w konkretnych branżach. Ponadto akty prawne ulegają nieustannym zmianom, stąd spełnienie tych wszystkich przepisów

jest niewątpliwie dużym wyzwaniem dla wszystkich organizacji, które przetwarzają dane osobowe. Zapewnienie bezpieczeństwa danych osobowych zgodnie z obowiązującymi przepisami jest dodatkowo skomplikowane faktem, iż obecnie praktycznie wszystkie organizacje korzystają z nowoczesnych rozwiązań branży IT, ponieważ przetwarzanie, dostęp do danych, a także szybki i bezpieczny transfer są ich kluczowymi potrzebami. Ogromna część przedsiębiorstw, oferując swoje produkty czy usługi, korzysta z różnego rodzaju rozwiązań IT, by móc je sprzedawać drogą elektroniczną. Z kolei organizacje, które nie prowadzą sklepu internetowego, do zarządzania przedsiębiorstwem korzystają na przykład z systemów ERP, baz danych czy chmur. Obecne przepisy prawne, które regulują w Polsce bezpieczeństwo w cyberprzestrzeni, są jeszcze słabo rozwinięte, a przecież cyberprzestrzeń ma transgraniczny charakter i zapewnienie bezpieczeństwa w tym obszarze jest niezmiernie trudne. Tym bardziej, że w obecnym świecie w cyberprzestrzeni dane osobowe przetwarzane są na ogromną skalę (Stępień 2018, s. 49-59).

Podsumowując, należy podkreślić, że wszystkie organizacje stoją przed wyzwaniem, jakim jest zapewnienie tajności, spójności i niezawodności czynności dotyczących gromadzenia, przetwarzania i udostępniania posiadanych danych tylko osobom do tego uprawnionym. Zwłaszcza, że we współczesnym skomputeryzowanym świecie dodatkowo katalog zagrożeń należy poszerzyć o te wynikające ze stosowania systemów komputerowych (Żebrowski, Kwiatkowski 2000, s. 70). Mając wiedzę o tym, że istnieje bardzo dużo różnego rodzaju zagrożeń dla bezpieczeństwa informacyjnego, powinno się w pierwszej kolejności dokonać ich identyfikacji, oszacować ryzyko, czyli dokonać jego analizy i oceny, wprowadzić odpowiednie procedury ochrony danych na podstawie macierzy ryzyka oraz na bieżąco kontrolować skuteczność wprowadzonych rozwiązań.

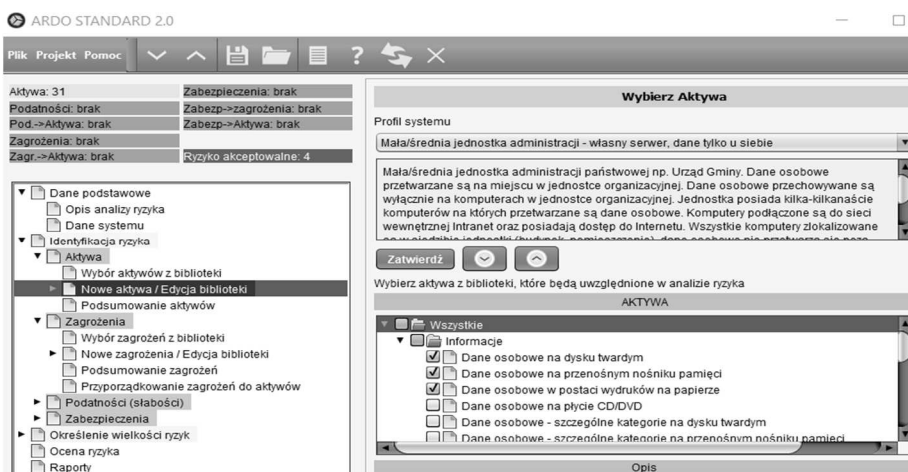
Analiza ryzyka dla bezpieczeństwa danych osobowych

Jednym z obszarów coraz bardziej znaczących w zarządzaniu przedsiębiorstwem jest zarządzanie bezpieczeństwem, które swoim zakresem obejmuje wiele elementów, w tym bezpieczeństwo informacji. W obszarze bezpieczeństwa wykorzystuje się nowe technologie wspomagające jego zarządzanie, takie jak na przykład bazy danych, systemy GIS czy zintegrowane systemy zarządzania (Wyganowska, Tobór-Osadnik 2020, s. 148-159). Dotyczy to oczywiście także bezpieczeństwa informacyjnego, gdyż istnieje wiele gotowych rozwiązań służących do wspomagania zarządzania bezpieczeństwem informacyjnym w różnych jego aspektach. Zatem w przypadku zarządzania bezpieczeństwem danych osobowych również można skorzystać z gotowych programów komputerowych.

Odnosząc się do bezpieczeństwa danych osobowych, warto przypomnieć, że RODO zmieniło budowany przez organizacje model systemu ochrony danych osobowych oparty na wymaganej prawem dokumentacji na model opierający się na analizie ryzyka związanego z przetwarzaniem tych danych. Stąd obecnie organizacje, tworząc system ochrony danych osobowych, przeprowadzają szczegółową analizę ryzyka związanego z przetwarzaniem tych informacji i na jej podstawie dobierają odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo danych (Odlanicka-Poczobutt, Szyszka-Schuppik 2018, s. 419-432). Do tego celu

można wykorzystać na przykład program do analizy ryzyka danych osobowych ARDO firmy F-tec. Program ten umożliwia właśnie przeprowadzanie analizy ryzyka. Ryzyko naruszenia bezpieczeństwa wyliczane jest jako kombinacja prawdopodobieństwa wystąpienia zagrożenia i skutków jego działania na aktywa. Korzystając z programu, można wygenerować macierz ryzyka, przedstawiającą ryzyka naruszenia bezpieczeństwa aktywów w wyniku działania zagrożeń, oraz raporty. Ponadto w programie zawarto biblioteki aktywów, zagrożeń, podatności i zabezpieczeń, co wpływa na automatyzację pracy.

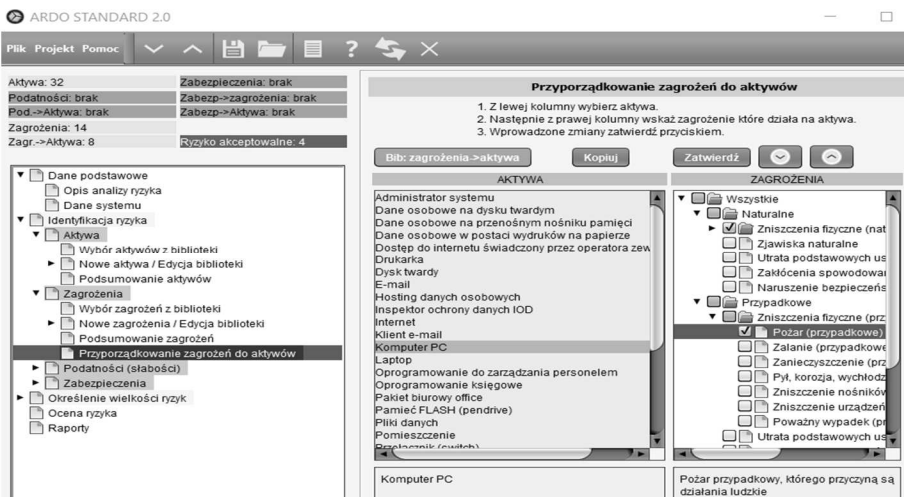
Aplikacja jest łatwa w obsłudze. Składa się z kilku zakładek, w których wypełnia się dane, korzystając do tego celu z gotowych bibliotek lub dokonując samodzielnego wyboru. Wszelkie wybory są widoczne w oknie nawigacji, w którym zmiany zostają wyświetlone na zielono. W pierwszej zakładce „Dane podstawowe” znajduje się opis analizy ryzyka oraz opis analizowanego systemu. Należy w niej podać nazwę jednostki organizacyjnej i opisać w skrócie zasady funkcjonowania organizacji. Kolejną zakładką jest „Identyfikacja ryzyka”, w której są: aktywa, ryzyka, podatności i zabezpieczenia. Poszczególne elementy można wybrać z gotowych bibliotek lub – gdy istnienie taka konieczność – dodać do biblioteki. Zatem w przypadku aktywów można skorzystać z gotowych szablonów dla różnych profili systemu. Wówczas po wyborze konkretnego profilu wyznaczone zostają automatycznie poszczególne aktywa. Oczywiście zawsze istnieje możliwość dokonania zmian, tj. gdyby nie wszystkie wybrane aktywa odpowiadały analizowanemu systemowi, można je odznaczyć lub też dodać brakujące (rys. 9.1)



Rysunek 9.1. Identyfikacja ryzyka

Źródło: opracowanie własne

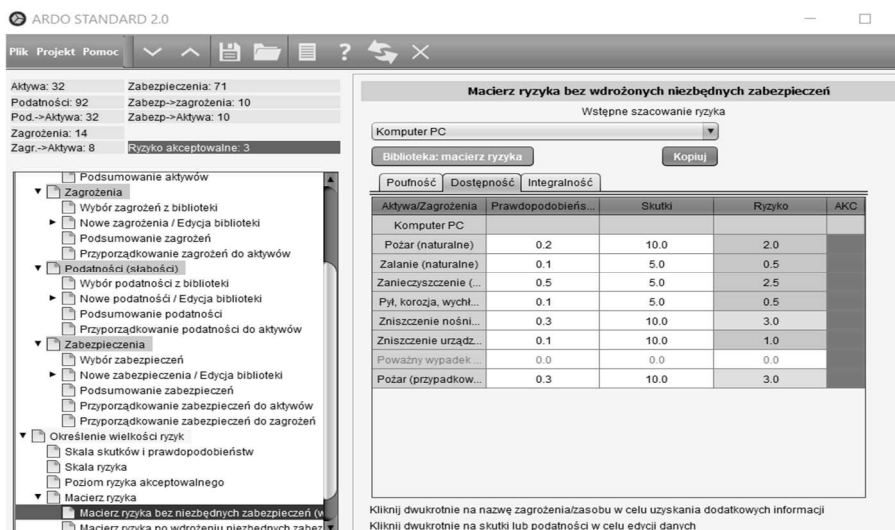
Następnie przyporządkowuje się do wybranych aktywów ryzyka, podatności i zabezpieczenia. W tym kroku również można skorzystać z gotowych bibliotek lub samodzielnie wskazać, które elementy będą przypisane do wybranych aktywów. (rys. 9.2).



Rysunek 9.2. Przypisywanie zagrożeń do aktywów

Źródło: opracowanie własne

Następną zakładką jest „Określenie wielkości ryzyk”, w której po wybraniu poziomu ryzyka akceptowalnego z dostępnej skali można stworzyć macierz wstępnego szacowania ryzyka (bez zabezpieczeń) oraz macierz ryzyka po wdrożeniu niezbędnych zabezpieczeń. Istnieje tu również możliwość wczytania danych z biblioteki, ale zaleca się dokonanie weryfikacji wczytanych danych. Ryzyka podzielone są wg cech informacji na: „Poufność”, „Dostępność” i „Integralność” (rys. 9.3). Przedostatnią zakładką jest „Ocena ryzyka”, również w podziale wg cech informacji. Z kolei ostatnia zakładka to „Generowanie raportów”.



Rysunek 9.3. Macierz ryzyka

Źródło: opracowanie własne

Podsumowanie

Postęp cywilizacyjny, rozwój środków przekazu oraz coraz to większe zasoby informacji wpływają na powstawanie nowych zjawisk, powiększając tym samym katalog bezpieczeństwa o nowe dziedziny. Przekładem tych zmian może być pojęcie „bezpieczeństwo informacyjne”, którego zakres znaczeniowy na przestrzeni lat bardzo się zmienił. Z tego względu obecnie w literaturze przedmiotu wyróżnia się ujęcia skupione na jakimś konkretnym fragmencie, jak np. ochronie informacji niejawnych, bezpieczeństwie teleinformatycznym czy bezpieczeństwie danych osobowych.

Zarządzanie bezpieczeństwem tych ostatnich związane jest z wieloma wytycznymi wynikającymi z przepisów prawnych, w tym RODO, które zmieniło budowany przez organizacje model systemu ochrony danych osobowych – z opartego na wymaganej prawem dokumentacji na model opierający się na analizie ryzyka związanego z przetwarzaniem tych danych. Stąd w dzisiejszych czasach organizacje, tworząc system ochrony danych osobowych, przeprowadzają szczegółową analizę ryzyka związanego z przetwarzaniem tych informacji. Analiza ta ma umożliwić dobór odpowiednich środków technicznych i organizacyjnych, zapewniając bezpieczeństwo danych.

Ze względu na pracochłonność i złożoność dokonywania tych analiz przedsiębiorstwa coraz częściej korzystają z nowoczesnych technologii. Ciekawym rozwiązaniem w tym zakresie jest program do analizy ryzyka danych osobowych ARDO firmy F-tec. Ryzyko naruszenia bezpieczeństwa wyliczane jest w programie jako kombinacja prawdopodobieństwa wystąpienia zagrożenia i skutków jego działania na aktywa. Program jest bardzo intuicyjny i łatwy w obsłudze, więc praktycznie nie wymaga szkolenia w tym zakresie. Dobrze rozbudowane biblioteki i gotowe opcje z przyporządkowanymi zagrożeniami, słabościami i zabezpieczeniami do aktywów ze względu na rodzaj działalności pozwalają na zautomatyzowanie zarządzania bezpieczeństwem w zakresie bezpieczeństwa danych osobowych. Korzystając z aplikacji, można zatem wygenerować macierz ryzyka, przedstawiającą ryzyko naruszenia bezpieczeństwa aktywów w wyniku działania zagrożeń, oraz raporty.

Literatura

1. Grzebiela K. (2018), *Pojęcie i istota bezpieczeństwa informacyjnego*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje”, 30, s. 87-101.
2. Herman M. (2002), *Potęga wywiadu*, Bellona, Warszawa.
3. Janczak J., Nowak A. (2013), *Bezpieczeństwo informacyjne. Wybrane problemy*, Wydawnictwo AON, Warszawa.
4. Koziej S. (2011), *Teoria sztuki wojennej*, Bellona, Warszawa.
5. Krysiński M., Miller P. (2016), *Cloud Computing – szansa i ryzyko dla firmy*, „Ekonomiczne Problemy Usług”, 123, s. 245-254.
6. Liderman K. (2012), *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa.
7. Madej M. (2009), *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] Madej M., Terlikowski M. (red.), *Bezpieczeństwo teleinformatyczne państwa*, s. 17-40, Wydawnictwo PISM, Warszawa.

8. Nowak A., Nowak M. (2011), *Zarys teorii bezpieczeństwa narodowego*, Difin, Warszawa.
9. Nowak A., Scheffs W. (2010), *Zarządzanie bezpieczeństwem informacyjnym*, Wydawnictwo AON, Warszawa.
10. Odlanicka-Poczobutt M., Szyszka-Schuppik A. (2018), *Bezpieczeństwo danych osobowych w świetle nowych przepisów (RODO) – przegląd historyczny*, „Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie”, 118, s. 419-432.
11. Polończyk A. (2017), *Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa*, [w:] Batorowska H., Musiał E. (red.), *Bezpieczeństwo informacyjne w dyskursie naukowym*, s. 79-94, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Kraków.
12. Program do Analizy Ryzyka Danych Osobowych, <https://f-tec.pl/program-do-analizy-ryzyka-danych-osobowych/> (dostęp: 25.06.2021).
13. Rysz S.J. (2020), *Bezpieczeństwo danych osobowych. Część 1 – Specyfika determinant tożsamości człowieka w XXI w.*, „Zeszyty Naukowe SGSP”, 75, 3, s. 205-221.
14. Sienkiewicz P. (2006), *Spółeczeństwo informacyjne jako społeczeństwo ryzyka*, [w:] Haber L.W., Niezgodna M. (red.), *Spółeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcyjne*, s. 400-409, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków.
15. Stępień A. (2018), *Bezpieczeństwo danych osobowych w cyberprzestrzeni – Big Data*, „Przedsiębiorczość i Zarządzanie”, XIX, 2, 3, s. 49-59.
16. *Świat w 2025. Scenariusze Narodowej Rady Wywiadu USA* (2009), Alfa Sagittarius, Kraków.
17. Ura E., Pieprzny S. (2015), *Bezpieczeństwo wewnętrznego państwa*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów.
18. Włodarczyk E., Rybak A. (2020), *Baza danych wspomagająca zarządzanie BHP w wybranym przedsiębiorstwie*, [w:] Wyganowska M., Tobór-Osadnik K. (red.), *Studium wybranych czynników efektywnego i bezpiecznego funkcjonowania przedsiębiorstw górniczych*, s. 148-159, Wydawnictwo Naukowe Śląsk, Katowice.
19. Żebrowski A., Kwiatkowski M. (2000), *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków.

MODERN TECHNOLOGIES SUPPORTING THE RISK ANALYSIS FOR SECURITY OF PERSONAL DATA

Abstract: The sense of security is one of the basic human needs that can be guaranteed thanks to the available resources and technology. Currently, there are various categories of security, among which information security has found its place, including the security of personal data. Personal data are subject to special protection regulated by a number of legal provisions, compliance with which has been undoubtedly a big challenge for all organizations processing such data. All the more so that the current legal regulations impose a model based on the analysis of the risk associated with processing of personal data. Therefore, nowadays organizations creating a personal data protection system are forced to carry out a detailed risk analysis related to the processing of such information. In order to do so, new technologies supporting safety management might be used. The aim of this chapter is to present how important and at the same time compiled is the provision of personal data protection and to show a computer program that supports the necessary risk analysis related to the processing of this information.

Keywords: computer program, information security, personal data security, risk analysis

IV

Bezpieczeństwo w instytucjach i samorządzie terytorialnym

Rozdział 10

ZNACZENIE DOSKONALENIA W PROCESIE ROZWOJU ZAWODOWEGO PRACOWNIKÓW ADMINISTRACJI PUBLICZNEJ I PODNOSZENIA BEZPIECZEŃSTWA KRAJU

Łukasz Skiba¹²

Streszczenie: Współcześnie, ze względu na postrzeganie człowieka jako najcenniejszego kapitału organizacji, rośnie zainteresowanie wiedzą dotyczącą tego, jak prawidłowo zarządzać pracownikiem. Spośród licznych elementów mających związek z zarządzaniem personelem jednymi z ciekawszych (a zarazem zasadniczych dla omawianego zagadnienia), powiązanych zarówno z inwestycją w pracownika, jak i instytucję, są szkolenia urządzane wewnątrz lub na zewnątrz jednostki organizacyjnej. Czas pandemii COVID-19 wyraźnie pokazał, jak potrzebne są szkolenia mające bezpośredni wpływ na bezpieczeństwo zarówno zdrowotne, jak i cybernetyczne, militarne itp. Celem rozdziału będzie zbadanie nastawienia i chęci uczestnictwa w szkoleniach wytypowanych do badań pracowników urzędu gminy.

Słowa kluczowe: administracja publiczna, bezpieczeństwo, doskonalenie, rozwój zawodowy

Wprowadzenie

Począwszy od przejścia naszego kraju na gospodarkę wolnorynkową (w latach 90. XX wieku) następuje coraz większe zainteresowanie problemami zarządzania organizacjami. Zakres zagadnień, z jakimi wiąże się pojęcie „zarządzanie”, jest bardzo szeroki – od aspektów materialnych, finansowych, prawnych itp. po te związane z pracownikami. W miarę wzrastania konkurencji na wolnym rynku zaczęto coraz bardziej doceniać zasoby ludzkie jako podstawę przewagi konkurencyjnej lub wzrostu jakości świadczonych usług przez instytucje publiczne.

Do około 2015 roku dominował model zarządzania personelem, gdyż w warunkach kryzysu gospodarczego ugruntował się tzw. rynek pracy pracodawcy. Wysoki poziom bezrobocia sprzyjał praktykom wykorzystywania pracowników, łamania ich praw oraz pojawianiu się szeregu patologii (np. pracy „na okrągło”, pracy „na czarno”, nieterminowej wypłaty wynagrodzenia za pracę czy mobbingu) (Król,

¹² Politechnika Częstochowska, Wydział Zarządzania

Ludwicyński 2007, s. 58-59). W obecnym czasie deficytu „rąk do pracy” kształtuje się rynek pracy pracownika (tzw. model zarządzania zasobami ludzkimi). To pracodawca stara się zachęcić, „przyciągnąć” potencjalnego pracownika. W tym celu wykorzystuje on takie narzędzia jak np. praca w dogodnym dla pracownika czasie i miejscu, systemy premiowe i nagrody, bony zakupowe, kafeteryjne systemy wynagrodzeń, opieka medyczna, programy emerytalne, a także służbowe telefony, laptopy, samochody, karty kredytowe, mieszkania itp. Pracodawcom zależy przede wszystkim na posiadaniu w zespole pracowniczym osób o odpowiednich kwalifikacjach i umiejętnościach, dlatego też coraz chętniej oferują swoim pracownikom możliwość doksztalcania i szkoleń.

Sytuacja kryzysowa, jaką jest czas pandemii, jasno ukazała potrzebę i wagę szkoleń zarówno w kontekście organizacji w wąskim znaczeniu (firma, przedsiębiorstwo, instytucja), jak i tym szerszym (państwo, UE, Europa, świat). To one pozwalają w sposób elastyczny i szybki dostosowywać się organizacjom do zmian i związanych z nimi potrzeb. Mając świeżo w pamięci ostatnie 1,5 roku, można wskazać obszary, które nie mogłyby prawidłowo funkcjonować bez szkoleń, narażając tym samym organizacje i kraj na straty m.in. demograficzne, materialne, polityczne. Główne z tych obszarów to np. służba zdrowia, urzędy, szkolnictwo, straż pożarna, policja, wojsko, obrona terytorialna. Nowe, nieoczekiwane realia kryzysu pandemicznego wymusiły na zarządzających i ekspertach opracowanie szeregu wytycznych, procedur i strategii, które należało wdrożyć, a w tym celu trzeba było przeprowadzić szkolenia.

W wymiarze gospodarczym kryzys dla jednych jest stratą, a dla innych szansą rozwoju: np. zamknięcie galerii handlowych stało się okazją do przejścia sprzedaży przez firmy wysyłkowe i dostawców (spektakularny rozwój firmy Allegro czy InPost oraz spóźniona decyzja o budowie paczkomatów ORLEN). Chcąc wykorzystać swoją szansę, organizacje muszą szybko i efektywnie dostosowywać się do nowych warunków, czemu służą szkolenia. Każdy kryzys (nawet pandemiczny) jest sytuacją przejściową i nienaturalną dla organizacji, lecz oprócz strat i trudności, jakie za sobą niesie, może być też dobrą okazją do zdobycia przydatnych umiejętności, doświadczenia i wiedzy. Te z kolei mogą stać się dobrą trampoliną do rozwoju zawodowego połączonego z awansem. Przełożeni mają okazję, aby obserwować zaangażowanie podwładnych i to, jak sobie radzą.

Mając powyższe na uwadze, należy przyjrzeć się postawom samych pracowników. To od ich stosunku do szkoleń, zaangażowania w zdobywanie nowej wiedzy i umiejętności, a także wiary w to, że ich zapał zostanie dostrzeżony przez zarządzających i odpowiednio doceniony, zależeć będzie powodzenie powziętych przez organizację przedsięwzięć. Dlatego w niniejszym rozdziale zostanie poddany diagnozie ów stosunek pracowników do szkoleń – czy są przeświadczeni, że szkolenia realnie wpływają na ich rozwój (podnoszą wiedzę i kompetencje oraz realnie wpływają na awans zawodowy) i czy dostrzegają racjonalność tego rodzaju szkoleń (czy są faktycznie przydatne w trakcie pracy). Gdyby nastawienie pracowników do szkoleń okazało się negatywne, mogłoby to oznaczać, że bezpieczeństwo publiczne państwa jest zagrożone.

Doskonalenie a rozwój zawodowy

Zasoby ludzkie, tak samo jak zasoby finansowe oraz rzeczowe, potrzebują ciągłego rozwoju po to, by podołać aktualnym, a także przyszłym potrzebom instytucji. Taki rozwój jest bardzo ważny, bo poszerza i prowadzi do polepszenia wiedzy i zdolności do istotnych działań, jakie wykonują pracownicy, a te z kolei wykorzystywane są do osiągnięcia celów organizacji (Jasiński 2007, s. 120). Podstawę takiego doskonalenia tworzą różne formy szkoleń, które z perspektywy organizacji adaptują pracownika do tego, by wywiązał się z obecnych i przyszłych zadań, zaś z perspektywy pracownika – poszerzają horyzonty i zaspokajają jego potrzebę samorealizacji (Jasiński 2007, s. 85). R.W. Griffin dostrzega, że pojęcie „szkolenia” zazwyczaj dotyczy uczenia się pracowników technicznych lub operacyjnych, a także tego, w jaki sposób mogą oni wykonać wyznaczone prace oraz czynności, do jakich zostali zatrudnieni. Jednakże rozróżnia on też pojęcie „doskonalenia”, czyli „rozwoju”. Jest ono połączone z uczeniem się, wdrażaniem oraz nabywaniem przez pracowników i menedżerów niezbędnych umiejętności potrzebnych do wykonywania działań na teraźniejszym oraz przyszłym stanowisku pracy (Dębska 2012, s. 38). Zdaniem Z. Sekuły szkolenie można określić jako rozwój oraz nabywanie umiejętności, również po części wiedzy, która jest niezbędna do realizowania pracy na danym stanowisku, a także dający możliwość podjęcia pracy na innych stanowiskach w różnych zawodach (Sekuła 2008, s. 81).

Proces szkoleniowy zaczyna się od rozpoznania oraz analizy potrzeb. Rozpoznanie, czyli identyfikacja, to nic innego, jak ustalenie potrzeb szkolenia oraz rozwoju pracowników organizacji, a także organizacji jako całości. Natomiast analiza potrzeb szkoleniowych następuje zaraz po ich rozpoznaniu. Bazuje na określeniu odpowiednich, efektywnych sposobów zaspokajania danej potrzeby (Rae 2021, s. 14). Takiej analizy potrzeb dokonuje się w trzech różnych obszarach: organizacji (firma, grupa, pracownik), stanowiska oraz pracownika (wiedza, umiejętności, kompetencje, postawa, standardy efektywności) (Armstrong 2001, s. 455-456). Również analizy można dokonać w trzech poziomach: doskonalenia, wdrożenia oraz wprowadzenia innowacji (Serafin 2011, s. 193).

Stworzenie planu oraz programu szkoleniowego jest następnym krokiem w procesie szkoleniowym. Zaczynając od istoty planowania, która jest wielostronną funkcją zarządzania, można przyjąć, iż w odniesieniu do działań szkoleniowych planowanie obejmuje takie elementy, jak (Pocztowski 2008, s. 289):

- określenie celów szkolenia (oczekiwanych wyników);
- analizowanie sytuacji szkoleń, by określić negatywne oraz pozytywne czynniki, które mogą w jakiś sposób wpłynąć na osiągnięcie celów;
- badanie pracowników uczących się w kierunku ich możliwości szkoleniowych;
- wybranie metody szkoleniowej, by realizować cele;
- uzgodnienie budżetu, jaki można wydać na szkolenie;
- ustalenie czasu oraz miejsca szkolenia;
- ustalenie programu szkoleniowego w zaplanowanym okresie;
- ustalenie kontroli wcześniej zaplanowanych działań.

Ostatnim etapem rozwoju przez szkolenie jest ocena jego efektów. Najbardziej znany jest model oceny skuteczności szkoleń stworzony przez D.L. Kirkpatricka, który składa się z czterech poziomów (Pocztowski 2008, s. 303; Matejek 2014, s. 334):

- I – ocena reakcji na szkolenie,
- II – ocena uczenia się,
- III – ocena zmian w zachowaniu,
- IV – ocena wyników.

Wyróżnia się trzy miejsca, w jakich mogą odbywać się szkolenia (Armstrong 2001, s. 457-460):

- w miejscu pracy na danym stanowisku pracy,
- w miejscu pracy poza stanowiskiem pracy,
- poza miejscem pracy.

W literaturze przedstawiane są również metody szkoleniowe, które w praktyce klasyfikuje się według zróżnicowanych kryteriów. Do tych, które spotykamy najczęściej, należą (Suchodolski 2004, s. 149-150; Golnau 2004, s. 353):

- pasywne (tradycyjne) oraz aktywne;
- indywidualne oraz grupowe;
- na stanowisku pracy (przyuczanie, instrukcje, asystentura, zastępstwo, następcą, wielostronne kierowanie, koła jakości, ośrodki uczenia się) lub poza stanowiskiem pracy (wykład, rozmowa nauczająca, studia przypadków, gry planistyczne, odgrywanie ról, nauczanie programowe, treningi dynamiki grupy, *action learning*);
- informacyjne (wiedza) lub szkoleniowe (umiejętności) albo mieszane.

Szkolenia są bardzo istotnym przedsięwzięciem w życiu zawodowym każdego pracownika, ponieważ poszerzają zakres jego umiejętności nie tylko z korzyścią dla wykonywania pracy w chwili obecnej, na danym stanowisku, ale także innej pracy w przyszłości, związanej z kompletnie innym stanowiskiem pracy. Poprzez prowadzenie odpowiednich szkoleń kadra pracownicza staje się pewniejsza i wykonuje zdecydowanie lepiej swoje obowiązki, angażując się w pracę. Z punktu widzenia zarządzających, dzięki klarownemu zrozumieniu przez pracowników powagi wykonywanych zadań, w danej organizacji jest łatwiej zapanować nad wydawaniem poleceń zespołowi.

Bezpieczeństwo narodowe

Bezpieczeństwo narodowe to „stan uzyskany w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, tak zewnętrznymi, jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa” (*Słownik...* 2002, s. 29). Bezpieczeństwo można definiować jako stan (poczucie podmiotu) lub jako proces (zapewnianie poczucia bezpieczeństwa) (Goryń 2020, s. 49). Częściej jednak, z uwagi na dynamiczną naturę tego zjawiska, wybiera się drugie z tych podejść. We wskazanym kontekście bezpieczeństwo konkretnego podmiotu będzie związane

z tymi wszystkimi jego aktywnościami, które zapewniają mu możliwość dalszej egzystencji (przetrwania) oraz realizacji własnych interesów w niesprzyjającym, groźnym otoczeniu (przez wykorzystywanie szans, walkę z przeciwnościami, ograniczanie ryzyka i zapobieganie).

Podmiotem bezpieczeństwa mogą być poszczególne osoby, grupy społeczne, narody, społeczności międzynarodowe czy też ludzkość na całym globie (np. podczas pandemii), czyli wszystkie te podmioty, które mają własne ambicje i interesy (Goryń 2020, s. 57). W związku z powyższym ze względu na skalę wyodrębniono następujące rodzaje bezpieczeństwa: indywidualne (osobowe), grupowe (plemienne, rodowe), narodowe (krajowe/państwowe) i międzynarodowe (regionalne, globalne). Z uwagi na charakter niniejszego rozdziału skoncentrowano się w nim na bezpieczeństwie narodowym. Podmiot ma do czynienia z bezpieczeństwem we wszystkich dziedzinach swej aktywności, stąd jego struktura jest tożsama ze strukturą funkcjonowania. Zatem w obrębie bezpieczeństwa narodowego można wyodrębnić takie jego dziedziny, jak: bezpieczeństwo ekonomiczne, społeczne, militarne, publiczne, ekologiczne, informacyjne itp. (Faldowski 2018, s. 111). Bardziej ogólny, dychotomiczny podział bezpieczeństwa dzieli je, ze względu na to, gdzie usytuowane są szanse, wyzwania, ryzyka oraz zagrożenia, na bezpieczeństwo wewnętrzne i zewnętrzne (Kitler 2011, s. 100).

Często też spotyka się określenie „bezpieczeństwo fizyczne”. Odnosi się ono do ochrony i obrony przed ingerencjami (działaniami, zjawiskami) niszczącymi. Państwo (naród) może w tym celu wykorzystać siły i środki, jakimi np. dysponują: wojsko, policja, wywiad, kontrwywiad, straż graniczna, straż pożarna oraz różne służby ochrony itp. Bezpieczeństwo „fizyczne” łączy w sobie dwie główne dziedziny bezpieczeństwa: bezpieczeństwo militarne i bezpieczeństwo cywilne (pozamilitarne). Pierwsze jest częścią bezpieczeństwa zewnętrznego, drugie – wewnętrznego (Koziej 2011, s. 20).

Zagrożenia, zarówno te bezpośrednie, jak i pośrednie, mają destrukcyjne oddziaływanie na podmiot. Można podzielić je na:

- potencjalne i realne,
- subiektywne i obiektywne,
- zewnętrzne i wewnętrzne,
- militarne i pozamilitarne,
- kryzysowe i wojenne,
- intencjonalne i przypadkowe (losowe).

Opis zagrożeń intencjonalnych pozwala wyodrębnić cztery elementy: aktor oraz jego intencje, możliwości i czas na reakcję. Wraz z narastaniem wrogości przeciwnika wzrasta poziom zagrożenia rozwojem jego możliwości do ataku i zniszczenia oraz upływaniem czasu na reakcję (Fish, McCraw, Reddish 2004, s. 4).

Współczesne strategie operacyjne bezpieczeństwa wskazują na trzy rodzaje działań: działania stabilizacyjne (polegające na utrzymywaniu i promowaniu bezpieczeństwa); reagowanie kryzysowe (często określane mianem zarządzania kryzysowego) i działania obronne (wojenne) (Koziej 2011, s. 30). W tym miejscu należy zauważyć, że nowoczesne strategie reagowania kryzysowego są wielokrotnie (z uwagi na typ zagrożenia) strategiami międzynarodowymi.

Kolejną ważną tendencją w omawianej dziedzinie jest coraz bardziej zanikająca granica między militarnymi i pozamilitarnymi zagrożeniami kryzysowymi. Konsekwencją owego zatarcia różnicy jest konieczność zintegrowanego reagowania kryzysowego (cywilno-wojskowego) (Koziej 2011, s. 35). Pozazbrojne działania obejmują oddziaływanie w sposób aktywny na przeciwnika środkami pozamilitarnymi. Ma to na celu osłabienie jego potencjału wojennego oraz podtrzymywanie własnego potencjału obronnego przez rozwinięcie parasola ochronnego nad ludnością i strukturami państwa, a ponadto zapewnienie materialnych i niematerialnych fundamentów przetrwania w czasie wojny, a także wsparcie własnych i sojuszniczych (jeśli takie są) sił zbrojnych.

Na system bezpieczeństwa narodowego składa się całość sił, środków i zasobów (odpowiednio zorganizowanych, utrzymywanych i przygotowanych) przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa. System ten obejmuje system kierowania i szereg podsystemów wykonawczych. Pierwszy z wymienionych jest częścią systemu bezpieczeństwa narodowego przeznaczoną do kierowania jego funkcjonowaniem. System kierowania odnosi się do organów władzy publicznej oraz kierowników jednostek organizacyjnych. Organy te wykonują zadania związane z bezpieczeństwem narodowym (w tym dowodzenia Siłami Zbrojnymi RP) wraz z organami doradczymi i aparatem administracyjnym (sztabowym) oraz procedurami funkcjonowania i infrastrukturą (stanowiska, centra kierowania i zarządzania, system łączności) (Koziej 2011, s. 32). Podsystemy systemu bezpieczeństwa narodowego pozostają w dyspozycji organów kierowania bezpieczeństwem. Są to siły i środki wykonawcze przewidziane do realizacji ustawowo określonych zadań w dziedzinie bezpieczeństwa. Jeśli zachodzi potrzeba, można je połączyć stosownie do głównych dziedzin bezpieczeństwa w trzy podsystemy:

- obronności państwa (obrony narodowej, bezpieczeństwa wojskowego);
- ochrony państwa (ludności, instytucji, zasobów i infrastruktury, czyli podsystem bezpieczeństwa cywilnego, niemilitarnego);
- społeczno-gospodarczego wsparcia bezpieczeństwa.

Podsystem ochrony państwa to ta część całego systemu bezpieczeństwa narodowego, która jest przeznaczona do wykorzystywania szans, sprostania wyzwaniom, zmniejszenia ryzyka i przeciwdziałania zewnętrznym i wewnętrznym zagrożeniom o charakterze pozamilitarnym.

Wpływ na nowe postrzeganie bezpieczeństwa narodowego mają stale ewoluujące zagrożenia. Obecnie istnieje nowy etap stosunków międzynarodowych, w ramach którego współczesne zagrożenia stały się globalne i mogą dotyczyć każdego państwa (Olak 2016, s. 469). Do nie tak dawna najbardziej uciążliwymi zagrożeniami były klasyczne klęski żywiołowe (powódź, susza, grad, trzęsienia ziemi, plagi, czasem epidemie itp.) i terroryzm (bezpośrednie zabijanie: wysadzanie lub atak z bronią w rękę). Oczywiście zagrożenia te do dzisiaj stanowią bezpośrednie niebezpieczeństwo dla społeczeństwa, wpływając na funkcjonowanie wielu ludzi, państw i instytucji, zwłaszcza w sferach gospodarczych i społecznych (Borkowski 2001, s. 65). Jednakże ze względu na rozwój cywilizacyjny zagrożenia również zmieniały swój charakter i stąd mamy dzisiaj do czynienia z pandemiemi, cyberterroryzmem czy atakami hybrydowymi.

Metodologia przeprowadzonych badań

Przedmiotem pracy jest opinia badanych na temat wpływu szkoleń zleczanych przez pracodawcę na rozwój zawodowy pracowników. Natomiast celem postawionym badaniu jest sprawdzenie, czy pracownicy chcą uczestniczyć w szkoleniach oraz czy proces szkolenia ma wpływ na podwyższenie kompetencji, wiedzy i umiejętności, które można będzie wykorzystać w praktyce, podczas realizacji zadań służbowych.

W pracy zastosowano metodę badań sondażowych z wykorzystaniem ankiety. Kwestionariusz ankiety zawierał 19 pytań (plus tzw. metryczka), mających na celu uzyskanie odpowiedzi na postawione w pracy szczegółowe pytania badawcze:

1. Czy w urzędzie są organizowane szkolenia?
2. Czy poprzez szkolenia pracodawca troszczy się o rozwój zawodowy swoich pracowników (np. ilość, dostęp do szkoleń, realny wpływ na awans)?
3. Czy organizowane szkolenia są odbierane przez pracowników jako przydatne w codziennej pracy zawodowej?

Badania przeprowadzono na przełomie lipca i sierpnia 2021 roku (w warunkach pracy stacjonarnej) wśród pracowników urzędu gminy wiejskiej powiatu częstochowskiego. Dobór próby badawczej był proporcjonalny pod względem płci zatrudnionych. W opracowaniu uwzględniono dane badawcze pochodzące z 45 poprawnie wypełnionych, anonimowych ankiet papierowych.

Zebrany materiał badawczy

Strukturę demograficzną ankietowanych opisano w tabeli 10.1.

Tabela 10.1. Zróżnicowanie badanych pod względem: płci, wieku, wykształcenia i stażu pracy

	Płeć		Wiek		Wykształcenie				Staż pracy	
	K	M			podś.	zaw.	śred.	wyż.		
Liczba	33	12	21-30 lat	3	1	5	9	30	< 1 rok	1
			31-40 lat	8					1-10 lat	12
			41-50 lat	22					11-20 lat	25
			> 50 lat	12					> 20 lat	7
%	73,3	26,7	21-30 lat	6,7	2,2	11,1	20,0	66,7	< 1 rok	2,2
			31-40 lat	17,8					1-10 lat	26,7
			41-50 lat	48,9					11-20 lat	55,6
			> 50 lat	26,7					> 20 lat	15,6

Źródło: opracowanie własne na podstawie przeprowadzonych badań ankietowych

W przypadku pytania o obejmowane stanowisko odpowiedzi opisywane były ogólnie. Większość, bo aż 20 osób odpowiedziało, że zajmuje samodzielne stanowisko, nikt z ankietowanych nie zakreślił odpowiedzi dotyczącej stanowiska kierowniczego. Pozostali ankietowani, a więc 25 osób, to pracownicy obsługi. Analizując

udzielone przez ankietowanych odpowiedzi, można zauważyć, że pracownicy urzędu dostrzegają pozytywy szkoleń przeprowadzanych przez pracodawcę, ale też wskazują pewne obszary, które należałoby poprawić. Pozytywne strony szkolenia to:

- Fakt organizowania szkoleń w urzędzie – 100% osób opisywało szkolenia w urzędzie, stąd wniosek, że pracodawca organizuje szkolenia dla pracowników.
- Szkolenia są potrzebne – to opinia 93,3% badanych.
- Urzędnicy chętnie wezmą udział w szkoleniach (86,7%).
- Badani nie są zgodni, co do najlepszego momentu na organizowanie szkoleń. Świadczy o tym rozkład odpowiedzi: „powinien być to proces stały – 37,8%; „podczas objęcia nowych obowiązków” – 33,3%; „na początku zatrudnienia” – 28,9%.
- Najlepsza częstotliwość szkoleń to: „bardzo często” – 13,3% i „często” – 62,2% (w sumie 75,5%), „trudno powiedzieć” – 6,7%, „rzadko” – 17,8%, „bardzo rzadko” – 0%.
- Po udziale w szkoleniach urzędnicy oczekują głównie „zdobycia wiedzy” – 42,3%. Inne wskazania to: „wzrost kompetencji na zajmowanym stanowisku” – 31,1%), „awans” – 22,2%, „zaspokojenie ambicji” – 4,4%, „inne” – 0%.
- Udział w szkoleniach przyczynia się w stopniu „odpowiednim” do rozwoju zawodowego – 42,3%, „znaczącym” – 33,3%, „nieznaczącym” – 24,4%.
- Szkolenia raczej powinny być brane pod uwagę przy ocenie pracowniczej: „zdecydowanie tak” – 26,7% i „raczej tak” 60,0% (w sumie 86,7%), „trudno powiedzieć” – 6,7%, „raczej nie” – 4,4%, „zdecydowanie nie” – 2,2%.
- Pracownicy raczej wykorzystują wiedzę i umiejętności zdobyte na szkoleniach, w swojej pracy: „zdecydowanie tak” – 15,5% i „raczej tak” – 60% (w sumie 75,5%), robią to w stopniu „dobrym” – 46,7% i „bardzo dobrym” – 11,1%.
- Podczas szkolenia uwaga skupiona jest na „tematyce i programie” – 40% oraz „dostępności i zrozumiałości materiałów” – 28,9%, ponadto „atmosfera podczas szkolenia” – 20,0% i „miejsce szkolenia” – 11,1%.
- Najbardziej odpowiadającą formą szkolenia są szkolenia „dla osób określonego szczebla” – 33,3%, „prowadzone przez osoby z zewnątrz” – 28,9%) oraz „indywidualne” – 22,2%, zaś „prowadzone przez dział wewnętrzny” – 15,6%.
- Delegując na szkolenie, pracodawca „chce podnieść kwalifikacje pracowników” – 57,8%, a oprócz tego istnieje „zapotrzebowanie na wiedzę wśród pracowników” – 20,0%, pracodawca kieruje się „efektami, jakie przyniesie wiedza i umiejętności nabyte” – 17,8%, chce „dać satysfakcję pracownikom” – 4,4%.
- Pracownicy oczekują szkoleń „łączących teorię z praktyką” – 44,4%, a także: „szkoleń praktycznych” – 28,9% i „szkoleń teoretycznych” – 26,7%.
- Pracownicy uważają, że pracodawca raczej dba o rozwój zawodowy swoich pracowników – „zdecydowanie dba” 28,9% i „raczej dba” 44,4% (w sumie 73,3%), pozostali odpowiedzieli: „trudno powiedzieć” – 13,4%, „raczej nie” – 11,1 %, „zdecydowanie nie” – 2,2%.
- Liczba szkoleń zdaniem większości respondentów „pozostała bez zmian” – 44,4% lub „wzrosła” – 40%, natomiast „spadek” wskazało tylko 15,6% ankietowanych.

- Jako negatywne strony szkoleń w badanym urzędzie wymieniono:
- Najczęściej stosowana metoda szkolenia to „wykład” – 51,1%), pozostałe sposoby/narzędzia szkolenia to: „materiały dydaktyczne” – 17,8%, „instruktarz” – 15,6%, „komputer” – 8,9%; „coaching” – 4,4%, „mentoring” – 2,2%.
- Uzyskane na szkoleniu informacje są podstawowe (wymagają uzupełnienia np. przez rozmowę) – 60%. Pozostali badani udzielili odpowiedzi: „wyczerpujące” – 35,6%, „niedostateczne” – 4,4%.
- Decyzję o tematyce szkolenia podejmuje „pracodawca” – 60%, czasem też: „konsultuje decyzję z pracownikami, ale nie zawsze uwzględnia ich sugestie” – 33,3%, „pracownicy zawsze mają wpływ na wybór tematyki szkolenia” – 6,7%.
- W opiniach aż 60,0% badanych „nie ocenia się efektów szkoleń”, przeciwnie jest w przypadku 40%: „ocena za pomocą ankiety” – 31,1% oraz przez „spotkanie i rozmowę” – 8,9%.

Podsumowanie

Doskonalenie zawodowe w postaci szkoleń organizowanych dla urzędników są niezwykle ważnym elementem, ponieważ ma na celu wyposażenie każdego pracownika w daną wiedzę oraz umiejętności, jakie są niezbędne do wykonywania konkretnie określonej pracy lub podczas objęcia nowej, zleconej. Coraz częściej pracodawcy zwracają uwagę na podnoszenie kwalifikacji swoich podwładnych, dlatego szkolenia powinny być stałym procesem lub być realizowane według programów szkoleniowych wedle projektów rozwoju ścieżek kariery.

Personel badanego urzędu gminy pracuje w dobrych warunkach pracy, jest również na bardzo dobrej drodze do własnego ciągłego rozwoju i doskonalenia się. Wszystkie szkolenia prowadzą do tego, że pracownicy stale zwiększają swoją pomysłowość, innowacyjność, a zdobyta wiedza i umiejętności pomagają umocnić ich pozycje zawodowe. Szkolenia dają urzędnikom powód do zadowolenia, ponieważ to dzięki nim mają nowe spojrzenie na wykonywane dotychczas zadania, znajomość aktualnych przepisów, procedur i praktyk postępowania. Fakt delegowania na szkolenie poprawia nastawienie pracowników, gdyż odbierają to jako formę docenienia przez pracodawcę. Wyniki przeprowadzonych badań dowodzą, że szkolenia pracowników urzędu gminy wiejskiej odgrywają istotną rolę w ich życiu zawodowym, a pracodawca troszczy się o rozwój swoich podwładnych.

Reasumując, należy podkreślić, iż szkolenia ankietowanych urzędników w kontekście bezpieczeństwa kraju spełniają pozytywną rolę, jaką im wyznaczono (wskazuje na to pozytywne nastawienie do szkoleń, chęć uczestnictwa, ocena efektów itp.). Czas pandemii wyraźnie pokazał konieczność szybkiej reakcji w warunkach zagrożenia. Należy zatem uznać fakt, że natychmiastowe działania w sytuacji zagrożenia czy kryzysowej pomoże uniknąć lub przynajmniej zminimalizować jej negatywne skutki. W okresie minionego 1,5 roku zarówno rządzący, jak i zarządzający mieli okazję przekonać się, że tylko szkolenia są tym narzędziem, które w sytuacji zagrożenia pozwala reagować szybko, elastycznie i na szeroką skalę. Natomiast przeprowadzone badania wykazały, że urzędnicy są otwarci na szkolenia, stąd nie ma w tym aspekcie zagrożenia dla bezpieczeństwa naszego kraju. Warto jednak

przeanalizować wskazane przez badanych elementy, które mogą podnieść efektywność tych szkoleń.

Literatura

1. Armstrong M. (2001), *Zarządzanie zasobami ludzkimi*, Dom Wydawniczy ABC, Kraków.
2. Borkowski R. (2001), *Cywilizacja, technika, ekologia. Wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku*, Wydawnictwa Akademii Górniczo-Hutniczej, Kraków.
3. Dębska E. (2012), *Chaos pojęciowy wokół szkoleń i treningów. Próba uporządkowania terminologii*, „Edukacja Dorosłych”, 1, 66, s. 23-42.
4. Faldowski M. (2018), *Współczesny wymiar bezpieczeństwa*, „Zeszyty Naukowe SGSP”, 66, 2/2, s. 109-122.
5. Fish J.M., McCraw S.J., Reddish Ch.J. (2004), *Fighting in the Gray Zone: A Strategy to Close the Preemption Gap*, US Army War College, Strategic Studies Institute, September.
6. Golnau W. (red.) (2004), *Zarządzanie zasobami ludzkimi*, CeDeWu, Warszawa.
7. Goryń P. (2020), *Bezpieczeństwo społeczne – jedno czy wiele?*, [w:] Boćkowski D., Goryń P., Goryń K. (red.), *Bezpieczeństwo i jego percepcja w dyskursie społecznym i militarnym*, s. 47-61, Wydawnictwo Uniwersytetu w Białymstoku.
8. Jasiński Z. (2007), *Motywowanie w przedsiębiorstwie*, Wydawnictwo Placet, Warszawa.
9. Kitler W. (2011), *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Wydawnictwo AON, Warszawa.
10. Koziej S. (2011), *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe”, II –18, s. 19-39.
11. Król H., Ludwicyński A. (2007), *Zarządzanie zasobami ludzkimi*, Wydawnictwo Naukowe PWN, Warszawa.
12. Matejek P. (2014), *Szkolenia pracownicze w nowoczesnej organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie”, 27, 100, s. 325-335.
13. Olak K., Olak A. (2016), *Współczesne rozumienie bezpieczeństwa narodowego*, „Acta Scientifica Academiae Ostroviensis. Sectio A. Nauki Humanistyczne, Społeczne i Techniczne”, 7, 1, s. 467-480.
14. Pocztowski A. (2008), *Zarządzanie zasobami ludzkimi. Strategie – procesy – metody*, PWE, Warszawa.
15. Rae L. (2021), *Planowanie i projektowanie szkoleń*, Wydawnictwo Nieoczywiste, Warszawa.
16. Sekuła Z. (2008), *Motywowanie do pracy. Teorie i instrumenty*, PWE, Warszawa.
17. Serafin K. (2011), *Identyfikacja potrzeb szkoleniowych jako istotny obszar działań w zarządzaniu personelem*, „Problemy Zarządzania”, 9, 4, s. 191-203.
18. *Słownik terminów z zakresu bezpieczeństwa narodowego* (2002), Wydawnictwo AON, Warszawa.
19. Suchodolski A. (2004), *Rozwój pracowników*, [w:] Listwan T. (red.), *Zarządzanie kadrami*, C.H. Beck, Warszawa.
20. Szczęsna A., Danielewicz D. (2004), *System szkoleń*, [w:] Rostkowski T. (red.), *Nowoczesne metody zarządzania zasobami ludzkimi*, Difin, Warszawa.

THE SIGNIFICANCE OF IMPROVEMENT IN THE PROCESS OF PROFESSIONAL DEVELOPMENT OF PUBLIC ADMINISTRATION EMPLOYEES AND INCREASING THE SECURITY OF THE COUNTRY

Abstract: Due to the perception of a human being as the most valuable capital of an organization, there is a growing interest in the knowledge of how to properly manage

an employee. Among the numerous elements related to personnel management, one of the most interesting (and at the same time essential for the discussed issue), which is related to both the investment in the employee and the institution, is training organized inside or outside the organizational unit. The time of the COVID-19 pandemic has clearly shown the need for training that has a direct impact on health security, as well as cyber, military and other. The aim of the chapter will be to examine the attitude, willingness to participate in training, selected for the research of secondary school employees.

Keywords: improvement, professional development, public administration, security

Rozdział 11

WPŁYW PRACY ZDALNEJ W WARUNKACH PODWYŻSZONEGO RYZYKA NA BEZPIECZEŃSTWO I HIGIENĘ PRACY NAUCZYCIELI AKADEMICKICH W MYŚL KONCEPCJI *WORK-LIFE-BALANCE*

Aleksandra Zyska¹³, Adam Pawlak¹⁴, Michał Braczkowski¹⁵

Streszczenie: W ostatnim czasie praca zdalna zdominowała zadania pracownicze wielu zawodów. Dużym wyzwaniem była dla pracowników, którzy do tej pory nie mieli z nią żadnej styczności. W świetle raportów i dostępnych doniesień pracownicy w różny sposób radzili sobie z sytuacją i warunkami narzuconymi z góry, a wymuszonymi pandemią COVID-19. Również nauczyciele akademicki byli zmuszeni do dużych zmian, zwłaszcza w aspekcie warunków pracy dydaktycznej. Niniejszy rozdział przedstawia wpływ pracy zdalnej w czasach pandemicznych na szeroko pojęte bezpieczeństwo i higienę pracy nauczycieli akademickich w myśl zasady *work-life-balance*. Badania wykonano przy pomocy autorskiego kwestionariusza ankietowego wśród losowo wybranych nauczycieli akademickich w całej Polsce przez Internet. Badania miały charakter dobrowolny i anonimowy. Zaprezentowane wyniki są częścią większej całości.

Słowa kluczowe: bezpieczeństwo i higiena pracy, ergonomia, praca zdalna, *work-life-balance*

Wprowadzenie

Ochrona zdrowia i życia pracownika jest obowiązkiem każdego pracodawcy (*Kodeks pracy*), a bezpieczne warunki pracy są priorytetem we wszystkich organizacjach. Na to bezpieczeństwo składa się wiele elementów środowiska pracy – zarówno materialnych, jak i pozamaterialnych (Koradecka 2008, s. 17; Ulewicz i in. 2015, s. 78). Efektywne i rzetelne, ale również realne dbanie o bezpieczne i higieniczne warunki pracy stało się w okresie podwyższonego ryzyka, jakim niewątpliwie jest pandemia COVID-19, bardzo trudne. Wiele zawodów zostało „przeniesionych” do pracy zdalnej w warunkach domowych, które nie są naturalnym środowiskiem

¹³ Uniwersytet Opolski, Wydział Lekarski

¹⁴ Uniwersytet Opolski, Wydział Lekarski

¹⁵ Uniwersytet Opolski, Wydział Lekarski

pracy. Taką grupą zawodową, która w sposób natychmiastowy, bez odpowiedniego przygotowania została przeniesiona z zadaniami pracowniczymi do miejsc zamieszkania, byli nauczyciele akademicki (Romaniuk, Łukasiewicz-Wieleba, Kohut 2020, s. 15). Wraz ze zmianą środowiska pracowniczego pojawiły się nowe zagrożenia i niedogodności, które obniżały efektywność oraz jakość pracy nauczycieli (Jeran 2016, s. 54). Pomimo tego, że generalnie nauka zdalna jest zjawiskiem bardzo pozytywnym, gdyż m.in. daje możliwość większej liczbie osób korzystać z edukacji, to już praca zdalna wymuszona kryzysem związanym z pandemią COVID-19 niesie wiele negatywnych zjawisk oraz barier (Marinoni, van't Land, Jensen 2020, s. 9). Bariery te mogą mieć charakter organizacyjny (np. brak umiejętności zarządzania czasem bądź brak odpowiednich warunków, by efektywnie nim zarządzać), społeczny (ekstrawertycy źle znoszą pracę w trybie zdalnym), a także kompetencyjny (brak umiejętności w obszarze IT, zwłaszcza wśród starszych nauczycieli) oraz materialny – techniczny (brak odpowiedniego sprzętu i oprogramowania).

Praca zdalna w opinii nauczycieli akademickich

Edukacja zdalna jest przez specjalistów uznawana za bardzo istotny element wzmacniania jakości kształcenia oraz sposób pozwalający uczyć się większej liczbie osób (zwłaszcza wykluczonej z edukacji tradycyjnej). Główną zaletą jest przede wszystkim elastyczność dotycząca czasu i miejsca uczenia się, dzięki czemu możliwe staje się łączenie tego procesu z innymi obowiązkami: zawodowymi i rodzinnymi. Jakość nauki w trybie online zależy w głównej mierze od jakości oferowanych zajęć, która z kolei uzależniona jest od kompetencji merytorycznych, dydaktycznych i informatycznych nauczycieli oraz od ich gotowości do pracy online. Bardzo duże znaczenie ma także przygotowanie technologiczne danej uczelni. Chodzi tu nie tylko o platformę, ale również dostępne rozwiązania organizacyjne i formalnoprawne, które będą pozwalać na prowadzenie efektywnych zajęć zdalnych. Przygotowanie takich kursów w trybie online wymaga dodatkowego czasu i wysiłku. Istotne jest wsparcie techniczne i metodyczne dla nauczycieli akademickich ze strony uczelni, a doświadczenie związane z uczestnictwem w takich zajęciach jest praktycznie niezbędne (Romaniuk, Łukasiewicz-Wieleba, Kohut 2020, s. 15-16). Należy przewidzieć różne sytuacje i reakcje studentów, które są zupełnie inne niż w sali akademickiej. W przestrzeni wirtualnej zmienia się rola nauczyciela, zaś tradycyjne metody pracy z uczniem nie muszą być równie skuteczne jak w trybie online (Armstrong 2000; Alexander 2001).

Kryzys związany z koronawirusem rozpoczął się 12 marca 2020 roku, a więc dwa tygodnie po rozpoczęciu semestru letniego roku akademickiego 2019/2020. Ministerstwo Nauki i Szkolnictwa Wyższego ogłosiło wówczas zawieszenie zajęć dydaktycznych na uczelniach wyższych do 25 marca. Decyzja była podyktowana koniecznością zapobiegania rozprzestrzenianiu się choroby COVID-19. 23 marca pojawiło się rozporządzenie przedłużające okres zawieszenia zajęć stacjonarnych do 10 kwietnia oraz wprowadzające obowiązek kształcenia zdalnego. Osoby prowadzące zajęcia na uczelniach wyższych niejako w trybie awaryjnym zostały więc zobowiązane do prowadzenia zajęć zdalnych. Dość powszechnie zaczęto określać tę

sytuację mianem „e-learningu” lub „online learningu”, jednak jeszcze pod koniec marca pojawiły się głosy, że jest to w istocie *emergency remote teaching*, a więc „awaryjne kształcenie zdalne”. W ramach próby rozróżnienia tych dwóch aktywności edukacyjnych podkreślano różnicę między „dobrze zaplanowanym doświadczeniem kształcenia online (...) a kursami online oferowanymi w odpowiedzi na kryzys czy katastrofę” (Siwińska, Łysik 2020, s. 17). Jak z kolei zareagował świat? Boston University wprowadził jedne z najbardziej restrykcyjnych programów ochrony przed koronawirusem. Mało która uczelnia zdecydowała się pójść taką drogą. W tej kwestii w Ameryce panuje dowolność – każdy college i uniwersytet sam ustala zasady funkcjonowania w semestrze jesiennym. Według danych zebranych przez Davidson College z Północnej Karoliny na blisko 3 tys. amerykańskich uczelni ponad 1300 wprowadziło nauczanie online jako jedyny lub główny model funkcjonowania. Na tryb tradycyjny, w mniejszym lub większym zakresie, zdecydowało się około 900 szkół wyższych (Siwińska, Łysik 2020, s. 34). W Wielkiej Brytanii szkoły wyższe były zamknięte od marca. We wrześniu po raz pierwszy pojawiło się na nich ponad 2 mln studentów. Rząd w Londynie oraz lokalne władze wydały szereg zaleceń m.in. częstsze wietrzenie pomieszczeń, dezynfekcję powierzchni, a przede wszystkim ograniczenie kontaktów towarzyskich i kwarantannę. Studenci w Szkocji mieli np. zakaz organizowania przyjęć, spotkań, chodzenia do barów i restauracji. Uniwersytety w Niemczech, szykując się na drugą falę pandemii, wprowadziły studium hybrydowe. Obowiązkowe były maseczki i utrzymanie dystansu 1,5-2 m, a w pracowniach, stołówkach czy bibliotekach mogło przebywać mniej ludzi. Ograniczenia dotyczyły też liczby osób, które mogą jednocześnie korzystać z pomieszczeń socjalnych, wind albo uczelnianych samochodów (Siwińska, Łysik 2020, s. 38).

W Polsce planowano, że zajęcia w roku akademickim 2020/2021 będą odbywać się przede wszystkim zdalnie. Na niektórych uczelniach zostały wprowadzone modele hybrydowe, gdzie wykłady oraz konwersatoria odbywać się miały online, zaś przedmioty wymagające obecności w laboratorium czy warsztacie w salach uczelni z zachowaniem określonych zasad. Do rzeczywistości cyfrowej stopniowo przenoszone były kolejne elementy życia akademickiego – chociażby uroczyste rozpoczęcie roku akademickiego (Siwińska, Łysik 2020, s. 41). Obecnie powrócono do tradycyjnej formy nauczania (stacjonarnego). Jak długo potrwa ta forma pracy nauczyciela akademickiego? Na pewno jest to uzależnione od liczby zachorowań.

Kryzys związany z pandemią COVID-19 spowodował, że cała społeczność akademicka została przeniesiona do pracy zdalnej w warunkach domowych. Taka sytuacja wywołała wiele negatywnych zjawisk. Uciążliwość warunków oraz sposobu pracy wpłynęła w istotny sposób zarówno na jakość kształcenia, jak i edukacji. Ogólnodostępne raporty wskazały na przyczyny, które zdaniem badanych wpływały negatywnie na pracę zdalną w warunkach domowych nauczycieli akademickich. Były to m.in. niedostatki w zapleczu techniczno-technologicznym (brak odpowiedniego oprogramowania, nierzadko brak sprzętu czy dostępu do Internetu). Również organizacja pracy pozostawiała wiele do życzenia zarówno z perspektywy dawcy usługi dydaktycznej (nauczyciela), jak i biorecy (studenta). Jeśli jedna ze stron nie posiadała odpowiedniego zaplecza techniczno-organizacyjnego, wówczas proces

nauczania zdalnego nie był ani efektywny, ani rzetelny. Należy tutaj zwrócić uwagę na fakt, iż studenci, podejmując decyzję o studiowaniu, nie przewidzieli, że będą musieli wrócić do rodzinnego domu (w którym mogło nie być warunków do nauki) bądź posiadać sprzęt (komputer, dostęp do Internetu), który jest niezbędny do nauki zdalnej. Bariery zdalnego nauczania, ale i uczenia się odcisnęły bardzo mocne piętno m.in. na frekwencję podczas zajęć dydaktycznych w trybie zdalnym oraz zaliczenie poszczególnych przedmiotów. Wielu studentów przerwało naukę bądź nie zaliczyło ostatniego roku i powtarzają go w trybie stacjonarnym obecnie (Klimowicz 2020, s. 24).

Podsumowując, należy podkreślić, że praca i nauka w trybie zdalnym przysporzyły wielu problemów zarówno nauczycielom, jak i studentom. Na potrzeby niniejszego rozdziału anonimowo zapytano nauczycieli akademickich, jakich największych problemów doświadczyli w związku z przejściem na pracę zdalną i przeniesieniem jej w prywatne warunki mieszkaniowe. Respondenci wskazali przede wszystkim czynniki technologiczno-techniczne (brak kamerki w komputerze, brak odpowiedniej liczby komputerów w domu, by wraz z pozostałymi członkami wykonywać swoje obowiązki w tym samym czasie, brak oprogramowania), organizacyjne (nieefektywne zarządzanie czasem przejawiające się m.in. zbyt dużą ilością czasu spędzanego przed komputerem i na przygotowaniach materiałów dla studentów, przenikanie się obowiązków domowych i zawodowych). Również brak odpowiedniego poziomu kompetencji i umiejętności z zakresu posługiwania się zarówno sprzętem, jak i programami komputerowymi (obszar IT) wśród nauczycieli akademickich stanowił barierę dla efektywnego wykonywania pracy w trybie zdalnym. Wyniki zbiorcze przedstawiono w tabeli 11.1.

Tabela 11.1. Przyczyny problemów związanych z przejściem na pracę zdalną w domu w opinii nauczycieli akademickich

Przyczyny	Odpowiedzi „tak” w % ujęciu
Brak odpowiedniego sprzętu i oprogramowania	34%
Brak wysokich kompetencji w obszarze IT	43%
Brak realnego kontaktu ze wszystkimi studentami	35%
Nieefektywne zarządzanie czasem, wynikające z nakładania się obowiązków domowych	75%
Wydłużony czas pracy zawodowej związany z przygotowaniem materiałów dla studentów i weryfikowaniem ich wiedzy	78%
Stres związany z nowymi warunkami pracy	38%

Źródło: opracowanie własne

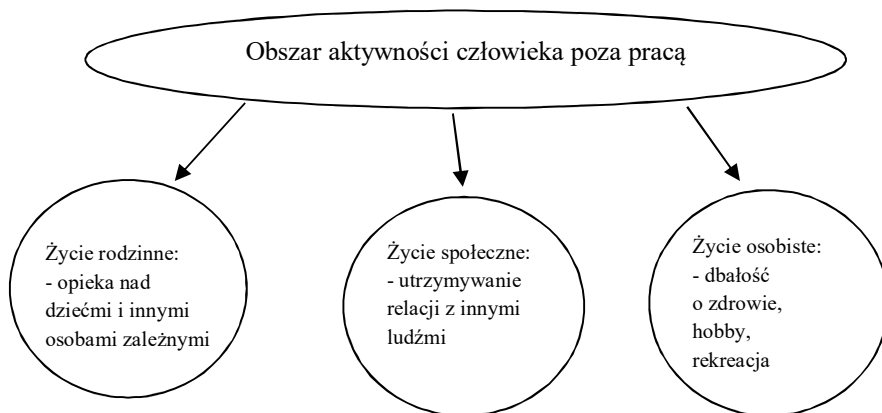
Jak wynika z informacji zawartych w tabeli 11.1, aż 3/4 respondentów za przyczyny problemów związanych z przejściem na pracę zdalną w domu uznało wydłużony czas pracy zawodowej spowodowany przygotowaniem materiałów dla studentów i weryfikowaniem ich wiedzy, a także nieefektywne zarządzaniem czasem, które wynikało z nakładania się obowiązków domowych na zawodowe. Co trzeci nauczyciel uskarżał się na brak realnego, w trybie rzeczywistym kontaktu ze studentami oraz brak odpowiedniego sprzętu i oprogramowania. Brak wysokich kompetencji w obszarze IT stanowiło również nie lada wyzwanie dla nauczycieli akademickich. Podsumowując, należy stwierdzić, że sytuacja kryzysowa, która wymusiła na nauczycielach pracę zdalną w domu, obnażyła ich braki w umiejętnościach z obszaru IT oraz problemy w efektywnym zarządzaniu czasem i radzeniu sobie ze stresem.

Bezpieczeństwo i higiena pracy zdalnej w warunkach podwyższonego ryzyka a *work-life-balance* w opinii nauczycieli akademickich

Koncepcja *work-life-balance* narodziła się w latach 70. ubiegłego stulecia, ale duży rozgłos zyskała w drugiej dekadzie XXI wieku ze względu na rosnące wskaźniki pracoholizmu, a także zbyt dużą ilość czasu spędzanego na obowiązkach domowych (Babczyński 2011, s. 19). Przyczyną z jednej strony było dążenie do jak największych sukcesów i kariery, a z drugiej praca zdalna, która wymaga dobrego zorganizowania swojego czasu. Utrzymanie zdrowej równowagi między sferą zawodową i prywatną jest możliwe tylko wtedy, gdy człowiek w odpowiedni sposób zadba o swoje zdrowie psychiczne i czas poświęcany na sprawy rodzinne i towarzyskie. Zgodnie z badaniami psychologicznymi to właśnie wsparcie społeczne zmniejsza stres, działa motywująco, a także minimalizuje ryzyko pracoholizmu i wypalenia zawodowego (Hildt-Ciupińska 2014, s. 14).

Równowaga „praca – życie prywatne”, czyli wspomniane *work-life-balance*, jest trudne do zdefiniowania. Wynika to m.in. z niejednoznaczności pojęć zawartych w tym sformułowaniu, przede wszystkim „życia”, które w tym przypadku obejmuje cały obszar aktywności człowieka poza pracą (Greenhaus, Collins, Shaw 2003). Są to takie sfery jak m.in. życie rodzinne, życie społeczne, życie osobiste. Ta wspomniana triada jest zaprezentowana na rysunku 11.1. Życie rodzinne oznacza przede wszystkim opiekę sprawowaną nad dziećmi, ale również nad każdą osobą, która tego wymaga i jest od nas zależna. Życie społeczne z kolei oznacza wszelkie relacje, jakie utrzymujemy z innymi ludźmi. Ostatni element triady, czyli życie osobiste, to przede wszystkim dbanie o własne zdrowie, aktywność fizyczna i rekreacja oraz realizowanie swojego hobby.

W dzisiejszych czasach bardzo łatwo jest zapomnieć o granicy pomiędzy życiem prywatnym a sferą zawodową. Wagę tego problemu potwierdzają badania przeprowadzone przez Organizację Współpracy Gospodarczej i Rozwoju (OECD). Według OECD Polska kilka lat temu zajmowała 2. miejsce w Europie pod względem czasu spędzanego w pracy (OECD 2018).



Rysunek 11.1. Triada elementu składowego *work-life-balance* – obszaru aktywności człowieka poza pracą

Źródło: opracowanie własne

Na potrzeby niniejszego rozdziału zapytano anonimowych respondentów wykonujących pracę nauczyciela akademickiego, jak oceniają swoją równowagę „praca – życie prywatne” w warunkach podwyższonego ryzyka i pracy zdalnej wykonywanej w warunkach domowych. Prawie wszyscy badani nauczyciele zgodnie przyznali, że równowaga jest zaburzona przez przeniesienie pracy do domu. Ponadto stwierdzili, że takie warunki pracy nie są optymalne i negatywnie wpływają na ich samopoczucie. Jako przyczynę wskazywali najczęściej brak odosobnionego miejsca na wykonywanie pracy zawodowej, wydłużenie czasu poświęcanego na przygotowanie materiałów do zajęć oraz przenikanie poszczególnych zadań pracy zawodowej z domowymi, co z kolei skutkuje rozdrażnieniem, zmęczeniem i brakiem czasu na wypoczynek. Wyniki badań przedstawiono w tabeli 11.2.

Tabela 11.2. Przyczyny zaburzenia równowagi *work-life-balance* w związku z wykonywaniem pracy zdalnej w warunkach domowych przez nauczycieli akademickich

Przyczyny	Odpowiedzi „tak” w % ujęciu
Przeniesienie pracy zawodowej do domu	98%
Większe niż w normalnych warunkach spędzanie czasu nad przygotowaniem materiałów dydaktycznych i sprawdzaniu efektów uczenia się studentów	87%
Brak warunków do efektywnej i spokojnej pracy zdalnej w warunkach domowych (inni domownicy)	92%
Przenikanie się zadań zawodowych i prywatnych (pełnienie ról społecznych)	76%
Brak odpowiednich zabezpieczeń techniczno-technologicznych (komputer z kamerką, brak dostępu do Internetu)	45%

Źródło: opracowanie własne

Respondenci wskazali również skutki tego zaburzenia, które wynika z przeniesienia pracy zawodowej do miejsca zamieszkania. W tabeli 11.3 przedstawiono wyniki. Ogólne zmęczenie zauważył co drugi badany nauczyciel akademicki (51%). Prawie 70% badanych wskazywało ból kręgosłupa, spowodowany zbyt długim siedzeniem przy komputerze. Badani nauczyciele akademicy zaznaczyli również, że praca zdalna w warunkach domowych w okresie podwyższonego ryzyka spowodowała brak czasu na jakąkolwiek aktywność fizyczną (64%).

Tabela 11.3. Skutki zaburzenia równowagi work-life-balance w związku z wykonywaniem pracy zdalnej w warunkach domowych przez nauczycieli akademickich

Skutki	Odpowiedzi „tak” w % ujęciu
Zmęczenie	51%
Ból głowy	34%
Brak motywacji do pracy	44%
Rozdrażnienie, poddenerwowanie	87%
Rozkojarzenie	67%
Ból kręgosłupa związany ze zbyt długą pracą siedzącą przy komputerze	68%
Dolegliwości mięśniowo-szkieletowe	76%
Nadużywanie leków nasennych i używek (kawa, papierosy, energetyki itp.)	23%
Brak czasu na aktywność fizyczną	64%

Źródło: opracowanie własne

Zaburzenie równowagi praca – życie prywatne skutkuje negatywnymi zjawiskami zarówno w sferze prywatnej, jak i zawodowej. Należy jednak pamiętać, że o równowagę w tych dwóch obszarach życia powinien troszczyć się nie tylko pracownik, ale i pracodawca, prowadząc optymalną politykę zatrudnienia. To również w jego interesie leży bowiem potrzeba utrzymania wspomnianego balansu. Pracodawca nie powinien przeciążać pracownika obowiązkami, pamiętając o tym, że ma on również życie osobiste, które nie powinno być zaniedbywane.

Podsumowanie

Praca zdalna wśród grupy zawodowej, jaką są nauczyciele akademicy, przyniosła w ich opinii wiele negatywnych zjawisk i skutków zarówno w sferze zdrowia fizycznego, jak i psychicznego, a także w obszarze zawodowym i prywatnym. Brak warunków, by w pełni odseparować zadania pracy zawodowej od zadań wynikających z pełnienia różnych ról społecznych w życiu prywatnym, dość mocno zaburzył równowagę w myśl koncepcji *work-life-balance*. Skumulowanie wszystkich zadań w jednym miejscu (najczęściej w domu) spowodowało przenikanie się życia

prywatnego z życiem zawodowym, co często skutkowało zaburzeniem proporcji i brakiem motywacji. Z kolei brak tych proporcji wywoływał wśród nauczycieli poczucie braku satysfakcji zarówno z wykonywania pracy zawodowej, jak i obowiązków domowych. Praca zawodowa stawała się przykrym obowiązkiem, a obowiązki domowe nie były realizowane według założeń badanych nauczycieli. Praca zdalna w domu oprócz wzmocnionych dolegliwości mięśniowo-szkieletowych, na które w ankiecie uskarżali się respondenci, spowodowała również zaburzenia granicy pomiędzy życiem prywatnym a zawodowym, co przekładało się na obniżoną jakość pełnienia ról w obu sferach – i zawodowej, i prywatnej. Można mieć tylko nadzieję, że powrót nauczycieli akademickich do pracy stacjonarnej przywróci im zarówno poczucie bezpieczeństwa, jak i znaczenia roli pełnionej w życiu zawodowym i prywatnym. Wyniki przeprowadzonych badań oraz te pochodzące z raportów wskazują na to, że istnieje ogromna potrzeba podniesienia kompetencji nauczycieli akademickich z obszaru IT oraz efektywnego zarządzania czasem, a także doposażenia ich w sprzęt umożliwiający efektywną i rzetelną pracę zdalną, jeśli zajdzie taka potrzeba.

Literatura

1. Alexander S. (2001), *E-learning Developments and Experiences*, „Education and Training”, 43, 4/5, s. 240-248.
2. Armstrong L. (2000), *Distance Learning: An Academic Leader's Perspective on a Disruptive Product. Change*, „The Magazine of Higher Learning”, 32, 6, s. 20-27.
3. Hildt-Ciupińska K. (2014), *Work-Life-Balance a wiek pracowników*, „Bezpieczeństwo Pracy. Nauka i Praktyka”, 10, 520, s. 14-17.
4. Greenhouse H.J., Collins M.K., Shaw D.J. (2003), *The Relations Between Work Family Balance and Quality of Life*, „Journal of Vocational Behaviour”, 63, s. 510-531.
5. Jeran A. (2016), *Praca zdalna jako źródło problemów realizacji funkcji pracy*, „Opuscula Sociologica”, 2, s. 41-69.
6. Klimowicz M. (2020), *Polskie uczelnie w czasie pandemii*, Raport projektu SpołTech, Warszawa.
7. *Kodeks pracy* (2021), Wydawnictwo Infor, Warszawa.
8. Koradecka D. (2008), *Bezpieczeństwo i higiena pracy*, CIOP-PIB, Warszawa.
9. Marinoni G., van't Land H., Jensen T. (2020), *The Impact of COVID-19 on Higher Education Around the World*, The International Association of Universities, Paris, https://www.iau-aiu.net/IMG/pdf/iau_covid19_and_he_survey_report_final_may_2020.pdf (dostęp: 12.04.2021).
10. OECD (2018), *International Productivity Gaps: Are Labour Input Measures Comparable?*, „OECD Statistics Working Papers”, https://www.oecd-ilibrary.org/economics/international-productivity-gaps_5b43c728-en (dostęp: 12.04.2021).
11. Romaniuk M.W., Łukasiewicz-Wieleba J., Kohut S. (2020), *Nauczyciele akademicki wobec kryzysowej edukacji zdalnej*, „E-mentor”, 5, 87, s. 15-26.
12. Siwińska B., Łysik J. (2020), *Internacjonalizacja w czasach pandemii*, Fundacja Edukacyjna Perspektywy, Warszawa.
13. Ulewicz R. i in. (2015), *Wybrane aspekty zarządzania bezpieczeństwem i higieną pracy*, Oficyna Wydawnicza SMJiP, Częstochowa.

HEALTH AND SAFETY IMPACT OF REMOTE WORK IN HIGH-RISK CONDITIONS OF ACADEMIC TEACHERS IN THE LIGHT OF WORK-LIFE-BALANCE CONCEPT

Abstract: Recently, remote working has dominated the employee tasks of many professions. It has been a major challenge for many workers who had no previous exposure to it. According to reports and available reports, employees have coped in different ways with the situation and conditions imposed from above and enforced by the COVID-19 pandemic. Also academics have been forced to make big changes, especially in the aspect of teaching working conditions. This chapter explores the impact of remote working in pandemic times on the broader health and safety of academic teachers according to the work-life-balance principle. The research was carried out using an original survey questionnaire among randomly selected academic teachers across Poland via the Internet. The research was voluntary and anonymous. The presented results are part of a larger whole.

Keywords: occupational health and safety, ergonomics, remote working, work-life-balance

Rozdział 12

ROZWÓJ SMART CITIES W POLSCE W KONTEKŚCIE WYKORZYSTANIA ENERGII ODNAWIALNEJ

Wioletta Skrodzka¹⁶

Streszczenie: W rozdziale zaprezentowano koncepcję inteligentnego miasta w kontekście wykorzystania energii odnawialnej. Inwestycje w odnawialne źródła energii są obecnie popularnym kierunkiem transformacji miejskiej. Celem rozdziału jest analiza i ocena poziomu wdrożenia energetyki odnawialnej w przestrzeni miejskiej jako filaru koncepcji Smart City. Zdefiniowano pojęcie „polityka miejska” oraz jej odniesienie do zarządzania energetyką miejską. Omówiono kontekst definicyjny pojęcia „smart cities”. Podkreślono powiązanie koncepcji Smart Cities ze zrównoważonym rozwojem energetyki. Przeanalizowano stopień wykorzystania energetyki odnawialnej w Polsce na tle innych krajów UE. Zaprezentowano przykłady miast – liderów wykorzystujących OZE w przestrzeni miejskiej.

Słowa kluczowe: energia odnawialna, polityka miejska, Smart Cities

Wprowadzenie

W 2020 roku źródła odnawialne wygenerowały 38% energii elektrycznej w UE, wyprzedzając paliwa kopalne i stając się po raz pierwszy w historii głównym źródłem energii w Europie. Współcześnie stanowią one nieodłączny element energetyki zarówno w makro-, jak i mikroskali w instalacjach miejskich oraz prywatnych nieruchomościach. Energetyka odnawialna stanowi dla wielu miast zasób niedostatecznie wykorzystany. Jednak to właśnie miasta są największymi konsumentami energii i w głównej mierze odpowiadają za zanieczyszczenia środowiska, emisję dwutlenku węgla i nieefektywne wykorzystanie zasobów. Mimo iż miasta zajmują tylko 2% powierzchni ziemi, to wytwarzają aż 80% globalnego produktu krajowego brutto na świecie. Równocześnie to właśnie miasta odpowiadają za 60-80% zużycia energii i 75% emisji dwutlenku węgla (International Resource Panel 2018). Chociaż aglomeracje miejskie dysponują dużym potencjałem do transformacji energetycznej, niestety nie wszystkie gminy i samorządy lokalne w jednakowym stopniu reagują zmianami w zakresie wykorzystania energii odnawialnej, efektywności energetycznej czy też elektromobilności (Ziv i in. 2018, s. 487-498). Często barierą jest niemożność dostosowania istniejących systemów zarządzania i wykorzystania dostępnych

¹⁶ Politechnika Częstochowska, Wydział Zarządzania

zasobów energetycznych do innowacyjnych podejść w zakresie produkcji i zużycia energii (Cowell i in. 2017, s. 1139-1155). Czasami jednak przyczyna leży w inercji władz miasta lub niechęci lokalnych mieszkańców do zmian. Miasta wspierające tanie, wydajne i przynoszące duże zyski inicjatywy energetyczne mają przewagę konkurencyjną w globalnej gospodarce. Mogą skuteczniej promować wzrost zatrudnienia i zmniejszać koszty utrzymania infrastruktury. Inteligentna sieć energetyczna, charakteryzująca się wykorzystaniem energetyki odnawialnej, jest jednym z elementów inteligentnego miasta. Występowanie OZE jako elementu energetyki miejskiej poprawia stan środowiska miasta i jednocześnie wpływa pozytywnie na zdrowie i jakość życia mieszkańców. Jest również nieodzownym elementem bezpieczeństwa pozamilitarnego.

W rozdziale skupiono uwagę na prawidłowym zdefiniowaniu pojęcia „polityka miejska” i jej odniesieniu do zarządzania energetyką miejską. Ze względu na wieloaspektowość i złożoność pojęcia „smart cities” omówiono jego kontekst definicyjny. Podkreślono powiązanie koncepcji Smart Cities ze zrównoważonym rozwojem energetyki. Przeanalizowano stopień wykorzystania energetyki odnawialnej w Polsce na tle innych krajów UE. Zaprezentowano ciekawe przykłady miast – liderów wykorzystujących OZE w przestrzeni miejskiej. W gminach wiejskich i na przedmieściach stopień wykorzystania np. paneli fotowoltaicznych na domach jednorodzinnych jest inny niż w przypadku miast. Wynika to głównie z odmiennego typu architektury. Jednak nowo powstające osiedla wielorodzinne coraz częściej wykorzystują energię odnawialną, np. do oświetlenia ulic czy też powierzchni użyteczności wspólnej mieszkańców. Badania ukazały, że polskie miasta mają jeszcze dużo do nadrobienia w stosunku do liderów wykorzystania OZE w Europie.

Koncepcja Smart Cities

Literatura przedmiotu podaje wiele definicji pojęcia „smart city”. R. Giffinger wymienia sześć składników charakteryzujących inteligentne miasto: inteligentna gospodarka (ang. *smart economy*), inteligentni mieszkańcy (ang. *smart people*), inteligentny urząd (ang. *smart governance*), inteligentna mobilność (ang. *smart mobility*), inteligentne środowisko (ang. *smart environment*) oraz inteligentne życie (ang. *smart living*) (Giffinger i in. 2007). B. Cohen analogicznie w swojej definicji określa charakterystyczne gałęzie działalności (Cohen 2012). Dokonuje również klasyfikacji na podstawie stopnia wykorzystania nowoczesnych technologii, wyróżniając trzy rodzaje Smart City (URENIO 2018; Gotlibowska 2018, s. 67-68). Z kolei W. Kurniawati wymienia sześć kluczowych wskaźników wdrażania Smart City (Kurniawati i in. 2019). Natomiast C.F. Calvillo, A. Sánchez-Miralles i J. Villar definiują Smart City jako zrównoważony i wydajny ośrodek zapewniający swoim mieszkańcom wysoką jakość życia i gwarantujący optymalne zarządzanie swoimi zasobami (Calvillo, Sánchez-Miralles, Villar 2016, s. 273-287). Literatura przedmiotu podkreśla często powiązanie z cyfrowym, inteligentnym, wirtualnym miastem, wypuklając charakter technologiczny Smart City (Winkowska, Szpilko Pejic 2019, s. 70-86), zastosowanie inteligentnie działających produktów i usług, sztucznej inteligencji, infrastruktury wyposażonej w mobilne terminale, różnego rodzaju czujniki, akulatory

(Klein, Kaefler 2008; Komninos 2011, s. 172-188; Lee, Phaal, Lee 2013, s. 286-306; Peng, Nunes, Zheng 2017, s. 845-876). Inne definicje zwracają uwagę na infrastrukturę społeczną, kapitał intelektualny tworzący Smart City (Nam, Pardo 2011; Winters 2011, s. 253-270; Bakici, Almirall, Wareham 2013, s. 135-148). Jeszcze inne podkreślają wspólnotowy charakter. Traktują inteligentną społeczność jako wspólnotę członków, organizacji i instytucji zarządzających, które współpracują ze sobą celem realizacji wspólnych celów (Paskaleva i in. 2015; Pereira i in. 2017, s. 526-553). Większość definicji podkreśla dbałość o środowisko jako element koncepcji Smart City: ochrona zielonych zasobów, efektywność energetyczna oraz zrównoważona energetyka miejska (Giffinger i in. 2007; Komninos 2011, s. 119-134; Neirrotti i in. 2017, s. 25-36).

Pomiar oceny miasta jako „smart” jest skomplikowanym zagadnieniem. Mierniki oceny przedstawiło wielu autorów. Uniwersytet Wiedeński utworzył ranking miast średniej wielkości predestynujących do bycia „smart” (Giffinger i in. 2007). Własnym systemem pomiaru dysponuje też Intelligent Community Forum (ICF), które ogłasza ranking miast w ramach Smart21 Communities. Również G.C. Lazaroiu i M. Roscia zaproponowali metodologię oceny i porównania miast w ramach koncepcji Smart City (Lazaroiu, Roscia 2012, s. 326-332). Ciekawą koncepcję wskaźników pomiaru, bazującą na raportach z projektów UE, zbiorze danych z Urban Audit oraz wybranych wskaźnikach ze statystyk Komisji Europejskiej (European Green City Index; TISSUE, Trends and Indicators for Monitoring the EU; Strategia Tematyczna Zrównoważonego Rozwoju Środowiska Miejskiego) przedstawił P. Lombardi i in. (Lombardi i in. 2012, s. 137-149). D. Reckien i in. na podstawie bazy danych Urban Audit porównali 850 miast pod względem ich dostosowania się do zmian klimatu. Ich analiza wykazała, że wielkość miasta, ustawodawstwo krajowe i sieci międzynarodowe mogą wpływać na rozwój lokalnych planów klimatycznych (Reckien i in. 2018). F. Monforti-Ferrario i in. przeanalizowali działania dotyczące łagodzenia zmian klimatycznych w miastach zrzeszonych w ramach inicjatywy Porozumienia Burmistrzów (CoM). Zbudowali wskaźniki pomiaru ich wpływu na poziom zanieczyszczenia powietrza (Monforti-Ferrario i in. 2018, s. 222-234). Interesującą analizę porównawczą wpisującą się w tematykę Smart City i dotyczącą zrównoważonego rozwoju przeprowadziła Ź. Kılıkş (Kılıkş 2018). Wskaźnikiem złożonym był Wskaźnik Zrównoważonego Rozwoju Systemów Energii, Wody i Środowiska (SDEWES City Sustainability Index). Indeks SDEWES jest obecnie stosowany do 120 miast Europy Południowo-Wschodniej.

Opisane definicje i metody pomiaru wskazują na to, jak szeroka może być koncepcja Smart City. Stąd często rozważania naukowe nie są prowadzone w sposób całościowy, a jedynie oceniane są pojedyncze aspekty funkcjonowania miasta.

Polityka miejska

Literatura przedmiotu określa krajową politykę miejską jako celowy proces prowadzony przez rząd, koordynujący i łączący działania wielu podmiotów dla osiągnięcia wspólnego celu urbanizacyjnego w określonym, długoterminowym horyzoncie czasowym (Ryś i in. 2019). Niektórzy autorzy podkreślają, iż jest to

wielopoziomowy, angażujący wiele różnych podmiotów proces skoncentrowany na rozwoju ludzkim, mający na celu transformację obszarów miejskich (Cheshire, Nathan, Overman 2014). Analogiczną definicję przyjmuje Agenda ONZ ds. Osiedli Ludzkich UN-Habitat, promująca rozwój polityk miejskich jako jedno z najważniejszych narzędzi realizacji celów zrównoważonego rozwoju. O ważności tematyki polityki miejskiej świadczy to, iż jest ona rozważana w ramach polityk unijnych w postaci priorytetów wprowadzanych w zakresie europejskiej polityki spójności¹⁷. Polityka miejska jest również elementem bezpieczeństwa pozamilitarnego. Kraje członkowskie UE są zobligowane do przygotowania dokumentu dotyczącego krajowej polityki miejskiej (Szlachta 2013). W Polsce obowiązująca jest *Krajowa Polityka Miejska 2023* (KPM). Została ona przyjęta przez Radę Ministrów jesienią 2015 roku. Obecnie trwa proces jej aktualizacji i integracji ze *Strategią na Rzecz Odpowiedzialnego Rozwoju SOR* oraz powstałymi na poziomie międzynarodowym dokumentami: *Agendą na rzecz Zrównoważonego Rozwoju* (*Agenda...* 2015), *Nową Agendą Miejską ONZ*, *Agendą Miejską dla UE* czy też przyjętą w 2020 roku *Kartą Lipską* i *Agendą Terytorialną*. W kwietniu 2019 roku odbyło się Krajowe Forum Miejskie zorganizowane przez Ministerstwo Funduszy i Polityki Regionalnej (MFIPR) we współpracy z UN-Habitat, podczas którego przedstawiciele samorządu terytorialnego oraz organizacji miejskich sygnowali *Deklarację o współpracy na rzecz realizacji krajowej polityki miejskiej* oraz *Nowej Agendy Miejskiej ONZ*. Można wymienić wiele programów dotyczących obszarów miejskich zaakcentowanych w KPM 2023. Program „Czyste powietrze” jest silnie powiązany z wątkiem „Niskoemisyjność i efektywność energetyczna” KPM 2023. Oferuje on dofinansowanie wymiany starych i nieefektywnych źródeł ciepła na paliwo stałe na nowoczesne i proekologiczne, a także przeprowadzenie towarzyszących temu prac termomodernizacyjnych budynku. Innym przykładem jest konkurs dotacji „Inteligentne miasta współtworzone przez mieszkańców” finansowany w ramach „Programu Operacyjnego Pomoc Techniczna 2014-2020”. Ciekawą inicjatywą jest projekt SOR „Partnerska Inicjatywa Miast”. Jego celem jest promocja współpracy samorządów, wsparcie potencjału rozwojowego mniejszych miast oraz innowacyjnych pilotażowych przedsięwzięć pod patronatem Ministerstwa Funduszy i Polityki Regionalnej. Inną formą działania są Zintegrowane Inwestycje Terytorialne (ZIT) – forma współpracy samorządów współfinansowana ze środków Funduszy Europejskich. Na zasadzie partnerstwa jednostki samorządu terytorialnego miast mogą realizować wspólne cele i przedsięwzięcia finansowane z Europejskiego Funduszu Rozwoju Regionalnego (EFRR) i Europejskiego Funduszu Społecznego (EFS). Komisja Europejska patronuje również w tworzeniu unijnego Porozumienia Burmistrzów na rzecz klimatu i energii, w ramach którego władze lokalne i regionalne prezentują swoje działania na rzecz gospodarki niskoemisyjnej, otrzymują wsparcie, wymieniają dobre praktyki i dzielą się zasobami. Jest to sieć władz lokalnych o najszerszym w tej chwili zasięgu na świecie, obejmującym ponad 8800 miast.

¹⁷ Przykładem jest pakt amsterdamski ustanawiający agendę miejską dla UE, przyjęty przez ministrów państw członkowskich UE ds. rozwoju miast 30 maja 2016 r. w Amsterdamie.

Identyfikując cele polityki miejskiej, należy uwzględnić nie tylko procesy urbanizacji, nierówności ekonomiczne występujące pomiędzy miastami lub poszczególnymi obszarami miejskimi, ale również problematykę kongestii centrów miejskich, jakości życia mieszkańców, dostępności mieszkalnictwa oraz skutków związanych z nieodpowiednim zagospodarowaniem przestrzeni miejskiej czy zanieczyszczenia środowiska. W czasach kryzysu klimatycznego, który niesie szereg wyzwań środowiskowych, to właśnie miasta, ich sposób gospodarowania oraz zarządzanie procesami urbanizacyjnymi mają istotne znaczenie dla ograniczenia negatywnego oddziaływania człowieka na środowisko. Zwartość przestrzeni miejskiej i koncentracja osadnicza pozwalają wdrożyć szereg rozwiązań zmniejszających poziom antropopresji w sposób znacznie bardziej efektywny niż w przypadku osadnictwa rozproszonego. Większe wykorzystanie energii odnawialnej, zrównoważona mobilność, tworzenie infrastruktury miejskiej o niemal zerowym zużyciu energii i budynków neutralnych pod względem wykorzystania paliw kopalnych przyczynią się do znaczącej redukcji emisji gazów cieplarnianych i zwiększenia efektywności energetycznej.

Kompetencje miasta a zrównoważona energetyka

Gmina miejska może występować w roli regulatora lokalnego rynku energii, odbiorcy bądź dostawcy energii, ale również jako inwestor lub wytwórca energii (Swora 2019, s. 235). Na mocy artykułu 18 Ustawy z dnia 10 kwietnia 1997 r. *Prawo energetyczne* do zadań gminy w zakresie energetyki należy m.in. planowanie i organizacja zaopatrzenia w ciepło, energię elektryczną i paliwa gazowe w gminie oraz procesu racjonalizacji zużycia energii, a także promowanie rozwiązań zmniejszających zużycie energii. Jest to działalność pozostająca w sferze zadań własnych o charakterze użyteczności publicznej z obszaru zaopatrzenia w energię elektryczną. Gmina może być wytwórcą energii elektrycznej z OZE na mocy uczestnika klastra energii, członka spółdzielni energetycznej lub w sposób pośredni przez przedsiębiorstwo energetyczne będące producentem energii odnawialnej (Kosiński, Trupkiewicz 2016, s. 106).

Klastry energii i spółdzielnie energetyczne

Prawodawstwo UE przewiduje występowanie podmiotów, które można określić społecznościami energetycznymi. Ich koncepcję działania różnicuje prawodawstwo, na którym są oparte. Przede wszystkim należy wymienić działającą w obszarze energii odnawialnej społeczność energetyczną wprowadzoną dyrektywą o wsparciu energii ze źródeł odnawialnych (REDII 2018). Innym rodzajem jest działająca na podstawie dyrektywy rynkowej (Dyrektywa rynkowa 2019) obywatelska społeczność energetyczna (CEC – *Citizens Energy Community*). Odmiennym pod względem działania podmiotem są działający grupowo prosumenci energii elektrycznej (REDII 2018).

Prawodawstwo polskie definiuje dwie formy: klastry energii oraz spółdzielnie energetyczne, które zdefiniowano prawnie w połowie 2016 roku. Nowelizacja

ustawy OZE z dnia 19 lipca 2019 roku (Dz.U. 2019 poz. 1524) doprecyzowała szczegółowo funkcjonowanie tych podmiotów. Ustawa OZE definiuje pojęcie „klastra energii” jako cywilno-prawne porozumienie, w którego skład mogą wchodzić: osoby fizyczne, osoby prawne, jednostki naukowe lub jednostki samorządu terytorialnego. Ustawa określa również cel działalności. Jest nim wytwarzanie i równoważenie zapotrzebowania dystrybucji lub obrót energią z odnawialnych źródeł lub innych w ramach sieci dystrybucyjnej o napięciu znamionowym niższym niż 110 kV na obszarze nieprzekraczającym granic jednego powiatu lub 5 gmin w rozumieniu ustawy o samorządzie gminnym (Szyrski 2017). Udział podmiotów naukowych i ze świata gospodarczego zwiększa produktywność, innowacyjność i przedsiębiorczość. Szansa powodzenia biznesowego jest dużo większa. Natomiast udział władz lokalnych w klastrze energii wpływa pozytywnie na odbiór społeczny tego typu przedsięwzięć. Jako uczestnik klastra gmina może partycypować, wykorzystując własne nieruchomości do wytwarzania energii odnawialnej.

W przeciwieństwie do klastra energii spółdzielnie energetyczne są zakładane po to, aby wyprodukowana w ich ramach energia zaspokoiła indywidualne zapotrzebowanie podmiotów wchodzących w jej skład. Klaster ma charakter biznesowy, podczas gdy spółdzielnia wytwarza energię tylko na rzecz jej członków. Podstawową różnicą pomiędzy klastrami a spółdzielniami energetycznymi jest posiadanie przez spółdzielnie osobowości prawnej. Ustawowa definicja spółdzielni energetycznej zawarta w art. 2 pkt 33a ustawy o OZE bazuje na Ustawie z dnia 16 września 1982 r. *Prawo spółdzielcze*. Warunki, które musi spełniać spółdzielnia, wymienione są m.in. w art. 38e ustawy o OZE. Precyzują one, iż liczba jej członków nie może przekraczać 1000, a łączna moc zainstalowana elektryczna wszystkich instalacji odnawialnego źródła energii, należących do członków spółdzielni, musi umożliwiać pokrycie nie mniej niż 70% rocznego zapotrzebowania na energię elektryczną wszystkich członków tej spółdzielni. Sprawdzona w innych obszarach działania formuła spółdzielni jest atrakcyjna dla nowych członków. Wadą tej formy działalności jest ograniczenie terenowe w stosunku do klastrów energii. Zapisy unijne, szczególnie te dla obywatelskiej społeczności energetycznej, w dużym stopniu korespondują z definicją klastra energii w prawodawstwie polskim, natomiast dla społeczności działających w zakresie OZE z zapisami o spółdzielniach energetycznych.

Udział miasta w rozwoju spółdzielni energetycznych czy też klastrów energii umożliwia włączenie się lokalnych mieszkańców w produkcję energii odnawialnej oraz wykorzystanie jej do własnych celów. Tego typu dywersyfikacja źródeł energii poprawia efektywność energetyczną poprzez zmniejszenie strat sieciowych i przyczynia się do zachowania bezpieczeństwa energetycznego kraju. Wszystkie te elementy wpisują się w koncepcję Smart City.

Udział energii odnawialnej w strukturze produkcji energii pierwotnej

Ostatnie lata przyniosły wiele unijnych aktów prawnych dotyczących promowania odnawialnych źródeł energii. Zgodnie z celem przyjętym w 2009 roku zużycie energii do roku 2020 miało w 20% pochodzić ze źródeł odnawialnych (Dyrektywa

2009/28/WE). W 2018 roku zmieniono ten cel na 32% w 2030 roku (Dyrektywa (UE) 2018/2001). Ostatnie dokumenty z 11 grudnia 2019 roku (*Europejski Zielony Ład*) określają Europę jako neutralną dla klimatu do 2050 roku (KE 2019). Zrównoważony rozwój energetyki odgrywa ważną rolę w strategii UE i przekłada się na wymiar polityk miejskich. W europejskiej strategii zrównoważonego rozwoju jest reprezentowany przez cel 7 i monitorowany przy użyciu wskaźników służących ocenie stopnia osiągnięcia przez poszczególne kraje założonych celów polityki: energetycznej, klimatycznej i ekologicznej.

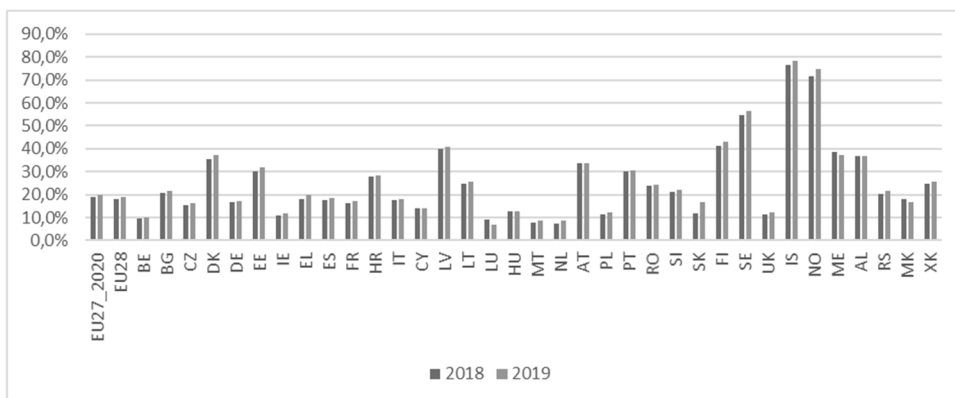
W literaturze przedmiotu można odnaleźć wiele wskaźników monitorujących zrównoważony rozwój: wskaźniki IAEA, wskaźniki Eurostatu oraz wskaźniki GUS. Wskaźniki IAEA podzielone są na trzy wymiary: społeczny, gospodarczy i środowiskowy (IAEA 2005). Obejmują one kompleksowo problematykę zrównoważonego rozwoju energii. Baza Eurostatu również zawiera listę wskaźników zrównoważonego rozwoju (SDG). Cel nr 7 w ramach tej listy obejmuje tematykę powszechnego dostępu do nowoczesnych usług energetycznych, poprawy efektywności energetycznej i zwiększenia udziału energii odnawialnej. W jego ramach wyodrębniono m.in. następujące wskaźniki: emisje gazów cieplarnianych, zużycie energii pierwotnej, wydajność energetyczna, zależność od importu energii według produktów, udział energii odnawialnej w ostatecznym zużyciu energii brutto. Polska baza GUS również zawiera wskaźniki monitorujące realizację celów zrównoważonego rozwoju w zakresie energii: odsetek ludności z dostępem do elektryczności, odsetek ludności wykorzystującej podstawowo czyste paliwa i technologie, udział energii ze źródeł odnawialnych w końcowym zużyciu energii brutto, energochłonność pierwotna, oficjalna pomoc rozwojowa na rzecz mitygacji i adaptacji do zmian klimatu. Różnorodność wskaźników umożliwia monitorowanie krajowego procesu rozwoju zrównoważonej energetyki. Niestety nie wszystkie dane występują na poziomie gmin lub powiatów, co zdecydowanie utrudnia monitoring w ramach problematyki Smart City.

Jednym z głównych wskaźników w obszarze monitorowania zmian klimatu i energii jest udział energii ze źródeł odnawialnych w końcowym zużyciu energii brutto. Wskaźnik ten informuje, jaki jest stopień wykorzystania energii pochodzącej z OZE w zużyciu końcowym energii w kraju. Rysunek 12.1 prezentuje udziały procentowe dla poszczególnych krajów europejskich w latach 2018-2019.

W 2018 roku produkcja energii ze źródeł odnawialnych w UE wynosiła 81 mln toe¹⁸ i stanowiła 18,9% w zużyciu energii końcowej brutto. W 2019 roku wynosiła 84,6 mln toe i stanowiła 19,7%. Do podstawowych źródeł energii odnawialnej w 2019 roku należały: energia wiatrowa (30 mln toe), energia wodna (29,5 mln toe), energia słoneczna (10,8 mln toe). W 2019 roku największe udziały energii ze źródeł odnawialnych w zużyciu energii końcowej brutto odnotowano w Islandii (78,2%), Norwegii (74,6%), Szwecji (56,4%), Finlandii (43,1%) i Łotwie (41%). Najniższe w Luksemburgu (7%), Malcie (8,5%), Holandii (8,8%) i Belgii (9,9%). W 2019 roku krajowe cele OZE na 2020 rok wypełniło 14 państw Unii Europejskiej. Najdalej od zrealizowania celów były: Francja (brak 5,8 pkt proc.), Holandia (5,2 pkt proc.) oraz Luksemburg (4 pkt proc.). Polska w 2019 roku osiągnęła 12,2% udziału zielonej

¹⁸ Ton oleju ekwiwalentnego – toe.

energii wobec poziomu 11,5% w 2018 roku. W Polsce w 2020 roku moc zainstalowana wszystkich odnawialnych źródeł energii w systemie elektroenergetycznym wynosiła prawie 10 GW, z czego poniżej 2% pochodziło z małych instalacji OZE¹⁹. W porównaniu z 2019 rokiem nastąpił wzrost o 33% instalacji wykorzystujących energię promieniowania słonecznego (PV). Przyrost mocy zainstalowanej w tym sektorze wyniósł prawie 41% (URE 2020). Tabela 12.1 prezentuje strukturę instalacji OZE w 2020 roku ze względu na źródło.



Rysunek 12.1. Calkowity udzial energii ze źródeł odnawialnych w końcowym zużyciu energii brutto w latach 2018-2019 (%)

Źródło: opracowanie własne na podstawie danych z GUS

Tabela 12.1. Struktura OZE w Polsce w 2020 r.

Rodzaj instalacji OZE ze względu na źródło:	Liczba instalacji	Moc zainstalowana (MW)
Hydroenergia (WO)	343	51,96
Energia promieniowania słonecznego (PV)	328	66,86
Biogaz (BG)	117	32,10
Energia wiatrowa (WI)	108	31,71
Biomasa (BM)	2	0,47
Łącznie	898	183,10

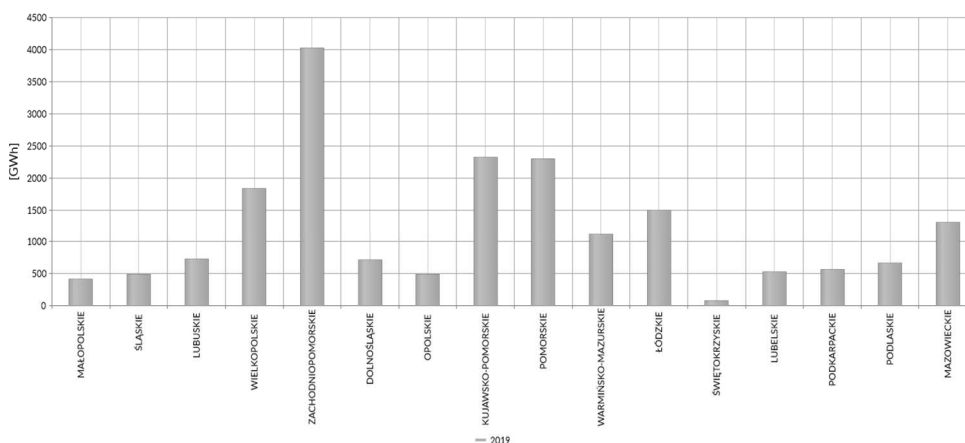
Źródło: (URE 2020)

W 2020 roku działały w Polsce 343 instalacje wykorzystujące energię wody o łącznej mocy zainstalowanej 51,96 MW. Największe pod względem łącznej mocy zainstalowanej równej 66,86 MW były źródła fotowoltaiczne w liczbie 328

¹⁹ Instalacje o łącznej mocy zainstalowanej elektrycznej większej niż 50 kW i mniejszej niż 500 kW, przyłączone do sieci elektroenergetycznej o napięciu znamionowym niższym niż 110 kV albo o mocy osiągalnej cieplnej w skojarzeniu większej niż 150 kW i nie większej niż 900 kW, w której łączna moc zainstalowana elektryczna jest większa niż 50 kW i mniejsza niż 500 kW.

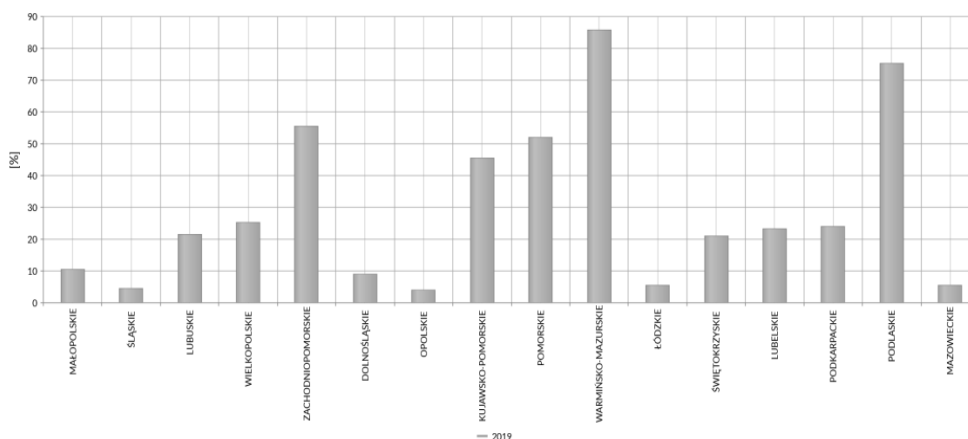
instalacji. Małe instalacje produkujące energię z biomasy były tylko dwie. Dane dotyczące instalacji OZE w podziale na województwa występują obecnie tylko dla 2019 roku (GUS). Rysunek 12.2 prezentuje wielkość produkcji energii w GWh w 2019 roku w elektrowniach wodnych (szczytowo-pompowych oraz przepływowych), wiatrowych oraz ciepłych zużywających wyłącznie paliwa odnawialne (biomasę, biogaz, biopaliwa).

Najwięcej energii odnawialnej (4024 GWh) wyprodukowano w 2019 roku w województwie zachodniopomorskim. Kolejne miejsca zajmują: województwo kujawsko-pomorskie (2323 GWh) i pomorskie (2 300,4 GWh). Najmniej energii odnawialnej produkowano w województwie świętokrzyskim (80,4 GWh). Procentowy udział energii odnawialnej w produkcji energii elektrycznej ogółem w poszczególnych województwach w 2019 roku prezentuje rysunek 12.3.



Rysunek 12.2. Elektrownie wodne i na paliwa odnawialne z podziałem na województwa

Źródło: opracowanie na podstawie danych z GUS



Rysunek 12.3. Udział energii odnawialnej w produkcji energii elektrycznej ogółem w 2019 r. z podziałem na województwa

Źródło: opracowanie własne na podstawie danych z GUS

W 2019 roku najwyższy udział (85,7%) energii odnawialnej w produkcji energii elektrycznej ogółem zaobserwowano w województwie warmińsko-mazurskim, zaś najniższy (4%) w województwie opolskim.

W ostatnich latach miasta na całym świecie podejmowały działania mające na celu przyspieszenie globalnego wykorzystania odnawialnych źródeł energii. Władze miast bezpośrednio wspierały je poprzez ustalanie konkretnych celów w zakresie energii odnawialnej, inwestowanie w odnawialne źródła energii i uchwalanie polityk promujących odnawialne źródła energii w całym mieście. Do końca 2020 roku władze co najmniej 834 miast w 72 krajach, obejmujących 558 milionów ludzi, ustaliło cele w zakresie energii odnawialnej w co najmniej jednym sektorze (energetyka, ciepłownictwo, chłodzenie, transport). W 617 miastach za cel postawiono sobie 100-procentowe pochodzenie energii ze źródeł odnawialnych (REC 2021). Często cele miast i ich lokalna polityka w zakresie zrównoważonej energii jest dużo bardziej ambitna niż polityka danego państwa. Tabela 12.2 prezentuje miasta europejskie o wysokim udziale wytwarzania energii elektrycznej z fotowoltaiki i elektrowni wiatrowych w 2019 roku.

Tabela 12.2. Miasta europejskie o wysokim udziale wytwarzania energii elektrycznej z fotowoltaiki i elektrowni wiatrowych w 2019 r.

Państwo	Miasto	Populacja	Udział energetyki słonecznej i wiatrowej w produkcji energii elektrycznej (%)	Udział energetyki odnawialnej* w produkcji energii elektrycznej (%)	Cele w zakresie energii odnawialnej i redukcji emisji
Dania	Gładsaxe	69 681	52%	77%	100% udział energii odnawialnej do roku 2035
Francja	Paryż	2 161 000	7%	21%	Neutralność węglowa i 100% udział energii odnawialnej do roku 2050
Niemcy	Berlin	3 644 826	1%	3%	Neutralność węglowa i 25% udział energii solarnej do roku 2050
Niemcy	Hamburg	1 841 179	15%	30%	100% udział energii odnawialnej do roku 2035; 55% redukcja emisji do roku 2030 (w porównaniu do roku 1990); neutralność węglowa do roku 2050

Hiszpania	Barcelona	4 588 000	7%	18%	45% redukcja emisji do roku 2030 (w porównaniu do roku 2005); neutralność węglowa do roku 2050
Hiszpania	Madryt	3 223 000	24%	41%	Brak danych
Hiszpania	Saragossa	649 404	8%	14%	Brak danych
Szwecja	Hyllie	32 998	Brak danych	Brak danych	100% udział energii odnawialnej lub pochodzącej z recyklingu** do roku 2030
Szwecja	Örebro	155 989	100%	100%	Neutralność węglowa do roku 2050
Wielka Brytania	Birmingham	1 149 000	21%	33%	60% redukcja emisji do 2027 (w porównaniu do roku 1990); krajowa neutralność węglowa do roku 2050
Wielka Brytania	Londyn	9 304 000	21%	23%	1 GW energii solarnej do roku 2030 i 2 GW energii solarnej do roku 2050; krajowa neutralność węglowa do roku 2050
Wielka Brytania	Manchester	547 627	6%	13%	Neutralność węglowa do roku 2038

*Obejmuje energię słoneczną, wiatrową, biomasę, geotermalną i wodną

** Energia pochodząca z recyklingu odpadów i ścieków do wytwarzania ciepła, energii elektrycznej i biogazu

Źródło: opracowanie własne na podstawie (REC 2021)

Poza umieszczonymi w tabeli liderami wiele innych miast europejskich inwestuje w energetykę odnawialną. Na przykład miasto Dniepr na Ukrainie w 2019 roku oddało do użytku 16 MW bioelektrownię. W Glasgow w Szkocji powstał zakład fermentacji beztlenowej, w którym przekształca się organiczne odpady składowiskowe na metan do produkcji energii elektrycznej. W Exeter w Anglii w 2020 roku powstał projekt solarny składający się z naziemnego panelu słonecznego o mocy 1,2 MW połączonego z magazynem energii w postaci baterii 1 MW/2 MWh. Również Ateny w Grecji uruchamiają od 2020 roku instalację systemów fotowoltaicznych w 50 szkołach na pokrycie potrzeb elektrycznych w instytucjach publicznych.

Kowno na Litwie planuje instalację systemów na 77 budynkach miejskich, w tym szkołach i zakładach opieki zdrowotnej. Również polskie miasta inwestują w energetykę odnawialną. Tychy w celu poprawy lokalnej jakości powietrza i obniżenia kosztów energii realizują plan dodania do końca roku 2021 setek odnawialnych systemów energetycznych, w tym 647 systemów fotowoltaicznych. We Wrocławiu na dachach 35 wieżowców w centrum miasta powstaje Wrocławska Elektrownia Słoneczna. Obejmuje ona 2771 modułów fotowoltaicznych o łącznej mocy 739 kWp. Powstała energia będzie wykorzystywana do zasilania części wspólnych budynków, a nadwyżki będą trafiać do sieci i będą rozliczane w ramach systemu opustów, pomniejszając rachunki za prąd pobierany od usługodawcy (*Zielone miasta... 2021*).

Posumowanie

Miasta mogą odegrać kluczową rolę w zakresie ochrony klimatu i promocji energii odnawialnej. *Agenda Miejska*, dokument przyjęty w 2016 roku na międzynarodowej konferencji w Ekwadorze, zawiera zasady promujące wizję zrównoważonego rozwoju na szczeblu lokalnym. Służą temu dobre praktyki czy platformy wymiany doświadczeń między miastami. Przykładem jest Porozumienie Burmistrzów, deklarujące redukcję emisji gazów cieplarnianych, różnego rodzaju standardy i certyfikacje pokroju normy ISO 37210, czy też projekt Eco-Miasto, zapoczątkowany przez Ambasadę Francji w 2013 roku. Oczekiwane trendy rozwoju gospodarczego wskazują na to, że w nadchodzących latach zużycie energii elektrycznej w miastach wzrośnie, co przyczyni się do zmiany profili podaży i popytu na energię. Rosnące zapotrzebowanie na energię elektryczną, przy równoczesnej konieczności realizacji celów klimatycznych, wymusi ewolucję infrastruktury energetycznej. Będzie musiała ona sprostać coraz większym dostawom odnawialnej energii elektrycznej. Celem ograniczenia strat w transporcie i dystrybucji energii elektrycznej, a także potencjalnym ograniczeniom inwestycji w infrastrukturę sieciową, wytwarzanie energii elektrycznej ze źródeł odnawialnych na miejscu w mieście stanie się koniecznością.

W rozdziale zaprezentowano koncepcję inteligentnego miasta w kontekście wykorzystania energii odnawialnej. Celem rozdziału była analiza i ocena poziomu wdrożenia energetyki odnawialnej w przestrzeni miejskiej jako filaru koncepcji Smart City. Zdefiniowano pojęcie „polityka miejska” i jej odniesienie do zarządzania energetyką miejską. Omówiono kontekst definicyjny pojęcia „smart cities”. Podkreślono powiązanie koncepcji Smart Cities ze zrównoważonym rozwojem energetyki. Przeanalizowano stopień wykorzystania energetyki odnawialnej w Polsce na tle innych krajów UE. Zaprezentowano ciekawe przykłady miast – liderów wykorzystujących OZE w przestrzeni miejskiej. Przeprowadzone badania wykazały, że zarządzanie inteligentnym miastem jest procesem niezwykle złożonym i musi uwzględnić wiele aspektów. Dotyczy nie tylko kwestii techniczno-infrastrukturalnych, ale rozszerza się o zakres społeczny, środowiskowy i ekonomiczny. Muszą one zostać połączone z technicznymi w jeden wspólnie działający system polityki miejskiej. Polskie miasta aspirują do bycia „smart”. Jednak ich droga do osiągnięcia

wyników europejskich miast liderów jest jeszcze odległa. Do najważniejszych wyzwań stojących przed polskimi miastami, które planują implementację koncepcji Smart City, należy m.in. szersze wykorzystanie najnowszych technologii do poprawy funkcjonowania miasta, zapewnienie właściwego poziomu jakości życia mieszkańców, ale przede wszystkim szeroko zakrojoną poprawę stanu środowiska naturalnego poprzez większe wykorzystanie energii odnawialnej i zmniejszenie śladu węglowego.

Literatura

1. *Agenda 2030* (2015), <http://www.un.org.pl/agenda-2030-rezolucja> (10.09.2021).
2. Bakici T., Almirall E., Wareham J. (2013), *A Smart City Initiative: The Case of Barcelona*, „Journal of the Knowledge Economy”, 4, 2, s. 135-148.
3. Calvillo C.F., Sánchez-Mirallas A., Villar J. (2016), *Energy Management and Planning in Smart Cities*, „Renewable and Sustainable Energy Reviews”, 55, s. 273-287.
4. Cheshire P.C., Nathan M., Overman H.G. (2014), *Urban Economics and Urban Policy. Challenging Conventional Policy Wisdom*, Edward Elgar, Cheltenham, Northampton.
5. Cohen B. (2012), *What Exactly is a Smart City?*, <http://www.fastcoexist.com/1680538/what-exactly-is-a-smart-city> (19.08.2021).
6. Cowell R. i in. (2017), *Sub-national Government and Pathways to Sustainable Energy*, „Environment and Planning C: Politics and Space”, 35, 7, s. 1139-1155.
7. Dyrektywa Parlamentu Europejskiego i Rady 2009/28/WE z dnia 23 kwietnia 2009 r. w sprawie promowania stosowania energii ze źródeł odnawialnych zmieniająca i w następstwie uchylająca dyrektywy 2001/77/WE oraz 2003/30/WE (Dz.Urz. UE L 140/16 z 05.06.2009).
8. Dyrektywa rynkowa (2019) – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/944 z dnia 5 czerwca 2019 r. w sprawie wspólnych zasad rynku wewnętrznego energii elektrycznej oraz zmieniająca dyrektywę 2012/27/UE (Dz.Urz. UE L 158/125 z 14.06.2019).
9. KE (2019), *Europejski Zielony Ład* (COM(2019)0640).
10. Giffinger R. i in. (2007), *Smart Cities. Ranking of European Medium-Sized Cities*, http://www.smart-cities.eu/download/smart_cities_final_report.pdf (23.08.2021).
11. Gotlibowska K. (2018), *Propozycja modelu miasta inteligentnego (Smart City) opartego na zastosowaniu technologii informacyjno-komunikacyjnych w jego rozwoju*, „Rozwój Regionalny i Polityka Regionalna”, 42, s. 67-80.
12. GUS, Wskaźniki zrównoważonego rozwoju, sdg.gov.pl/affordable-and-clean-energy/ (dostęp: 13.07.2021).
13. IAEA (2005), *Energy Indicators*, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1222_web.pdf (dostęp: 13.07.2021).
14. International Resource Panel (2018), *The Weight of Cities: Resource Requirements of Future Urbanization*, United Nations Environment Programme, Nairobi, Kenya.
15. Ministerstwo Funduszy i Polityki Regionalnej (2021), *Nowa Karta Lipska i Agenda Terytorialna UE 2030 przyjęte przez ministrów krajów wspólnoty europejskiej*, <https://www.gov.pl/web/fundusze-regiony/nowa-karta-lipska-i-agenda-terytorialna-ue-2030-przyjete-przez-ministrow-krajow-wspolnoty-europejskiej> (dostęp: 14.09.2021).
16. Kılış Ş. (2018), *Benchmarking South East European Cities with the Sustainable Development of Energy. Water and Environment Systems Index*, „Journal of Sustainable Development of Energy, Water and Environment Systems”, 6, 1, s. 162-209.
17. Klein C., Kaefer G. (2008), *From Smart Homes to Smart Cities: Opportunities and Challenges from an Industrial Perspective*, Proceedings of the 8th International Conference, NEW2AN and 1st Russian Conference on Smart Spaces „SMART 2008” St. Petersburg, Russia, Sep 3-5.

18. Komninos N. (2011), *Intelligent Cities: Variable Geometries of Spatial Intelligence*, „Intelligent Buildings International”, 3, 3, s. 172-188.
19. Komninos N., Pallot M., Schaffers H. (2013), *Smart Cities and the Future Internet in Europe*, „Journal of the Knowledge Economy”, 4, 2, s. 119-134.
20. Kosiński E., Trupkiewicz M. (2016), *Gmina jako podmiot systemu wspierania wytwarzania energii elektrycznej z Odnawialnych Źródeł Energii*, „Ruch, Prawniczy, Ekonomiczny i Socjologiczny”, 3, s. 93-107.
21. Krajowa Polityka Miejska (2021), <https://www.gov.pl/web/fundusze-regiony/polityka-miejska> (19.08.2021).
22. Kurniawati W. i in. (2019), *Local Wisdom in Malay Kampung Semarang as Representatives of Smart Environment*, IOP Conference Series: Earth and Environmental Science, 396(1).
23. Lazaroiu G.C., Roscia M. (2012), *Definition Methodology for the Smart Cities Model*, „Energy”, 47, 1, s. 326-332.
24. Lee J.H., Phaal R., Lee S. (2013), *An Integrated Service-Device-Technology Roadmap for Smart City Development*, „Technological Forecasting and Social Change”, 80, 2, s. 286-306.
25. Lombardi P. i in. (2012), *Modelling the Smart City Performance*, „Innovation: The European Journal of Social Science Research”, 25, 2, s. 137-149.
26. Monforti-Ferrario F. i in. (2018), *The Impact On Air Quality of Energy Saving Measures in the Major Cities Signatories of the Covenant of Mayors Initiative*, „Environment International”, 118, s. 222-234.
27. Nam T., Pardo T.A. (2011), *Conceptualizing Smart City with Dimensions of Technology, People, and Institutions*, The Proceedings of the 12th Annual International Conference on Digital Government Research, s. 282-291.
28. Neirrotti P. i in. (2014), *Current Trends in Smart City Initiatives: Some Stylised Facts*, „Cities”, 38, s. 25-36.
29. Paskaleva K. i in. (2015), *Stakeholder Engagement in the Smart City: Making Living Labs Work*, [w:] Rodríguez-Bolívar M. (red.), *Transforming City Governments for Successful Smart Cities*, s. 115-145, Public Administration and Information Technology, Springer International Publishing, Cham.
30. Peng G.C.A., Nunes M.B., Zheng L. (2017), *Impacts of Low Citizen Awareness and Usage in Smart City Services: The Case of London's Smart Parking System*, „Information Systems and e-Business Management”, 15, 4, s. 845-876.
31. Pereira G.V. i in. (2017), *Increasing Collaboration and Participation in Smart City Governance: A Cross-Case Analysis Of Smart City Initiatives*, „Information Technology for Development”, 23, 3, s. 526-553.
32. *Prawo energetyczne* (Dz.Urz. 2019 poz. 755 i 730).
33. *Prawo spółdzielcze* (Dz.Urz. 2018 poz. 1285).
34. REN (2021), *Renewables in Cities Global Status Report*, <https://www.ren21.net/reports/cities-global-status-report/> (dostęp: 23.08.2021).
35. Reckien D. i in. (2018), *How are Cities Planning to Respond to Climate Change? Assessment of Local Climate Plans from 885 Cities in the EU-28*, „Journal of Cleaner Production”, 191, s. 207-219.
36. REDII (2018) – Dyrektywa Parlamentu Europejskiego i Rady UE 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych (Dz.Urz. UE L 328/82 z 21.12.2018).
37. Ryś R. i in. (2020), *Wyzwania i rekomendacje dla krajowej polityki miejskiej*, Instytut Rozwoju Miast i Regionów, Warszawa, Kraków.
38. Smart21 Communities, <https://www.intelligentcommunity.org/smart21> (dostęp: 14.08.2021)
39. *Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*, <https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju> (dostęp:14.08.2021).

40. Swora M. (2018), *Działalność przedsiębiorstw energetycznych (wybrane obowiązki)*, [w:] Hauser R., Niewiadomski Z., Wróbel A. (red.), *System prawa administracyjnego. Publiczne prawo gospodarcze*, t. 8b, C.H. Beck, Warszawa.
41. Szlachta J. (2013), *Europejski wymiar polityki miejskiej w Polsce*, „Studia KPZK PAN”, 153, s. 24-42.
42. Szyrski M. (2017), *Rola samorządu terytorialnego w rozwoju odnawialnych źródeł energii*, Wolters Kluwer, Warszawa.
43. TISSUE (2007), *Trends and Indicators for Monitoring the EU*, <https://www.vttresearch.com/sites/default/files/pdf/publications/2007/P643.pdf> (dostęp: 14.08.2021).
44. URE (2020), *Raport 2020 – Zbiornicze informacje dotyczące wytwarzania energii elektrycznej z odnawialnych źródeł energii w małej instalacji*, <https://bip.ure.gov.pl/bip/o-urzedzie/zadania-prezesa-ure/raport-oze-art-17-ustaw/3556.Raport-zbiornicze-informacje-dotyczace-wytwarzania-energii-elektrycznej-z-odnawial.html> (dostęp: 20.08.2021).
45. URENIO (2018), *The 3 Generations of Smart Cities*, <http://www.urenio.org/2015/08/25/the-3-generations-of-smart-cities> (dostęp: 19.08.2021).
46. Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy o odnawialnych źródłach energii oraz niektórych innych ustaw (Dz.U. 2019 poz. 1524).
47. Winkowska J., Szpilko D., Pejic S. (2019), *Smart City Concept in the Light of the Literature Review*, „Engineering Management in Production and Services”, 11, 2, s. 70-86.
48. Winters J.V. (2011), *Why Are Smart Cities Growing? Who Moves and Who Stays*, „Journal of Regional Science”, 51, 2, s. 253-270.
49. *Zielone miasta i gminy. Raport 2021*, <https://www.innogy.pl/pl/duze-przedsiębiorstwa/raport-zielone-miasta-i-gminy> (dostęp: 12.08.2021).
50. Ziv G. i in. (2018), *The Potential Impact of Brexit on the Energy, Water and Food Nexus in the UK: A Fuzzy Cognitive Mapping Approach*, „Applied Energy”, 210, s. 487-498.

THE DEVELOPMENT OF SMART CITIES IN POLAND IN THE CONTEXT OF THE USE OF RENEWABLE ENERGY

Abstract: The chapter presents the concept of a smart city in the context of the use of renewable energy. Investments in renewable energy sources are currently a popular direction of urban transformation. The aim of the chapter is to analyze and assess the level of implementation of renewable energy in urban space as a pillar of the smart city concept. The chapter defines the concept of urban policy and its reference to municipal energy management. The definition context of the concept of smart cities was discussed. The link between the smart cities concept and sustainable energy development was emphasized. The degree of use of renewable energy in Poland was analyzed in comparison to other EU countries. Examples of cities-leaders using renewable energy in urban space are presented.

Keywords: renewable energy, urban policy, smart cities

V

**Bezpieczeństwo ideologiczne,
kulturowe i religijne**

Rozdział 13

BEZPIECZEŃSTWO IDEOLOGICZNE W POLSKIEJ PRZESTRZENI NAUKOWO-BADAWCZEJ NA TLE TEORII SEKURYZACJI

Paweł Łubiński²⁰

Streszczenie: Celem niniejszego rozdziału jest próba zdefiniowania, wskazania istoty i miejsca bezpieczeństwa ideologicznego jako samodzielnego wariantu bezpieczeństwa narodowego (państwa) na tle teorii sekuryzacji, która w znaczny sposób przyczyniła się do poszerzenia rozumienia bezpieczeństwa oraz katalogu jego zagrożeń. Niniejsza analiza dotyczyła będzie polskiej przestrzeni naukowo-badawczej z niezbędnym odniesieniem do podstaw teoretycznych szkoły kopenhaskiej rozwijającej teorię sekuryzacji. Poruszone zostaną zagadnienia sekuryzacji uwarunkowań i zagrożeń o charakterze ideologiczno-politycznym w nawiązaniu do teorii sektorów bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo ideologiczne, szkoła kopenhaska, teoria bezpieczeństwa, teoria sekuryzacji

Wprowadzenie

Bezpieczeństwo, wraz z powstaniem dyscypliny nauk o bezpieczeństwie²¹ w polskiej przestrzeni naukowo-badawczej, urosło do rangi zagadnienia niezwykle ważkiego, szeroko podejmowanego przez badaczy i analityków z dziedziny nauk społecznych. Przez ponad dekadę swojej obecności na arenie naukowej w Polsce nauki o bezpieczeństwie doczekały się wielu częściowych badań oraz zwartych opracowań i analiz z pogranicza teorii i praktyki funkcjonowania różnorodnych podmiotów bezpieczeństwa – jednostek, społeczeństw, narodów, państw czy struktur ponadpaństwowych. Choć przedmiotowe ujęcie bezpieczeństwa jako kategorii semantycznej zostało w polskiej literaturze skrupulatnie opisane, to jego typologia pozostawia pewną furtkę otwartą na nowe jego rodzaje i płaszczyzny. Nie bez znaczenia są tu interdyscyplinarność i konwergencja badań podejmowanych w obrębie nauk społecznych, które sprawiają, że wspomniane płaszczyzny poszerzają swoje ramy

²⁰ Uniwersytet Pedagogiczny im. KEN w Krakowie, Instytut Nauk o Bezpieczeństwie

²¹ Zgodnie z uchwałą Centralnej Komisji do Spraw Stopni i Tytułów z dnia 28 stycznia 2011 r. zmieniającą uchwałę w sprawie określenia dziedzin nauki i dziedzin sztuki oraz dyscyplin naukowych i artystycznych (M.P. 2011 nr 14 poz. 149).

znaczeniowe. We współczesnych realiach, pełnych nowych i nieoczywistych zagrożeń o charakterze hybrydowym, bezpieczeństwo również rozszerza swoje granice o kolejne sfery wymagające ochrony. Biorąc pod uwagę ochronę przed szeregiem zagrożeń o podłożu ideologicznym, tytułowe bezpieczeństwo ideologiczne nie wydaje się jednak kategorią nową, a mimo to znaczna część opracowań dotyczących tej sfery zagrożeń odnosi je do kategorii dużo obszerniejszej – bezpieczeństwa politycznego, zgodnie zresztą z wytycznymi teorii sekurytyzacji. Celem niniejszego rozdziału jest więc próba zdefiniowania, wskazania istoty i miejsca bezpieczeństwa ideologicznego jako samodzielnego wariantu bezpieczeństwa, na tle teorii sekurytyzacji, która w znaczny sposób przyczyniła się do poszerzenia rozumienia bezpieczeństwa oraz katalogu jego zagrożeń. Niniejsza analiza dotyczyła będzie polskiej przestrzeni naukowo-badawczej z niezbędnym odniesieniem po podstaw teoretycznych szkoły kopenhaskiej rozwijającej teorię sekurytyzacji.

Bezpieczeństwo a teoria sekurytyzacji

Na podstawie analizy treści obszernych zasobów literatury przedmiotu, biorąc pod uwagę bezpieczeństwo jako kategorię badań bezpieczeństwa, można stwierdzić, że typologie bezpieczeństwa i jego kategoryzacje proponowane przez wielu badaczy często są niespójne. M.A. Levy twierdzi, że bezpieczeństwo nie jest łatwe do zdefiniowania, a już kwestię tego, „czyje jest bezpieczeństwo” (narodu, systemu międzynarodowego, całego ludzkości), łatwo jest pominąć ze względu na fakt, iż wybór często zależy od celów naukowej analizy (Levy 1995, s. 39). Wspomniana względność czy też zależność wynika z otwartego katalogu kategorii klasyfikacyjnych i nowych podejść teoretycznych, które stale się pojawiają i poddają ewolucji (Scibiorek 2016, s. 218). Teoria sekurytyzacji, którą należy wiązać przede wszystkim z osobą O. Wævera, oraz jej naukowe pokłosie w postaci rozwijanych koncepcji teoretycznych (ale nierzadko o znaczących walorach praktycznych) tzw. szkoły kopenhaskiej (grupy badaczy zrzeszonych w kopenhaskim instytucie COPRI – *Conflict and Peace Research Institute*), dały asumpt do pogłębionej analizy kategorii bezpieczeństwa, głównie na tle jej podstawowego składnika, a mianowicie przetrwania.

Jak zauważa Ł. Fijałkowski: „Szkoła kopenhaska odegrała istotną rolę w poszerzeniu koncepcji bezpieczeństwa i w stworzeniu ram analizy, jak dana kwestia podlega sekurytyzacji i desekurytyzacji. Obiektem zainteresowania stał się sam proces, w jakim pewne kwestie stają się częścią sfery bezpieczeństwa. W ten sposób bezpieczeństwo nie było traktowane jako obiektywny fakt, lecz swoista konstrukcja wypływająca z interakcji społecznych” (Fijałkowski 2012, s. 152). Co istotne, w powyższym kontekście teoria sekurytyzacji odnosi się bezpośrednio do bezpieczeństwa, ale w jego intersubiektywnym ujęciu. Teoria ta zakłada, że ramy pojęciowe kategorii bezpieczeństwa ulegają poszerzeniu w związku z procesem „włączania” lub „wyłączania” pewnych zagadnień do/z jego sfery. Ów proces jest nakierowany na ciągłą zmianę określonych zagrożeń i uwarunkowań, w których podmiot bezpieczeństwa funkcjonuje, i ma charakter procesu społecznego (Zięba 2008, s. 15-16). Współcześnie ma to związek z charakterem środowiska bezpieczeństwa danego podmiotu: człowieka, instytucji czy państwa. Środowisko to bowiem jest nacechowane

właśnie permanentną zmiennością uwarunkowań i zagrożeń dla bezpieczeństwa, niepewnością co do możliwości lub braku możliwości zaistnienia konkretnych scenariuszy rozwoju społecznego, złożonością zjawisk i procesów regulujących związki między ludźmi i pojmowanie bezpieczeństwa, a także niejednoznacznością w samej już ocenie zastanej rzeczywistości. Rozszerzenie „pojemności” kategorii analitycznej, jaką uczyniono bezpieczeństwo, jest też udziałem perturbacji w środowisku VUCA, które odznacza się właśnie zmiennością, niepewnością, złożonością i niejednoznacznością – *volatility, uncertainty, complexity, ambiguity* (Łubiński 2021a, s. 136). Dla teoretyków sekurytyzacji istotne jest jednak to, kto decyduje o wspomnianym „włączeniu” lub „wyłączeniu” danej kwestii do/ze sfery bezpieczeństwa oraz to, w jaki sposób się to dokonuje, w jakich okolicznościach, dlaczego i z jakim skutkiem (Buzan, Wæver, de Wilde 1998, s. 32; Fijałkowski 2012, s. 151). Można zatem stwierdzić, że proces definiowania, pojmowania i rozumienia bezpieczeństwa, wedle powyższych wskazówek, jest dalece uzależniony od praktycznej sfery stosowania tego terminu, a także od kontekstu i intencji osób zainteresowanych danym rodzajem bezpieczeństwa bądź jego zagrożeniami. Niezwykle ważna wydaje się też w tym kontekście pewna hierarchia kwestii i problemów bezpieczeństwa, które w określonych okolicznościach będą górowały nad innymi i w związku z tym będą wyznaczały priorytet ich ważności nie ze względu na faktycznie występujące (choć być może niedostrzegane) zagrożenie, ale ze względu na znaczenie, jakie się mu nadaje (Fijałkowski 2012, s. 151).

Generalnie rzecz biorąc, badacze dość zgodnie podkreślają, że teoria sekurytyzacji powstała „w celu dostarczenia analitycznych ram dla badań nad zagrożeniami dla bezpieczeństwa. To ostatnie jest traktowane jako koncepcja samoodwoławcza (*self-referential concept*), tworzona w trakcie intersubiektywnego procesu określania danej kwestii jako problemu bezpieczeństwa” (Fijałkowski 2014, s. 114). W związku z tym można stwierdzić, że wedle teorii sekurytyzacji zagrożenie dla bezpieczeństwa zostaje nim dopiero w momencie uznania go za takie. Czynniki obiektywne nie mają w tym przypadku żadnego znaczenia (por. Buzan, Hansen 2009, s. 215-217). Skoro zatem zagrożenie może być uznane za faktycznie realne lub nierealne, to interpretacja podmiotu sekurytyzującego dany czynnik bezpieczeństwa jest elementem decydującym o jego ostatecznej (inter)subiektywnej kwalifikacji. Takie ujęcie może rodzić daleko idące konsekwencje. Poruszając się w sferze paradygmatu realistycznego w naukach o bezpieczeństwie i stosunkach międzynarodowych, brak kwalifikacji konkretnego rodzaju zagrożenia dla państwa do kategorii zagrożeń żywotnych lub ważnych, w sferze praktyki funkcjonowania instytucji państwowych, ale i całego społeczeństwa, może rodzić skutki często nieodwracalne w krótkiej perspektywie. Pojawia się tu kolejny problem, który dotyczy odpowiedzialności za identyfikację zagrożeń i planowanie strategiczne w sferze możliwości wykorzystania potencjału państwa do ochrony przed zagrożeniami. Odpowiedzialność w tym zakresie ponosi głównie podmiot zarządzający daną sferą polityki bezpieczeństwa, który obraca się wokół konkretnego kontekstu politycznego i ideologicznego. Teoria sekurytyzacji jest w tym sensie o tyle istotna, że poprzez uznanie danego typu zagrożeń za egzystencjalnie godzące w państwo, społeczeństwo lub inny podmiot, pozwala ona na zastosowanie środków nadzwyczajnych, których

ideologiczne uzasadnienie i interpretacja ze strony politycznych przywódców usprawiedliwiają ich działanie.

Sekurytyzacja uwarunkowań i zagrożeń ideologiczno-politycznych

Jeżeli chodzi o zakres badań prowadzonych w polskiej przestrzeni naukowej odnoszącej się do nauk o bezpieczeństwie czy nauk o polityce i administracji, to ideologiczne uwarunkowania bezpieczeństwa państwa oraz zagrożenia o charakterze ideologicznym nie są niczym nowym. Jednak fakt uważania danej kwestii za kwestię bezpieczeństwa ideologicznego można uznać za konsekwencję sekurytyzacyjnego podejścia do analizowanych aspektów. Proces sekurytyzacji może mieć zastosowanie jedynie wówczas, kiedy spełnione będą określone warunki. Ł. Fijałkowski wskazuje, że pierwszym z nich jest potraktowanie zagrożenia przez tzw. „aktora sekurytyzującego” jako zagrożenia egzystencjalnego, mającego wydatny wpływ na niezakłócone funkcjonowanie państwa i stanowiącego ryzyko wystąpienia konsekwencji niepożądanych dla realizacji interesów narodowych. Drugim czynnikiem będzie tu przyjęcie przez społeczeństwo interpretacji i argumentacji podmiotu/aktora sekurytyzującego, że wspomniane zagrożenie jest na tyle istotne, że wymaga stanowczej reakcji ze strony państwa i mobilizacji zasobów niezbędnych do jego przezwyciężenia. Dopiero wtedy można uznać, że dana kwestia jest kwestią bezpieczeństwa (Fijałkowski 2014, s. 116). Reasumując, zagrożeniem ideologicznym czyni się zagrożenie, które ma charakter światopoglądowo-polityczny, jest uważane za godzące w podstawy egzystencjalne państwa lub społeczeństwa oraz decyzja o uznaniu tego zagrożenia za istotne jest akceptowana przez społeczeństwo. Proces ten jest procesem wybitnie intersubiektywnym.

Niezależnie od subiektywnie przyjętej klasyfikacji bezpieczeństwa, opartej na głównych kryteriach podziału: podmiotowym, przedmiotowym, przestrzennym, czasowym, organizacyjnym, składu lub zasięgu (Korzeniowski 2013, s. 11), można stwierdzić, że ideologiczne uwarunkowania i zagrożenia bezpieczeństwa są elementami, które powodują, że kryterium przedmiotowe w typologii bezpieczeństwa przeważa nad wszystkimi innymi kryteriami i pozwala na zakwalifikowanie bezpieczeństwa ideologicznego jako subkategorii bezpieczeństwa narodowego (państwa) (Ulmann 1983, s. 133). W zgodzie z przedstawicielami szkoły kopenhaskiej (Barry Buzan, Ole Wæver i Jaap de Wilde), którzy w trakcie swoich badań zidentyfikowali następujące sektory bezpieczeństwa: wojskowy, państwowo-polityczny, społeczny, gospodarczy i ochrony środowiska (Buzan, Wæver, de Wilde 1998, s. 138-139), próbując wyodrębnić sektory (dziedziny) bezpieczeństwa, L. Chojnowski wymienia sektor polityczny, który obejmuje problematykę stabilności i suwerenności państwa, a także jego systemu konstytucyjnego i ideologii (Chojnowski 2017, s. 21). Podejście to wynika bezpośrednio z kategoryzacji interesów narodowych i państwowych dążeń, co świadczy o skuteczności polityki opartej na trzech filarach bezpieczeństwa: suwerenność (wewnętrzna i zewnętrzna), stabilność organizacyjna i ideologia. Ten ostatni element warunkuje funkcjonowanie podmiotów państwowych (Chojnowski 2015, s. 197). Ideologia jest kluczowym elementem wspomnianej triady, gdyż jest elementem konstytutywnym dla dookreślenia istoty ideologicznego

bezpieczeństwo państwa. W kontekście tego typu bezpieczeństwa sekurytyzacja jawi się także jako pewnego rodzaju ewentualne źródło nadużyć – O. Wæver stwierdza bowiem, że skoro aktor sekurytyzujący decyduje o tym, którą kwestię zakwalifikować do kwestii bezpieczeństwa, oraz o tym, jakie środki podjąć celem eliminacji zagrożenia (nie bacząc na obiektywne czynniki środowiska bezpieczeństwa), to istnieje uzasadnione ryzyko wykorzystania przez takiego aktora sytuacji do własnych celów oraz zastosowania środków, które poprzez sekurytyzację będą poza jakąkolwiek kontrolą społeczną (Wæver 1995a, s. 55-56). Dlatego też sekurytyzacja, jako proces nadawania konkretnym faktom społecznym, zjawiskom i zmianom interpretacji w kierunku sfery bezpieczeństwa, ma kluczowe znaczenie dla wyznaczania obiektów lub wartości podlegających prawnej i/lub faktycznej ochronie, a także tworzenia sytuacji prawnej i/lub faktycznej dominacji.

Zasygnalizowano już, że bezpieczeństwo ideologiczne wraz z jego zagrożeniami bywa rozpatrywane w kontekście kategorii znaczeniowo obszerniejszej, a mianowicie bezpieczeństwa politycznego, które z kolei jest jednym z wyodrębnionych przedmiotowo rodzajów (sektorów) bezpieczeństwa, co stało się udziałem reprezentantów szkoły kopenhaskiej w latach 90. (Zalewski 2017, s. 347). W swojej teorii sektorów bezpieczeństwa B. Buzan wskazuje, że bezpieczeństwo polityczne dotyczy stabilności organizacyjnej państw, systemów rządów i ideologii, które dają im legitymizację. Społeczeństwo zaś odnosi się do trwałości bezpieczeństwa w akceptowalnych warunkach ewolucji, tradycyjnych wzorcach języka, kultury oraz tożsamości religijnej i narodowej, a także obyczajów (Buzan 1991, s. 19-20). Biorąc to pod uwagę, bezpieczeństwo ideologiczne można rozpatrywać w kategoriach jego zbieżności pomiędzy polityką i bezpieczeństwem państwa. B. Buzan podkreśla, że w sferze politycznej zagrożenia egzystencjalne są tradycyjnie definiowane w kategoriach zasady konstytuującej państwo (suwerenności, a czasem także ideologii) (Buzan 1997, s. 16). Odwołując się do koncepcji B. Buzana, S. Zalewski wskazuje, że postrzeganie bezpieczeństwa przez państwa i ich społeczeństwa uległo zmianie, poszerzeniu zakresu jego pojmowania w kierunku stanu i procesu sprzyjającemu wzrostowi oczekiwań obywateli. Jednak możliwości państwa w zakresie sprostania tym oczekiwaniom nie wzrosły w stopniu, który odpowiadałby tym potrzebom. Tendencja ta, zdaniem wskazanego Autora, ma istotne znaczenie z trzech powodów: po pierwsze – źródła nowo pojawiających się zagrożeń nierzadko są trudne do rozpoznania, a tym samym do przeciwdziałania ich rozszerzaniu, stąd władza często traktuje je wybiórczo; po drugie – współczesne zagrożenia egzystencjalne i polityczne mają charakter asymetryczny i hybrydowy (zob. Wasiuta, Wasiuta 2021); po trzecie – władza publiczna musi posiadać poparcie społeczne dla działań podejmowanych w sferze bezpieczeństwa (Zalewski 2017, s. 355). Zauważyć tu można nawiązania do twórczości reprezentantów szkoły kopenhaskiej. Kluczowym aspektem jest uznanie dla nierozłączności korelacji występującej pomiędzy aktorem sekurytyzującym a obiektem bezpieczeństwa, którym w przypadku sektora politycznego będzie suwerenność narodowa lub „wyznawana” w państwie ideologia (Fijałkowski 2012, s. 154).

Bezpieczeństwo ideologiczne w polskiej przestrzeni badawczej

W. Kitler bezpieczeństwem ideologicznym nazywa właśnie proces obejmujący różnorodne działania i środki z zakresu bezpieczeństwa narodowego (bądź bezpieczeństwa w sensie generalnym; a więc bezpieczeństwa politycznego, militarnego, ekonomicznego, społecznego, kulturowego, energetycznego, ekologicznego, informacyjnego) (Kotowicz 2015, s. 134-137; Falecki 2018, s. 70), których głównym celem jest utrwalenie i kształtowanie wspólnoty światopoglądowej w dążeniu do realizacji poszczególnych interesów narodowych, przeciwdziałanie wszelkim ideologiom o skrajnym zabarwieniu oraz ochrona przed różnymi teoriami postulującymi bądź uzasadniającymi działania o negatywnych konsekwencjach dla narodowego interesu (Kitler 2011, s. 54). Bezpieczeństwo ideologiczne, poza wspomnianą ochroną państwa i społeczeństwa przed działaniami destrukcyjnymi dla wewnętrznego ładu i porządku konstytucyjnego, charakteryzuje się też działaniami zmierzającymi do zapewnienia przetrwania, rozwoju i wolności wyznawania innych niż uznawana powszechnie ideologii (zarówno świeckich, jak i religijnych) (Malak 2010) pod warunkiem, że nie niosą one ze sobą szkodliwych dla państwa i narodu rozwiązań ideowych (ideologia, obok strategii i religii w XX wieku, na co zwraca się uwagę również współcześnie, była uznawana za jeden z niematerialnych elementów/czynników globalnego środowiska bezpieczeństwa państwa) (Sójka 2016, s. 517). Połączenie wątku ideologii i jej znaczenia dla konstytutywnego porządku państwa oraz odpowiedniego poziomu tożsamości narodowej społeczeństwa było przedmiotem badań i analiz w wielu pracach naukowych na świecie już w latach 90. XX wieku (Buzan 1994; Buzan 1996; Buzan, Wæver, de Wilde 1998). Oczywiście należy dokonać tu rozróżnienia na bezpieczeństwo ideologiczne w sensie generalnym (odnoszące się do ideologii preferowanej przez społeczeństwo, znaczną jego część lub określoną grupę społeczną) oraz w sensie partykularnym (odnoszące się do ideologii „wyznawanej” przez wąską grupę sprawującą władzę w państwie lub o nią zabiegającą).

Bezpieczeństwo ideologiczne, biorąc pod uwagę jego podmiotowy charakter i zakres oddziaływania, można także rozpatrywać, opierając się na podziale na perspektywę wewnętrzną i zewnętrzną. W pierwszym przypadku działalność instytucji i podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa ideologicznego skupiać się będzie na ograniczeniu działalności (wpływu na społeczeństwo) partii politycznych, grup społecznych, grup nacisku politycznego oraz grup religijnych, które, realizując swoje partykularne interesy, propagują i rozpowszechniają ideologie niezgodne z podstawowymi zasadami ustrojowymi państwa. Natomiast w drugim przypadku zapewnienie bezpieczeństwa ideologicznego polegać będzie na ograniczeniu działania państw lub innych podmiotów stosunków międzynarodowych, które szerzą skrajne ideologie oraz podejmują starania o dokonanie zmian ustrojowych w rejonie swojego bezpośredniego oddziaływania (Urbanek 2013, s. 32). Zarówno pierwsze, jak i drugie ujęcie bezpieczeństwa ideologicznego kładzie nacisk na czynnik ochrony porządku ustrojowego (konstytucyjnego) państwa oraz szeroko pojętego porządku aksjologicznego, przed bezprawnym i sprzecznym z przyjętym systemem wartości oddziaływaniem innych (skrajnych) ideologii. Silne zakorzenienie w realistycznym paradygmacie stosunków międzypaństwowych pozwala na

stwierdzenie, że istotą bezpieczeństwa jest zapewnienie istnienia, przetrwania i ciągłości państwowej, a więc realizacja interesów narodowych (ochrona głównie przed czynnikami zewnętrznymi) niezależnie od zideologizowanej rywalizacji i nieuchronnego konfliktu interesów w sferze bezpieczeństwa (Zięba 2018, s. 18-20). To właśnie wiek XX upłynął pod znakiem dominacji takich radykalnych ideologii, jak faszyzm czy komunizm, i fakt stopniowego zastępowania ideologii innymi, pokrewnymi zagrożeniami dla narodowego i międzynarodowego ładu w XXI wieku, tj. np. fundamentalizmami, nie umniejsza znaczenia ideologii jako czynnika decydującego o stanie bezpieczeństwa w wymiarze wewnętrznym i zewnętrznym. Jak bowiem podaje W. Pokruszyński, należy uwypuklić „problem ideologiczno-polityczny jako jedno z podstawowych uwarunkowań bezpieczeństwa narodowego w systemie sojuszniczym (UE), w którym państwa członkowskie mają różne ideologie, a także swoje polityki i strategie bezpieczeństwa” (Pokruszyński 2010, s. 29-30). Podkreślenia wymaga też fakt, iż związki ideologii i polityki na płaszczyźnie zapewniania (czy też realizacji) bezpieczeństwa poszczególnych państw są na tyle trwałe, że bezpieczeństwo ideologiczne nierzadko traktowane jest w literaturze przedmiotu jako aksjologiczna (odwołująca się do konkretnych wartości) subkategoria bezpieczeństwa politycznego (czyli pewności przetrwania, rozwoju państwa i wewnętrznej stabilności rządów) (Buzan 1991, s. 19). Bezpieczeństwo ideologiczne w tym kontekście jawi się jako pojęcie odnoszące się do „pewności przetrwania i rozwoju ideologii, stanowiącej podstawę panującego w danym państwie systemu rządów” (Pawlikowska 2009, s. 62-63).

Bezpieczeństwo ideologiczne oraz jego zagrożenia można rozpatrywać z obiektywnego lub subiektywnego punktu widzenia. Bezpieczeństwo ideologiczne w sensie obiektywnym dotyczyć będzie ochrony przed zagrożeniem spowodowanym wszelkim działaniem lub zaniechaniem działania skutkującym ograniczeniami w zakresie wolności słowa, swobody sumienia i wyznania. W tym sensie bezpieczeństwo ideologiczne to ochrona przed negatywnym oddziaływaniem zasad innych ideologii, sprzecznych z interesem społeczeństwa, interesem narodowym, interesem państwa i jego racją stanu. Obiektywny charakter zagrożeń bezpieczeństwa ideologicznego świadczy z jednej strony o tym, że ich występowanie i oddziaływanie może być niezależne od świadomości człowieka, ale z drugiej strony – człowiek ma realny wpływ na kształtowanie systemu ochrony przed tego typu zagrożeniami. Bezpieczeństwo ideologiczne (wraz z jego zagrożeniami) może mieć także bardzo subiektywny charakter i może zależeć od rodzaju „wyznawanej” przez społeczeństwo lub konkretną grupę ideologii. Subiektywny stan bezpieczeństwa ideologicznego uwarunkowany jest przeżyciami, poglądami, ocenami i nierzadko intencjami konkretnego podmiotu (zgodnie z wymogami sekurytyzacji bezpieczeństwa). W takim przypadku zagrożeniem dla bezpieczeństwa ideologicznego będzie działanie lub zaniechanie działania sprzeczne z przyjętą (np. przez partię rządzącą) ideologią (Łubiński 2021, s. 311-312). Jak można powtórzyć za O. Wæverem, współcześnie zagrożenia lub przeszkody dla integracji społeczno-politycznej nie pochodzą od protestujących państw, ale od sił społecznych powstrzymujących ich bardziej entuzjastyczne elity polityczne (Wæver 1995, s. 404).

Problem występowania wielu różnych ideologii oraz fakt, iż bezpieczeństwo ideologiczne polega na zapewnieniu możliwości funkcjonowania tychże ideologii w jednej przestrzeni społecznej, kulturowej i politycznej (czego konsekwencją mogą być spory na tle ideologicznym), sprawiają, że proces zapewnienia bezpieczeństwa ideologicznego może napotkać na wiele trudności. Wynikać one mogą m.in. z subiektywnego charakteru poszczególnych ideologii występujących w państwie, antypaństwowego charakteru niektórych ideologii, wzajemnie wykluczających się zasad poszczególnych ideologii, upraszczania rzeczywistości i spłaszczania jej do wymiaru dwubiegunowego, absolutyzacji twierdzeń będących fundamentem danej ideologii, utopijnego wymiaru ideologii lub wywyższania tzw. „myślenia życzeniowego” ponad rzetelną analizę faktycznej rzeczywistości (Filipkowski 2005, s. 297; Łubiński 2021, s. 314). Zakres zapewniania bezpieczeństwa ideologicznego i jego semantyczna objętość wskazują na możliwość wyodrębnienia tego typu bezpieczeństwa z szerokiej kategorii, jaką jest bezpieczeństwo polityczne, zgodne z wytycznymi teorii sektorów bezpieczeństwa.

Podsumowanie

Szkola kopenhaska za sprawą jej wielkich twórców i reprezentantów stworzyła trwałe fundamenty teoretyczno-praktyczne, pozwalające na typologizowanie i kategoryzację rodzajów oraz sektorów bezpieczeństwa. Biorąc pod uwagę wytyczne teorii sekurytyzacji, a więc swoistą intersubiektywną możliwość klasyfikacji danego problemu czy zjawiska jako „kwestii bezpieczeństwa” (kwestii o znaczeniu egzystencjalnym) oraz uznanie dla takiego aktu przez społeczeństwo akceptujące przedsięwzięte do niwelacji tego zagrożenia środki nadzwyczajne (o ile rozpatruje się problem w perspektywie relacji na linii państwo – społeczeństwo), można stwierdzić, że w zasadzie każdy aspekt, który uznany zostanie za kwestię bezpieczeństwa ideologicznego oraz zaakceptowany – stanie się nim. Sekurytyzacja, jako proces nadawania konkretnym faktom społecznym, zjawiskom i zmianom interpretacji w kierunku sfery bezpieczeństwa, ma kluczowe znaczenie dla wyznaczania obiektów lub wartości podlegających prawnej i/lub faktycznej ochronie, a także tworzenia sytuacji prawnej i/lub faktycznej dominacji. Jest to o tyle istotne, że fakt uważania danej kwestii za kwestię bezpieczeństwa ideologicznego można uznać właśnie za konsekwencję sekurytyzacyjnego podejścia do analizowanych w rozdziale aspektów. Wyrażona na łamach innych prac naukowych potrzeba zgłębiania teorii, zakresu oddziaływania, społeczno-politycznego znaczenia, uwarunkowań i nowych zagrożeń bezpieczeństwa ideologicznego zostaje tu podtrzymana.

Literatura

1. Buzan B. (1991), *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Boulder-Hemel Hempstead, Harvester.
2. Buzan B. (1994), *National Security in the Post-Cold War Third World*, „Strategic Review for Southern Africa”, 16, s. 1-34.

3. Buzan B. (1996), *International Security and International Society*, [w:] Fawn R., Larkin J. (red.), *International Society After the Cold War: Anarchy and Order Reconsidered*, s. 261-287, London.
4. Buzan B. (1997), *Rethinking Security after the Cold War*, „Cooperation and Conflict”, 32, 5, s. 5-28.
5. Buzan B., Hansen L. (2009), *The Evolution of International Security Studies*, Cambridge University Press, Cambridge.
6. Buzan B., Wæver O., de Wilde J. (1998), *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder-London.
7. Chojnowski L. (2015), *Podmiotowo-przedmiotowe ramy analizy bezpieczeństwa a jego naukowa multidyscyplinarność*, [w:] Kitler W., Kośmider T. (red.), *Metodologiczne i dydaktyczne aspekty bezpieczeństwa narodowego*, s. 190-215, Difin, Warszawa.
8. Chojnowski L. (2017), *Bezpieczeństwo międzynarodowe. Aspekty instytucjonalne i organizacyjne*, Akademia Pomorska, Słupsk.
9. Falecki J. (2018), *Bezpieczeństwo*, [w:] Wasiuta O., Klepka R., Kopeć R. (red.), *Vademecum bezpieczeństwa*, s. 67-72, Wydawnictwo Libron, Kraków.
10. Fijałkowski Ł. (2012), *Teoria sekurytyzacji i konstruowanie bezpieczeństwa*, „Przegląd Strategiczny”, 1, s. 149-161.
11. Fijałkowski Ł. (2014), *Teoria sekurytyzacji a realistyczne ujęcie bezpieczeństwa*, [w:] Czaputowicz J., Haliżak E. (red.), *Teoria realizmu w nauce o stosunkach międzynarodowych. Założenia i zastosowania badawcze*, s. 109-121, Wydawnictwo Rambler, Warszawa.
12. Filipkowski J. (2005), *Ideologia*, [w:] Opara S., Radziszewska-Szczepaniak D., Żukowski A. (red.), *Podstawowe kategorie polityki*, s. 293-297, Instytut Nauk Politycznych UWM, Olsztyn.
13. Kitler W. (2011), *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Akademia Obrony Narodowej, Warszawa.
14. Korzeniowski M. (2013), *Wstęp do metodologii badań bezpieczeństwa narodowego*, Instytut Nauk Politycznych UWM, Olsztyn.
15. Kotowicz W. (2015), *Bezpieczeństwo narodowe*, [w:] Żukowski A. i in. (red.), *Podstawowe kategorie bezpieczeństwa narodowego*, s. 131-138, Instytut Nauk Politycznych UWM, Olsztyn.
16. Levy M.A. (1995), *Is the Environment a National Security Issue?*, „International Security”, 2, 20, s. 35-62.
17. Łubiński P. (2021), *Bezpieczeństwo ideologiczne*, [w:] Wasiuta O., Wasiuta S. (red.), *Encyklopedia bezpieczeństwa*, 1, s. 306-316, Wydawnictwo Libron, Kraków.
18. Łubiński P. (2021a), *Wieloaspektowy wymiar społecznych zagrożeń bezpieczeństwa państwa w środowisku VUCA*, [w:] Kaźmierczak D. i in. (red.), *Edukacja w świecie VUCA. Charakterystyka środowiska bezpieczeństwa*, s. 125-139, Wydawnictwo Libron, Kraków.
19. Malak K. (2010), *Typologia bezpieczeństwa. Nowe wyzwania*, <http://stosunki-miedzynarodowe.pl/bezpieczenstwo/954-typologia-bezpieczenstwa-nowe-wyzwania> (dostęp: 11.01.2019).
20. Pawlikowska I. (2009), *Bezpieczeństwo jako cel polityki zagranicznej państwa*, [w:] Zięba R. (red.), *Wstęp do teorii polityki zagranicznej państwa*, s. 59-78, Wydawnictwo Adam Marszałek, Toruń.
21. Pokruszyński W. (2010), *Teoretyczne aspekty bezpieczeństwa. Podręcznik akademicki*, Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów.
22. Sójka W. (2016), *Ewolucja środowiska bezpieczeństwa Polski i generowanie nowych kategorii zagrożeń w aspekcie bezpieczeństwa państwa*, [w:] Sienkiewicz P., Dela P. (red.), *Metodologia badań bezpieczeństwa narodowego*, VIII, Akademia Obrony Narodowej, Warszawa.
23. Ścibiorek Z. (2016), *Tożsamość nauk o bezpieczeństwie*, [w:] Ścibiorek Z., Zamiar Z. (red.), *Teoretyczne i metodologiczne podstawy problemów z zakresu bezpieczeństwa. Podręcznik akademicki*, s. 215-236, Wydawnictwo Adam Marszałek, Toruń.

24. Ullman R. (1983), *Redefining Security*, „International Security”, 1, 8, s. 129-153.
25. Urbanek A. (2013), *Państwo jako podmiot bezpieczeństwa narodowego – ujęcie dziedzinowe*, [w:] Urbanek A. (red.), *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, s. 11-39, Wydawnictwo Społeczno-Prawne, Słupsk.
26. Wæver O. (1995), *Identity, Integration and Security: Solving the Sovereignty Puzzle in E.U. Studies*, „Journal of International Affairs”, 48, 2, s. 403-404.
27. Wæver O. (1995a), *Securitization and Desecuritization*, [w:] Lipschutz L. (red.), *On Security*, s. 46-86, Columbia University Press, Nowy Jork.
28. Wasiuta O., Wasiuta S. (2021), *Zagrożenia hybrydowe jako wyzwanie dla środowiska bezpieczeństwa*, [w:] Kaźmierczak D. i in. (red.), *Edukacja w świecie VUCA. Charakterystyka środowiska bezpieczeństwa*, s. 49-80, Wydawnictwo Libron, Kraków.
29. Zalewski S. (2017), *Bezpieczeństwo polityczne państwa*, [w:] Pawłowski J. (red.), *Podstawy bezpieczeństwa narodowego (państwa)*, s. 345-372, Akademia Sztuki Wojennej, Warszawa.
30. Zięba R. (2008), *Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego*, [w:] Zięba R. (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, s. 15-42, Wydawnictwa Akademickie i Profesjonalne, Warszawa.
31. Zięba R. (2018), *Teoria bezpieczeństwa państwa w ujęciu neorealistycznym*, „Studia Politologiczne”, 49, s. 13-32.

IDEOLOGICAL SECURITY AND THE THEORY OF SECURITIZATION IN THE POLISH SCIENCE AND RESEARCH AREA

Abstract: The aim of this chapter is an attempt to define and indicate the essence and place of ideological security as an independent variant of national security (state) against the background of the theory of securitization, which has significantly contributed to broadening the understanding of security and the catalog of its threats. This analysis will concern the Polish research area with the necessary reference to the theoretical foundations of the Copenhagen school, developing the theory of securitization. The issues of securitization of conditions and threats of an ideological and political nature in relation to the theory of security sectors will be discussed.

Keywords: Copenhagen school, ideological security, security theory, securitization theory

Rozdział 14

BEZPIECZEŃSTWO KULTUROWE A PROGRAM WSPÓŁPRACY TRANSGRANICZNEJ POLSKA - BIAŁORUŚ - UKRAINA 2014-2020

Agnieszka Pieniążek²²

Streszczenie: Za sprawą projektów finansowanych w ramach Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina wspierane są m.in. procesy rozwojowe na pograniczu polsko-ukraińsko-białoruskim. Przedsięwzięcia skoncentrowane są m.in. na ochronie i promocji dziedzictwa kulturowego i przyrodniczego, zwiększeniu dostępności regionów, rozwoju infrastruktury, a także na wzmocnieniu służby zdrowia i rozwoju usług socjalnych oraz poprawie bezpieczeństwa granic. Głównym celem rozdziału jest próba oceny możliwości oddziaływania Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina na bezpieczeństwo kulturowe w Polsce. Analizą objęta została unijna perspektywa finansowa 2014-2020. Analizie poddano dokumenty programowe oraz informacje na temat wyników naborów projektów w ramach programu.

Słowa kluczowe: bezpieczeństwo kulturowe, programy UE, współpraca transgraniczna

Wprowadzenie

W roku 1990 uruchomiona została Inicjatywa Wspólnotowa Interreg – instrument wspierający m.in. współpracę regionów granicznych w państwach Wspólnoty Europejskiej. Początkowo przywiązywano do niej niewielką wagę, jednak z czasem przekształciła się ona w jeden z trzech celów polityki strukturalnej (Dołzbłasz, Raczyk 2011, s. 59).

W piątym okresie programowania (2014-2020) budżet ponad 100 programów Interreg wynosił około 10,1 mld euro (KE). W Polsce w ramach Europejskiej Współpracy Terytorialnej Interreg było wdrażanych siedem programów transgranicznych (Polska – Saksonia; Brandenburgia – Polska; Meklemburgia – Pomorze Przednie – Brandenburgia – Polska, Południowy Bałtyk, Litwa – Polska; Czechy – Polska; Polska – Słowacja), dwa programy transnarodowe (Region Morza Bałtyckiego, Europa Środkowa) oraz jeden międzyregionalny (Interreg Europa). Dodatkowe dwa

²² Państwowa Wyższa Szkoła Wschodnioeuropejska w Przemyślu, Instytut Nauk Społecznych i Ochrony Zdrowia

programy współpracy transgranicznej były realizowane w ramach Europejskiego Instrumentu Sąsiedztwa (EIS): Polska – Białoruś – Ukraina i Polska – Rosja (EWT).

Celem rozdziału jest ocena możliwości oddziaływania Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina na bezpieczeństwo kulturowe państwa. Analizie poddano dokumenty programowe oraz informacje na temat wyników naborów projektów w ramach tego Programu w perspektywie finansowej 2014-2020.

Badany materiał pozwolił na uzyskanie odpowiedzi na następujące pytania:

- 1) Czy w ramach Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina funkcjonuje pojęcie bezpieczeństwa kulturowego?
- 2) Czy Program, poprzez przedsięwzięcia realizowanego w jego ramach, przyczynia się do zapewniania bezpieczeństwa kulturowego?
- 3) W jaki sposób przedsięwzięcia realizowane w ramach Programu mogą przyczynić się do wzmocnienia bezpieczeństwa kulturowego?

Bezpieczeństwo kulturowe

Pojęcie „bezpieczeństwo kulturowe” jest terminem stosunkowo nowym, jednak – jak podkreśla J. Czaja – historia potwierdza, że „realnym i historycznie doskonale znanym”. Zaczęto go używać w czasie I wojenny światowej, jego rozkwit nastąpił w latach 60. XX wieku, a w latach 70. i 80. był już w powszechnym użyciu (Czaja 2013, s. 77-78). Wciąż jednak określenie „bezpieczeństwo kulturowe” definiowane jest w różny sposób.

Szereg definicji bezpieczeństwa kulturowego zostało przytoczonych w pracy autorstwa J. Czaj pt. *Kulturowy wymiar bezpieczeństwa. Aspekty teoretyczne i praktyczne*. Zdaniem tego Autora dotychczas podejmowane próby definiowania bezpieczeństwa kulturowego uwzględniają takie elementy jak zachowanie tożsamości kulturowej, czystości języka, kultury, istotnych dla narodów zwyczajów i religii. W wielu definicjach podkreślano związek między bezpieczeństwem kulturowym a prawami i wolnościami człowieka. Większość definicji bezpośrednio lub pośrednio wiąże bezpieczeństwo kulturowe z bezpieczeństwem narodowym (Czaja 2013, s. 80). Różne spojrzenia na definiowanie pojęcia „bezpieczeństwo kulturowe” przedstawiła również I. Oleksiewicz (2020, s. 155-172). W dalszej części rozdziału zaprezentowano kilka z nich.

Zbiorową próbę zdefiniowania tego pojęcia podjęli uczestnicy konferencji, która odbyła się w 1999 roku w Berlinie. Według tej grupy naukowców bezpieczeństwo kulturowe składa się z „bezpieczeństwa jednostkowego oraz poczucia zbiorowej tożsamości” i zawiera, nie ograniczając się wyłącznie do tych aspektów, „wolność myśli, sumienia, mowy, stylu życia, przynależności etnicznej, płci, poczucie przynależności do stowarzyszeń, związków, obejmując także kulturalne i polityczne współzawodnictwo” (Czaja 2013, s. 81). Z kolei G. Michałowska uważa, iż „bezpieczeństwo kulturowe w wymiarze narodowym oznacza warunki, w których społeczeństwo może utrzymywać i pielęgnować wartości decydujące o jego tożsamości, a jednocześnie swobodnie czerpać z doświadczeń i osiągnięć innych narodów” (Michałowska 1997, s. 132). Zdaniem T. Jemioła bezpieczeństwo kulturowe

państwa to „jego zdolność do pomnażania dotychczasowego dorobku kulturalnego oraz obrony przed niepożądanym wpływem innych kultur” (Jemiolo 2001, s. 20). Natomiast W. Kitler podkreśla, że „zasadniczym celem bezpieczeństwa kulturowego jest nie tylko ochrona dóbr kultury materialnej i dziedzictwa kulturowego, lecz w szerokim ujęciu także: ochrona wartości istotnych dla tożsamości narodowej, ochrona odrębności kulturowych związanych z etnicznością lub mniejszościami narodowymi, tworzenie otwartości kulturowej – swobodnego przepływu wartości powszechnie uznanych za cenne, promowanie kultury narodowej na świecie i tworzenie sprzyjających warunków do rozwoju kultury” (Hrynicki 2004, s. 194).

Jak podaje J. Czaja, dziedzictwo kulturowe wiąże się z „jednej strony z dobrami kultury szczególnie cennymi dla narodu, z drugiej – z przekazywaniem następnemu pokoleniu tradycyjnych wartości i idei w społeczeństwie. Tradycja jest nośnikiem wartości społecznych, tak długo istniejących w świadomości, jak długo mają aktualne znaczenie”. Zadaniem tego Autora nie ulega wątpliwości, że rola państwa i jego instytucji finansowo-gospodarczych jest niezwykle ważna dla rozwoju kultury i ochrony dziedzictwa kulturowego. Z kolei tożsamość kulturowa jest tym, co dla większości ludzi ma najważniejsze znaczenie (Czaja 2013, s. 69-7, 80).

Natomiast A. Włodkowska zwraca uwagę na charakter dualistyczny bezpieczeństwa kulturowego, które odnosi się do sfery państwowej (bezpieczeństwo kulturowe państwa) oraz społecznej (bezpieczeństwo kulturowe jednostek i wspólnot kulturowych – narodów, grup etnicznych, wspólnot wyznaniowych). Jej zdaniem bezpieczeństwo kulturowe w wymiarze społecznym nie zawsze jest tożsame z bezpieczeństwem kulturowym państw, co szczególnie jest widoczne w przypadku państw o ustrojach niedemokratycznych (Włodkowska 2009, s. 149).

Program Współpracy Transgranicznej Polska - Białoruś - Ukraina

Europejski Instrument Sąsiedztwa, w ramach którego funkcjonował badany Program, został przyjęty 11 marca 2014 roku w drodze Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 232/2014. Program ten był jednym z dwóch programów współpracy transgranicznej realizowanych w Polsce na zewnętrznych granicach Unii Europejskiej.

Po polskiej stronie Program był wdrażany w województwach: podlaskim (podregiony: białostocki, łomżyński i suwalski), mazowieckim (podregion: ostrołęcko-siedlecki), lubelskim (podregiony: bialski, chełmsko-zamojski, puławski i lubelski) oraz podkarpackim (podregiony: krośnieński, przemyski, rzeszowski i tarnobrzowski). Na Ukrainie Program wdrażano w obwodach: lwowskim, wołyńskim, zakarpackim, rówieńskim, tarnopolskim i iwanofrankowskim. Z kolei na Białorusi były to obwody: grodzieński, brzeski, miński (z miastem Mińsk) oraz homelski (PBUa).

Głównym celem Programu było wspieranie transgranicznych procesów rozwojowych na pograniczu Polski, Ukrainy i Białorusi. W jego ramach zdefiniowano trzy cele strategiczne:

- 1) Promowanie rozwoju gospodarczego i społecznego w regionach po obu stronach wspólnej granicy.

- 2) Rozwiązywanie wspólnych wyzwań dotyczących środowiska, zdrowia publicznego, bezpieczeństwa i ochrony.
- 3) Promocja lepszych warunków i zasad zapewniających mobilność osób, towarów i kapitału (Program Współpracy..., s. 9).

Dla działań w ramach współpracy transgranicznej określono również cztery cele tematyczne:

- 1) Promocja kultury lokalnej i zachowanie dziedzictwa historycznego („Dziedzictwo”).
- 2) Poprawa dostępności regionów, rozwoju trwałego i odpornego na klimat transportu oraz sieci i systemów komunikacyjnych („Dostępność”).
- 3) Wspólne wyzwania w obszarze bezpieczeństwa i ochrony („Bezpieczeństwo”).
- 4) Promocja zarządzania granicami oraz bezpieczeństwem na granicach, zarządzanie mobilnością i migracjami („Granice”).

W ramach poszczególnych celów tematycznych zostały zdefiniowane priorytety (tab. 14.1). Łączny budżet Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina wynosił 170,1 mln euro. Najwięcej środków zaplanowano na realizację przedsięwzięć w ramach drugiego celu tematycznego Dostępność – 55,9 mln euro, co stanowi 32,9 % alokacji. Na realizację projektów w ramach pierwszego celu tematycznego przeznaczono 38,4 mln euro, tj. 22,6% dostępnych środków. Więcej informacji na temat wielkości dostępnych środków w poszczególnych celach tematycznych zawarto w tabeli 14.1.

Wszystkie nabory cieszyły się bardzo dużym zainteresowaniem potencjalnych wnioskodawców. W pierwszym z naborów zakontraktowano 65 projektów. O dofinansowanie można było się ubiegać w ramach wszystkich celów tematycznych. Nabór składał się z dwóch etapów. W pierwszym złożono aż 749 koncepcji projektów, a następnie 383 pełnych wniosków aplikacyjnych (PBUb). Dofinansowanie otrzymał jednak co szósty wniosek. Drugi nabór był dedykowany wyłącznie przedsięwzięciom z pierwszego celu tematycznego. Złożono 250 wniosków aplikacyjnych. Do dofinansowania wybrano jednak co trzeci wniosek, tj. 74 projekty (PBUc).

Z uwagi na niewykorzystane środki w ramach drugiego naboru, pod koniec 2019 roku uruchomiono kolejny nabór, w ramach którego w pierwszym celu tematycznym złożono 178 wniosków o dofinansowanie, których łączna kwota przekraczała siedmiokrotnie dostępny budżet. Do dofinansowania wybrano jednak zaledwie 26 projektów (PBUd). Podkreślić należy, iż w oddzielnej procedurze wybrano 10 projektów strategicznych dla rozwoju regionów. Dofinansowanie nie było jednak dostępne dla przedsięwzięć w pierwszym celu tematycznym, czyli w zakresie promocji kultury lokalnej i zachowania dziedzictwa historycznego.

Analizując ogólną liczbę projektów wybranych do dofinansowania, zauważyć można, iż najwięcej projektów dotyczyło realizacji pierwszego celu tematycznego Promocja kultury lokalnej i zachowanie dziedzictwa historycznego (116 projektów). W przypadku pozostałych celów tematycznych dofinansowano po kilkanaście projektów. Tak duża liczba projektów wynikała z faktu, iż w drugim i trzecim naborze można było przygotowywać projekty, których maksymalna kwota dofinansowania nie przekroczyła 60 tys. euro. W ten sposób dofinansowano 100 przedsięwzięć. Dla porównania: w projektach regularnych wymagano, aby dofinansowanie wynosiło

nie mniej niż 100 tys. euro i nie więcej niż 2,5 mln euro. Dominowały tym samym znacznie większe projekty.

Tabela 14.1. Wysokość alokacji w poszczególnych celach tematycznych Programu Współpracy Transgranicznej Polska – Białoruś – Ukraina w perspektywie finansowej 2014-2020

Cel	Priorytet	Alokacja (w mln euro)
1. Promocja kultury lokalnej i zachowanie dziedzictwa historycznego („Dziedzictwo”)	1.1. Promocja kultury lokalnej i historii	38,4
	1.2. Promocja i zachowanie dziedzictwa naturalnego	
2. Poprawa dostępności regionów, rozwoju trwałego i odpornego na klimat transportu oraz sieci i systemów komunikacyjnych („Dostępność”)	1.1. Promocja kultury lokalnej i historii	55,9
	1.2. Promocja i zachowanie dziedzictwa naturalnego	
3. Wsparcie dla rozwoju ochrony zdrowia i usług socjalnych („Bezpieczeństwo”)	2.1. Poprawa i rozwój usług transportowych i infrastruktury	44,3
	2.2. Rozwój infrastruktury technologii informacyjno-komunikacyjnych	
4. Promocja zarządzania granicami oraz bezpieczeństwem na granicach, zarządzanie mobilnością i migracjami („Granice”)	3.1. Wsparcie dla rozwoju ochrony zdrowia i usług socjalnych	31,5
	3.2. Podejmowanie wspólnych wyzwań związanych z bezpieczeństwem	
	Razem	170,1

Źródło: (Annual Report... 2020)

„Bezpieczeństwo” w Programie Polska - Białoruś - Ukraina

Analiza dokumentów programowych wskazuje, iż Program nie posługuje się pojęciem „bezpieczeństwa kulturowego”. W dokumentach jest mowa jedynie o bezpieczeństwie w kontekście dwóch celów tematycznych: trzeciego – Wsparcie dla rozwoju ochrony zdrowia i usług socjalnych („Bezpieczeństwo”) – oraz czwartego – Promocja zarządzania granicami oraz bezpieczeństwem na granicach, zarządzanie mobilnością i migracjami („Granice”).

Realizacja przedsięwzięć w ramach trzeciego celu tematycznego powinna służyć poprawie jakości życia mieszkańców obszaru Programu poprzez ułatwianie dostępu

do systemu ochrony zdrowia, przeciwdziałanie rozprzestrzenianiu się chorób ponad granicami, a także rozwój usług społecznych i rynku pracy wraz z ograniczaniem bezrobocia. Z kolei realizacja przedsięwzięć w ramach celu tematycznego „Granice” miała przyczynić się do polepszenia efektywności infrastruktury i procedur granicznych, poprawy bezpieczeństwa granic oraz zwiększonej przepustowości na przejściach granicznych, a także poprawa ich stanu (Program Współpracy..., s. 13-14).

Tymczasem pierwszy cel tematyczny („Dziedzictwo”) miał służyć „ochronie i propagowaniu dziedzictwa kulturowego i historycznego regionów transgranicznych, wzmacnianiu powiązań kulturowych i współpracy, poprawie wizerunku i atrakcyjności regionu oraz zwieszaniu potencjału społeczności lokalnych”. Jak wskazano w dokumencie programowym, istnienie dobrze utrzymanych obiektów dziedzictwa kulturowego i przyrodniczego powiązane zostało z rozwojem turystyki transgranicznej i sprzyjać miało zwiększeniu liczby turystów. W ramach celu tematycznego możliwa była realizacja przedsięwzięć służących poprawie stanu fizycznego „obiektów” kultury i dziedzictwa naturalnego oraz realizacja działań „miękkich”. Zaproponowane zostały m.in. następujące indykatoryjne przedsięwzięcia:

- wspólne inicjatywy i wydarzenia dotyczące promocji, rozwoju i zachowania kultury lokalnej i historii;
- wspólne projekty mające na celu wsparcie, promocję i zachowanie tradycyjnego rzemiosła, rękodzieła i umiejętności;
- wspólne projekty dotyczące przygotowania i realizacji inwestycji w infrastrukturę turystyczną i usługi zwiększające użytkowanie dziedzictwa kulturowego w turystyce (np. trasy rowerowe, ścieżki edukacyjne itp.), włączając uzupełniającą infrastrukturę turystyczną służącą korzystaniu z dziedzictwa kulturowego (np. stojaki na rowery, oznakowanie, infrastruktura dla osób ze specjalnymi potrzebami itp.);
- wspólne tworzenie produktów turystycznych, z poszanowaniem konieczności ochrony dziedzictwa kulturowego;
- stymulowanie współpracy międzyinstytucjonalnej w zakresie dziedzictwa historycznego i kulturowego (wymiana dobrych praktyk, wspólne szkolenia i inne działania powiązane);
- konserwacja, zachowanie i adaptacja lub rozwijanie dziedzictwa kulturowego do celów turystycznych oraz społecznych, kulturalnych, edukacyjnych i innych celów społeczności lokalnych;
- wspólne inicjatywy mające na celu poprawę obiektów funkcjonujących w sferze kultury;
- wspólne szkolenia i wymiany personelu mające na celu poprawę umiejętności w zakresie zarządzania dziedzictwem kulturowym, rozwoju wspólnych produktów i usług turystycznych, marketingu zasobów dziedzictwa z obszaru Programu i innych umiejętności powiązanych (Program Współpracy..., s. 10-11).

W ramach opisywanego celu tematycznego planowana była również modernizacja historycznych obiektów architektury.

Podsumowanie

Program Współpracy Transgranicznej Polska – Białoruś – Ukraina nie posługuje się pojęciem „bezpieczeństwa kulturowego”. Pojęcie „bezpieczeństwa” odnosi się wyłącznie do dwóch celów tematycznych: trzeciego – Wsparcie dla rozwoju ochrony zdrowia i usług socjalnych („Bezpieczeństwo”) – oraz czwartego – Promocja zarządzania granicami oraz bezpieczeństwem na granicach, zarządzanie mobilnością i migracjami („Granice”). Niemniej ochrona dziedzictwa kulturowego była jednym z istotnych celów tematycznych. Około 1/5 dostępnych środków przeznaczona była na realizację przedsięwzięć w ramach tego celu. Ogromne zainteresowanie Programem i tym obszarem wsparcia potwierdzały wyniki naborów, co pozwoliło na stwierdzenie, że zapotrzebowanie na realizację przedsięwzięć było znacznie większe niż dostępne środki.

Niewątpliwie, z uwagi na charakter możliwych działań w ramach pierwszego celu tematycznego, Program stwarzał warunki do utrwalenia i pielęgnowania wartości decydujących o tożsamości mieszkańców regionów przygranicznych. Potwierdzają to przyjęte wskaźniki Programu, tj. co najmniej 30 obiektów dziedzictwa kulturowego i historycznego, które zostaną udoskonalone dzięki wsparciu Programu oraz co najmniej 97 wydarzeń kulturalnych, które zostaną zorganizowane w jego ramach. Na tym etapie brak jest możliwości zweryfikowania, w jakim stopniu wskaźniki te zostały osiągnięte, m.in. z tego względu, że część projektów jest jeszcze w trakcie realizacji. Równocześnie ograniczenia spowodowane trwającą pandemią COVID-19 przyczyniły się do istotnej modyfikacji części projektów.

Można jednak przyjąć, iż Program poprzez zaplanowane w jego ramach działania zdecydowanie może przyczynić się do wzmocnienia bezpieczeństwa kulturowego w kraju.

Literatura

1. *Annual Report 2019* (2020), https://www.pbu2020.eu/files/uploads/pages_en/AIR/PBU14-20-%20Annual%20Report%202018-2019_Technical%20part_final.pdf (dostęp: 23.09.2021).
2. Czaja J. (2013), *Kulturowy wymiar bezpieczeństwa Aspekty teoretyczne i praktyczne*, Krakowskie Towarzystwo Edukacyjne, Oficyna Wydawnicza AFM, Kraków.
3. Dołzbłasz S., Raczyk A. (2011), *Projekty współpracy transgranicznej na zewnętrznych i wewnętrznych granicach Unii Europejskiej – przykład Polski*, „Studia Regionalne i Lokalne”, 3, 45, s. 59-80.
4. KE, *Interreg: European Territorial Cooperation*, https://ec.europa.eu/regional_policy/pl/policy/cooperation/european-territorial/ (dostęp: 23.09.2021).
5. EWT, *Programy Europejskiej Współpracy Terytorialnej i Europejskiego Instrumentu Sąsiedztwa*, <https://www.ewt.gov.pl/strony/o-programach/przeczytaj-o-programach/> (dostęp: 23.09.2021).
6. Hrynicki W.M. (2004), *Pojęciowe aspekty bezpieczeństwa kulturowego oraz jego zagrożenia w Europie*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje”, 16, s. 190-204.

7. Jemiolo T. (2001), *Bezpieczeństwo kulturowe w warunkach globalizacji i procesów społecznych*, [w:] *Kultura narodowa w kształtowaniu świadomości obronnej społeczeństwa i bezpieczeństwa państwa*, „Zeszyt Problematyki TWO”, 3, 25, s. 20-31.
8. Michałowska G. (1997), *Bezpieczeństwo kulturowe w warunkach globalizacji procesów społecznych*, [w:] Bobrow D.B., Haliżak E., Zięba R. (red.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, s. 131-143, Wydawnictwo Naukowe Scholar, Warszawa.
9. Oleksiewicz I. (2020), *Kryzys kulturowy Unii Europejskiej czy wzrost bezpieczeństwa tożsamości kulturowej Europejczyków?*, „Przegląd Geopolityczny”, 33, s. 155-172.
10. PBUa, <https://www.pbu2020.eu/pl/pages/231> (dostęp: 23.09.2021).
11. PBUb, <https://www.pbu2020.eu/pl/pages/244> (dostęp: 23.09.2021).
12. PBUc, <https://www.pbu2020.eu/pl/pages/330> (dostęp: 23.09.2021).
13. PBUd, <https://www.pbu2020.eu/pl/pages/404> (dostęp: 23.09.2021).
14. Program Współpracy Transgranicznej EIS Polska – Białoruś – Ukraina 2014-2020, https://www.pbu2020.eu/en/pdfviewer?url=../files/uploads/JOP/JOP%20PBU14-20_v.02.12.2020_PL_4th%20revision.pdf#book/ (dostęp: 23.09.2021).
15. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 232/2014 z dnia 11 marca 2014 r., <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:077:0027:0043:PL:PDF> (dostęp: 23.09.2021).
16. Włodkowska A. (2009), *Bezpieczeństwo kulturowe*, [w:] Wojtaszczyk K.A., Materska-Sosnowska A. (red.), *Bezpieczeństwo państwa. Wybrane problemy*, s. 143-171, Oficyna Wydawnicza ASPRA-JR, Warszawa.

CULTURAL SECURITY AND POLAND - BELARUS - UKRAINE CROSS-BORDER COOPERATION PROGRAMME 2014-2020

Abstract: Projects financed under the Poland – Belarus – Ukraine Cross-Border Cooperation Programme, support, among others, development processes in the polish-ukrainian – belarusian borderland. The projects are focused, among others on protection and promotion of cultural and natural heritage, increasing accessibility of regions, the development of infrastructure, as well as strengthening of health care, development of social services and improvement of border security. The main aim of the chapter is an attempt to assess the possible impact of the Poland – Belarus – Ukraine Cross-Border Cooperation Program on cultural security in Poland. The analysis covers the EU financial perspective for the years 2014-2020. The program documents and information on the results of project calls under the Program were analyzed.

Keywords: cultural security, EU programmes, cross-border cooperation

Rozdział 15

BEZPIECZEŃSTWO RELIGIJNE W II RP. ROZWAŻANIA NA KANWIE USTAW Z DNIA 21 KWIETNIA 1936 R.

Jerzy Nikołaajew²³

Streszczenie: Podpisane w dniu 21 kwietnia 1936 roku dwie ustawy: o stosunku Państwa do Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej i o stosunku Państwa do Karaimskiego Związku Religijnego w Rzeczypospolitej Polskiej stanowią przykład właściwie zabezpieczonych przez władze państwowe interesów w zakresie bezpieczeństwa religijnego w relacjach z tzw. związkami wyznaniowymi mniejszościowymi. Ustawodawca wyraźnie określił granice ingerencji organów państwa w działalność wspólnot muzułmańskich i karaimskich na terytorium Rzeczypospolitej okresu międzywojennego. Zachowując wynikającą z Konstytucji Marcowej uprzywilejowaną pozycję Kościoła katolickiego w Polsce, władze państwowe zapewniły także możliwość prowadzenia działalności religijnej pozostałym wyznaniom, ale na innych zasadach.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo religijne, okres II Rzeczypospolitej, wyznania mniejszościowe

Wprowadzenie

„Bezpieczeństwo” to pojęcie właściwie i dość obszernie opisane w literaturze. Choć trudne do zdefiniowania w przepisach prawnych, łatwo jest „przyswojone” w praktyce. Szeroko rozumiane także w doktrynie doczekało się tego, że zaczęto je traktować jako konglomerat większej całości, której elementem składowym stało się „bezpieczeństwo religijne”, zwane również bezpieczeństwem wyznaniowym” lub „bezpieczeństwem konfesyjnym”. W okresie II Rzeczypospolitej generalnie deklarowano akceptację dla wielowyznaniowości obywateli, nawiązując w ten sposób do tradycji sarmackiego „państwa bez stosów” i równego traktowania także tzw. innowierców. Ażyl wyznaniowy miał być także kontynuowany po odzyskaniu przez Polskę niepodległości, choć wyznawcy tzw. religii mniejszościowych mieli świadomość tego, że religia katolicka formalnie (konstytucyjnie) uzyskała przewagę nad innymi wyznaniem, również tymi uznanymi przez władze publiczne. Także wyznawcy religii muzułmańskiej i karaimskiej, skupieni głównie na terenie wschodnich rubieży państwa (przeważnie zamieszkujący województwo wileńskie), uzyskali możliwość swobody kultu religijnego, choć ich autonomia została mocno okrojona

²³ Uniwersytet Opolski, Instytut Nauk Prawnych

poprzez konieczność podporządkowania się przez nich wymogom państwowym, począwszy od uczestnictwa w wyborze najwyższych władz związków religijnych, poprzez formalną podległość w zakresie prowadzonej działalności oświatowej, majątkowej, ochronę zabytków, prowadzenia cmentarzy aż po konieczność składania przysięgi lojalnościowej wobec władz cywilnych II RP. Ingerencja państwowa w kwestie obsady personalnej we wspólnotach muzułmańskich i karaimskich mogła mieć jedynie uzasadnienie powodowane ważnymi względami związanymi z eliminowaniem potencjalnych ekstremistów religijnych, którzy wyposażeni w uprawnienia duchownych mogliby naruszać porządek i bezpieczeństwa publiczne, będące fundamentem funkcjonowania państwa w pierwszych jego latach samodzielnego bytu organizacyjnego. Stąd też regulacje ustawowe miały zabezpieczać interesy publiczne przed jednostkowymi uprawnieniami obywateli, którym *de facto* wolność sumienia i wyznania zapewniały obie ustawy zasadnicze z okresu II RP.

Podpisana dnia 21 kwietnia 1936 roku ustawa o stosunku Państwa do Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej (Dz.U. 1936 nr 30 poz. 240; Dz.U. 1945 nr 48 poz. 271 i 273) i datowana na 21 kwietnia 1936 roku ustawa o stosunku Państwa do Karaimskiego Związku Religijnego w Rzeczypospolitej Polskiej (Dz.U. 1936 nr 30 poz. 241; Dz.U. 1945 nr 48 poz. 271 i 273) to przykład regulacji państwowych świadczących o tym, że w tzw. polityce wyznaniowej II RP dobrze wykorzystano elementy związane z bezpieczeństwem państwa. Mimo wielowiekowej obecności w Polsce muzułmanów i karaimów władze potraktowały obydwie wspólnoty religijne jako obce kulturowo, a nawet religijnie, a przez to niepewne politycznie i potencjalnie mogące naruszać zasady konstytucyjne, w tym bezpieczeństwo najwyższych organów państwa. Dlatego też przyjęto szczególne zasady wzajemnego odnoszenia się do siebie, ale na zasadach zaproponowanych przez państwowego ustawodawcę.

Biorąc pod uwagę specyfikę obydwu wyznań (wcale nie najliczniejszych liczbowo), ale też to, że ich wyznawcy zamieszkiwali te same regiony państwa, oraz uwzględniając niektóre wspólne elementy doktrynalne obu religii, zdecydowano się na podjęcie niniejszej problematyki, akcentując tylko niektóre zagadnienia formalnoprawne oraz z zakresu bezpieczeństwa państwa związanego z funkcjonowaniem tzw. mniejszościowych związków wyznaniowych występujących w Polsce przed 1939 rokiem.

Bezpieczeństwo a bezpieczeństwo religijne

Pojęcie „bezpieczeństwa” jest pojęciem zdecydowanie wieloznacznym i różnie interpretowanym w zależności od sposobu jego ujęcia. Zupełnie odmienne koncepcje dotyczące bezpieczeństwa propagowali przedstawiciele różnych dziedzin nauki, począwszy od Arystotelesa, poprzez myśl Monteskiusza, Kanta, Fromma, Frycza-Modrzewskiego czy Masłowa. Za każdym jednak razem *in fine* wskazywano na to, co przyjęło się w znaczeniu potocznym oznaczającym *de facto* brak zagrożenia i poczucie komfortu związanego z obawą o to, co naruszać może bezpieczny stan rzeczy. Natomiast w rozumieniu doktryny nauk o bezpieczeństwie wyróżniono kilka kategorii bezpieczeństwa. Należy do nich bezpieczeństwo narodowe,

bezpieczeństwo wewnętrzne oraz bezpieczeństwo zewnętrzne. Pośród kategorii bezpieczeństwa wewnętrznego najczęściej uwzględnia się podział na bezpieczeństwo polityczne, ekonomiczne, militarne, publiczne, ekologiczne, energetyczne, personalne, strukturalne, informacyjne, społeczne, kulturowe i religijne (Szymonik 2011, s. 16). Według W. Pokruszyńskiego bezpieczeństwo definiuje się jako stan spokoju, pewności, wolności, braku realnych zagrożeń, strachu lub ataku, ale także jako proces społeczny i jako naczelną potrzebę i wartość człowieka oraz całych grup społecznych. Ten sam autor odniósł się do pojęcia „bezpieczeństwa religijnego”, ale bez próby jego zdefiniowania. Wskazał jedynie na zagrożenia „Kościoła w Polsce po 1989 roku”, co jednak nie może być przecież substytutem definicji bezpieczeństwa religijnego. Według niego tego rodzaju zagrożenia można podzielić na dwie grupy. Do pierwszej kategorii (duchowej) zaliczył „relatywizm moralny, liberalizm, fundamentalizm religijny, degenerację pojęcia małżeństwa, obniżenie wartości wspólnot religijnych i degradację autorytetu duchownego”. Do zagrożeń natury materialnej włączono z kolei „fizyczne niszczenie świątyń, rabowanie i nielegalne wywożenie dzieł sztuki sakralnej, kradzieże mienia kościelnego i napadanie na duchownych na tle nienawiści i chęci zysku” (Pokruszyński 2012, s. 222). Na bazie tychże kryteriów i po uwzględnieniu opinii W. Pokruszyńskiego, że bezpieczeństwo religijne należy systematyzować tuż obok bezpieczeństwa kulturowego, należy się zgodzić ze stanowiskiem A. Harbatskiego, że bezpieczeństwo religijne jest częścią bezpieczeństwa kulturowego oraz z koncepcją, że „określenie bezpieczeństwo religijne można w tym kontekście utożsamiać z pojęciem bezpieczeństwa (zachowania) religii tradycyjnej (prawosławie, katolicyzm)” (Harbatski 2015, s. 140). Jakkolwiek obydwaj (tzn. W. Pokruszyński i A. Harbatski) słusznie zwrócili uwagę na nietożsame wzajemnie pojęcia „bezpieczeństwa religijnego”, „bezpieczeństwa wyznaniowego” czy „bezpieczeństwa konfesyjnego”. Przyznając im rację, należy zaznaczyć przede wszystkim konieczność wyraźnego rozróżnienia znaczenia pojęć: „religia”, „wyznanie” i „konfesja” (łac. *confessio*). O ile „religia” traktowana jest najczęściej w kategoriach systemu wierzeń i praktyk religijnych, określających relacje pomiędzy *sacrum* a *profanum*, oraz manifestowania poprzez doktrynę, kult, wspólnotowość i sferę duchową, to „wyznanie” jest już zupełnie inną kategorią pojęciową. W naukach teologicznych przyjęto traktować wyznanie jako określenie grupy religijnej opartej na jednym zestawie prawd wiary. Stąd też *credo*, czyli wyznanie wiary (w religii katolickiej poprzez formułę „Wierzę w Boga”), ale także uznawanie za wyznanie grupy religijnej skupionej w jednej strukturze organizacyjnej lub w wielu takich strukturach. W przypadku „konfesji”, oznaczającej z łaciny wyznanie lub przyznanie się (do Boga), rozumienie tego pojęcia może być jeszcze bardziej wieloznaczne aniżeli w przypadku religii czy wyznania. Pod pojęciem „konfesji” można przecież rozumieć wyznawaną wiarę, samą spowiedź (stąd: konfesjonał), przedsięwzięcie przed grobem męczennika, grobowiec z relikwiami męczennika znajdujący się wewnątrz kościoła czy jako ozdobna obudowa takiego grobowca w formie baldachimu, tak jak np. u św. Piotra na Watykanie, św. Wojciecha w Gnieźnie czy św. Stanisława na Wawelu (Eliade 2007, s. 90).

Jednak z punktu widzenia bezpieczeństwa wewnętrznego spór terminologiczny co do rozumienia pojęć: „religii”, „wyznania” czy „konfesji” traktować należy jako

kategorię drugorzędną. W realiach współczesnych, ale też i historycznych, zasadnicze znaczenie mieć powinien interes państwa, bezpieczeństwo jego konstytucyjnych organów oraz porządek i bezpieczeństwo publiczne odnoszące się do ogółu obywateli. Dlatego też rozważania tego typu winny opierać się głównie na pojęciach wykorzystywanych przez ustawodawcę. Stąd też w ujęciu jurydycznym bezpieczeństwo i porządek publiczny trzeba analizować poprzez pryzmat postanowień konstytucyjnych, zarówno *Konstytucji Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 roku (Dz.U. nr 78 poz. 483 z późn. zm.), jak i obydwu ustaw zasadniczych z okresu międzywojennego: z dnia 17 marca 1921 r. (Dz.U. nr 44 poz. 267, ze zm.) oraz z dnia 23 kwietnia 1935 r. (Dz.U. nr 30 poz. 227). Ma to tym większe znaczenie, że bezpieczeństwo religijne II RP kształtowane było również poprzez odpowiednie przepisy ustawowe regulujące stosunki państwo – wspólnoty religijne reprezentujące mniejszości wyznaniowe. Także postanowienia obecnie obowiązującej *Konstytucji* zawierają tzw. klauzule limityzacyjne (art. 31 ust. 3 *Konstytucji RP*) *de facto* umożliwiające stosowanie ograniczeń w zakresie korzystania z konstytucyjnych wolności i praw ze względu m.in. na konieczność zapewnienia bezpieczeństwa i porządku publicznego. Należy jednak podkreślić, że zarówno *Konstytucja* z 1997 roku, jak i ustawy zasadnicze z 1921 roku i 1935 roku nie definiowały pojęcia „porządku i bezpieczeństwa publicznego”, co nie było wówczas i nie stanowi obecnie przeszkody w formułowaniu ograniczeń obywatelskich z uwzględnieniem tegoż kryterium oceny. Nie zmienia to w niczym możliwości wprowadzania takiego porządku prawnego, który przede wszystkim zabezpiecza interesy państwa, a nie tylko jego obywateli, także w sferze realizowanej wspólnotowo bądź indywidualnie wolności sumienia i religii (Abramowicz 2018, s. 52).

Stosunki państwowo-kościelne w II RP

Należy stanowczo podkreślić, że stosunki pomiędzy władzą państwową a związkami wyznaniowymi kształtowały się głównie na podstawie kryterium struktury wyznaniowej ludności zamieszkałej na terytorium II Rzeczypospolitej. Przyjęto wówczas szacować, że około 3/4 stanowili katolicy, w tym także wierni obrządku grekokatolickiego (11,2%). Z szacunków państwowych wynikało, że inne wyznania reprezentowali prawosławni i wyznawcy religii mojżeszowej (po 10,5%) oraz luteranie należący do Kościoła Ewangelicko-Augsburskiego (3,7%). Ponadto ok. 1,3% obywateli II Rzeczypospolitej deklarowało przynależność do innych poza wymienionymi wspólnotami religijnymi, w tym związków religijnych muzułmańskich i karaimskich (Sawicki 1937, s. 46). Wielość wyznań nawiązywała do wielowiekowej polskiej tradycji szacunku dla wyznawców różnych religii, jakkolwiek *Konstytucja Marcowa*, fundamentalny akt prawny regulujący kwestie wyznaniowe, nie tylko została „wyposażona” w sakralną inwokację, ale nade wszystko uznawała prymat jednego wyznania ponad innymi. Z art. 114 tej ustawy zasadniczej wprost wynikało, że „wyznanie rzymsko-katolickie będące religią przeważającą większości narodu zajmuje w Państwie naczelne stanowisko wśród równouprawnionych wyznań”. Tak doprecyzowana i przyjęta w *Konstytucji* formuła pojęciowa nie oznaczała jednak traktowania II Rzeczypospolitej jako państwa wyznaniowego, chociaż miała

nie tylko poważne konsekwencje jurystyczne, ale również następstwa praktyczne. Przede wszystkim naruszona została deklarowana zasada równouprawnienia Kościołów i innych związków religijnych, skoro jedno wyznanie uzyskało wyższość nad pozostałymi. W konsekwencji ustawodawca przyjął podział związków wyznaniowych na dwie kategorie: prawnie przez państwo uznanych i nieposiadających tego przymiotu, czyli prawnie nieuznanych. Oznaczało to, że tylko prawnie uznane związki wyznaniowe mogły urządzać zbiorowe i publiczne nabożeństwa, a także samodzielnie prowadzić sprawy wewnętrzne swoich związków wyznaniowych oraz posiadać majątek (ruchomy i nieruchomości) wraz z prawem rozporządzania nim, a nadto posiadać i używać własnych fundacji do prowadzenia działalności naukowej bądź dobroczynnej. Dodatkowo pozycja Kościoła katolickiego w relacjach z władzą świecką wzrosła po 1925 roku, czyli po podpisaniu konkordatu, na podstawie którego także państwo przyjęło na siebie konkretne obowiązki wynikające z tej umowy o charakterze międzynarodowym (*Konkordat pomiędzy Stolicą Apostolską a Rzeczpospolitą Polską z dnia 10 lutego 1925 r.*). Układ ze Stolicą Apostolską był wyłomem od zasady, na podstawie której stosunki między państwem a związkami wyznaniowymi były regulowane wyłącznie w drodze ustawowej po porozumieniu się z ich uprawnionymi przedstawicielami (reprezentacjami). Natomiast w przypadku Kościoła katolickiego postanowienia konkordatowe gwarantowały mu pełną wolność poprzez możliwość przyjęcia również swobody w zakresie administracyjnym i organizacyjnym oraz jurysdykcyjnym, a także majątkowym. Ustalono także status prawny duchowieństwa katolickiego i zakres podległości wobec władzy państwowej, która to władza miała realny wpływ na obsadę wyższych stanowisk w hierarchii kościelnej. Wiązało się to z koniecznością złożenia przysięgi wierności Rzeczypospolitej i lojalności wobec rządu (Łukomski 1934, s. 57). W tym zakresie rozwiązanie „konkordatowe” wprowadzono jako swego rodzaju wzorzec także do przepisów ustawowych regulujących stosunki Państwo – Kościół, również wobec muzułmanów i karaimów, jakkolwiek ich wspólnoty religijne nie mogą być kwalifikowane formalnie jako Kościoły (Pietrzak 1988, s. 8). Nie zmienia to jednak faktu, że władze państwowe okresu II RP dość długo i z pewnymi oporami wprowadzały nowe rozwiązania prawne dotyczące statusu tzw. Kościołów mniejszościowych. Tłumaczono to również spuścizną po zaborcach, którzy niejednakowo traktowali rozmaite denominacje religijne, uznając jedne, a delegalizując inne. Jednak zasadnicze trudności dotykać mogły tych obywateli Rzeczypospolitej, którzy nie deklaruwali swojego wyznania lub byli bezwyznaniowcami. Miało to związek z tzw. przymusem wyznaniowym, czyli koniecznością wpisywania w rubrykach urzędowych w miejscu przeznaczonym na „wyznanie” swojej przynależności konfesyjnej. Stąd też osoby niewyznające żadnej religii (także ateści) znaleźli się poza „marginiesem”, gdyż większość, a w zasadzie wszystkie dokumenty urzędowe znajdowały się przecież w rejestrach kościelnych (dokładnie instytucji religijnych). Stąd też np. akty chrztu lub zgonu, wystawiane najczęściej w urzędach parafialnych, były w zasadzie jedynymi dokumentami tożsamości. Nie przyjmowano też koncepcji neutralności religijnej (światopoglądowej) na rzecz prezentowania nie tylko wewnętrznej sfery duchowości obywateli i eksponowania symboli religijnych w przestrzeni publicznej (Świątkowski 1962, s. 91).

Jednocześnie władza państwowa deklarowała konieczność zapewnienia opieki moralnej i religijnej w zakładach podlegających bezpośrednio państwu, np. w wojsku, więzieniach, państwowych szpitalach czy publicznych szkołach. Jednak w oświacie państwowej przyjęto założenie, że nauka religii dla uczniów katolickich była obowiązkowa, tak samo jak zatrudnianie dla nich katechetów szkolnych czy kapelanów katolickich w więzieniach lub w armii. Formalnie też zezwolono wyznawcom religii mniejszościowych na zakładanie szkół (ale własnym sumptem) i na prowadzenie tam działalności wychowawczej, z tym że pod nadzorem państwowych władz oświatowych. Wobec wyznawców wszystkich religii stosowano konstytucyjną zasadę zakazującą wykorzystywania religii w sposób niezgodny z porządkiem ustawowym, porządkiem publicznym oraz obyczajowością publiczną. W praktyce miało to także przełożenie na zakaz uznania nowego lub dotąd prawnie nieuznanego związku wyznaniowego w przypadku stwierdzenia, że „jego urządzenia, ustrój wewnętrzny lub doktryna religijna były przeciwne porządkowi publicznemu lub obyczajności publicznej” (art. 115 i 116 *Konstytucji Marcowej*). Generalnie zakazywano też uchylania się od obowiązków wobec państwa z motywacji religijnej (np. odmowa służby wojskowej), a regulacje *Konstytucji* z 1921 roku co do pryncypiów dotyczących wolności sumienia i religii potwierdziła także *Konstytucja* z 1935 roku (Osuchowski 1967, s. 47; Abramowicz 2019, s. 15).

Regulacje wynikające z Ustawy z dnia 21 kwietnia 1936 r. o stosunku Państwa do Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej

Relacje pomiędzy Państwem a Muzułmańskim Związkiem Religijnym w II RP uregulowano głównie w przepisach ustawy z dnia 21 kwietnia 1936 r. Na tej podstawie władze państwowe przyznały wyznawcom islamu prawną możliwość praktykowania religijnego opartego na własnym statucie religijnym, ale na zasadach określonych przez organy władzy świeckiej. Według zamysłu ustawodawcy interes państwa (rozumiany także w kategoriach jego szeroko pojmowanego bezpieczeństwa) miał być chroniony poprzez zastosowanie konkretnych rozwiązań ustawowych.

Po pierwsze, przyjęto założenie, że związek ten miał być „niezależny od jakichkolwiek obcokrajowych władz duchownych i świeckich” (art. 1 ustawy). Takie rozwiązanie całkowicie eliminowało jakiegokolwiek obce wpływy, np. ze strony państw arabskich (czy szerzej muzułmańskich) oraz centrum światowego islamu zlokalizowanego przecież poza granicami RP. Tego typu „kontrola” dawała przynajmniej formalnie możliwość ingerencji władzy państwowej (np. porządkowej) w sytuacji wystąpienia ekstremizmów religijnych ze strony wyznawców religijnej mahometańskiej.

Po wtóre, autonomia tego związku religijnego została ograniczona także w ten sposób, że choć mógł on rządzić się własnym prawem wewnętrznym, to jednak jego statut musiał być zatwierdzony przez władzę państwową i dopiero po uznaniu tego statutu Muzułmański Związek Religijny mógł być „partnerem” w relacjach z władzą II RP. Dlatego też Prezes Rady Ministrów (w tym przypadku Sławoj Składkowski) 26 sierpnia 1936 roku (czyli niedługo po wejściu w życie ustawy) podpisał stosowne

przepisy (Rozporządzenie Prezesa Rady Ministrów z dnia 26 sierpnia 1936 r. o uznaniu Statutu Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej). W ten sposób zrealizowano delegację wynikającą z art. 2 ustawy a realizację tych przepisów wykonawczych „poruczono” Ministrowi Wyznań Religijnych i Oświecenia Publicznego (pod tekstem rozporządzenia znajduje się podpis ówczesnego szefa tego resortu W. Świętosławskiego) „w porozumieniu z innymi ministrami”. I choć tych nie wskazano wyraźnie, to bez wątplenia leżało to w kompetencji ministra właściwego do spraw wewnętrznych a także w ograniczonym zakresie ministrów odpowiedzialnych za sprawy zagraniczne, wojskowe, sprawiedliwości, finansów (każdego według ich właściwości rzeczowej).

Po trzecie, władze państwowe miały również pośredni wpływ na obsadę stanowiska muftiego, skoro zdecydowano, że muftiego wybierało Najwyższe Kolegium Muzułmańskie spośród listy kandydatów zatwierdzonych przez Ministerstwo Wyznań i Oświecenia Publicznego. Dodatkowo jeszcze angażowano w procedurę wyboru muftiego wojewodę wileńskiego (Wilno było siedzibą muftiego – art. 4 ust. 2 ustawy), którego uczyniono pośrednikiem wymiany korespondencji „wyborczej” pomiędzy Kolegium a Ministerstwem. Jednocześnie ministrowi przyznano kompetencje do udzielania dyspensy od niektórych wymogów dla kandydata na stanowisko muftiego („w szczególnych wypadkach”). Chodziło tu o warunki dotyczące obywatelstwa polskiego, znajomości języka polskiego, wieku (ukończone 40 lat) oraz ukończenia studiów wyższych teologicznych lub języków wschodnich. Zwłaszcza możliwość udzielenia ministerialnej dyspensy ze względu na niespełnienie przesłanki obywatelstwa polskiego i znajomości języka polskiego świadczyła o faktycznej kontroli ze strony wojewody i ministerstwa. Także po ukończeniu wyborów na stanowisko muftiego jeden z egzemplarzy protokołu końcowego musiał być obowiązkowo wysyłany do ministerstwa za pośrednictwem wojewody wileńskiego i po zasięgnięciu jego opinii w tej sprawie.

Po czwarte, wybór muftiego bezwzględnie wymagał zatwierdzenia przez Prezydenta RP, a w rocie przysięgi składanej przez muftiego przed ministrem umieszczono formułę: „obietuję i przysięgam, że zachowując wierność Rzeczypospolitej, szanować będę Rząd Konstytucją ustanowiony i że sprawię, aby go szanowało podległe mi duchowieństwo. Dbały o dobro Rzeczypospolitej nie będę uczestniczył w żadnych poczynaniach, ani żadnych naradach, które by mogły przynieść szkodę Państwu Polskiemu lub porządkowi publicznemu. Przeciwnie, będę się starał usuwać wszelkie niebezpieczeństwa, o których bym wiedział, że zagrażają Państwu lub porządkowi publicznemu”. Stąd też dopiero po „lojalnościowej” deklaracji mufti mógł objąć swój urząd.

Po piąte, także członkowie Najwyższego Kolegium Muzułmańskiego (również ich zastępcy), czyli wybierający muftiego, musieli być zatwierdzeni przez ministerstwo i przed objęciem urzędu składali przysięgę przed wojewodą wileńskim (lub jego zastępcą), jednak bez tak ewidentnych odwołań do uprawnień władzy państwowej, jak w przypadku samego muftiego. Wymagano jednak od członków Kolegium, ażeby zwołując tzw. Wszechpolski Kongres Elekcyjny, powiadamiać z miesięcznym wyprzedzeniem ministerstwo. Podczas posiedzeń Kongresu delegowani przez ministra jego przedstawiciele mieli prawo aktywnego uczestnictwa, a nadto odpisy

protokołów z posiedzeń Kongresu za pośrednictwem wojewody wileńskiego wysyłano do ministerstwa. W ten sposób władze państwowe w Wilnie i w Warszawie na bieżąco monitorowały decyzje (nie tylko organizacyjne) najwyższych władz religijnych wyznawców islamu w Polsce.

Po szóste, tworzenie i znoszenie muzułmańskich gmin wyznaniowych na obszarze całego państwa, a także zmiany granic lub siedzib tych gmin wymagały uprzedniej zgody ze strony ministerstwa, choć formalnie dokonywało się to na podstawie stosownych zarządzeń Najwyższego Kolegium Muzułmańskiego. Ponadto wybór imama, czyli duchownego stojącego na czele gminy wyznaniowej, wymagał uprzedniej zgody wojewody wileńskiego, któremu pozostawiono możliwość złożenia sprzeciwu co do osoby kandydującej na ten urząd. Poza tym imamowie (także mu-ezini) przed objęciem stanowiska składali przysięgę przed starostą, a w przypadku stwierdzenia szkodliwej dla Państwa działalności wojewoda mógł żądać usunięcia takich duchownych ze stanowiska i w ostateczności uznać nawet takie stanowisko za opróżnione. Tak dalece posunięta ingerencja wojewody mogła być tłumaczona wyłącznie interesem bezpieczeństwa społeczności lokalnych, głównie z terenów Wileńszczyzny.

Po siódme, w ustawie (art. 34 ust. 1) postanowiono, że „podczas nabożeństwa w piątki każdego tygodnia oraz w dniu uroczystych świąt muzułmańscy duchowni odmawiać będą modlitwy za pomyślność Rzeczypospolitej i Jej Prezydenta, w dniu zaś świąt państwowych odprawią uroczyste nabożeństwo na intencję Rzeczypospolitej, Jej Prezydenta, Rządu i Wojska”. Taka formuła przyjęta w ustawie świadczyć może o akceptacji (wymuszonej?!) środowiska polskich muzułmanów wobec władzy państwowej i jej działań, jakkolwiek z uwagi na obiektywne trudności związane z brakiem dostępu do źródeł (tekstu projektu ustawy) trudno jednoznacznie stwierdzić, że tego typu rozwiązanie zostało zaproponowane przez duchownych reprezentujących Muzułmański Związek Religijny w Rzeczypospolitej Polskiej.

Po ósme, państwowe władze oświatowe oraz ministerstwo sprawowało ogólny nadzór nad szkolnictwem wyznaniowym dotyczącym religii muzułmańskiej, a jednocześnie Najwyższe Kolegium Muzułmańskie mogło otwierać własne szkoły duchowne, ale tylko za zgodą ministerialną. Także nauczycieli w tych szkołach mianował i zwalniał mufti, tyle że w porozumieniu z właściwymi władzami szkolnymi (kuratoria oświaty).

Po dziewiąte, kwestie związane z zakładaniem, rozszerzaniem lub zamykaniem oraz zarządaniem cmentarzami wyznaniowymi wyłączono spod kompetencji władz Muzułmańskiego Związku Religijnego i polecono stosowanie przepisów państwowych o cmentarzach wyznaniowych (art. 40 ustawy). W ten sposób zadbanie o ujednolicenie przepisów dotyczących prawa funeralnego w Polsce i o podległość wszystkich cmentarzy właściwym władzom sanitarnym.

Po dziesiąte, choć ustawodawca w art. 38 ustawy zapewnił Związkowi otrzymywanie dotacji obejmujących wydatki osobowe i rzeczowe, jednak te ustalano corocznie w budżecie państwowym i były one przyznawane przez ministerstwo w wysokości określonej przez władze państwowe. Nie zawsze jednak przekazywane kwoty odpowiadały zgłaszanym wcześniej zapotrzebowaniom.

Po jedenaste, ustawodawca (w art. 35 ustawy) zagwarantował Związkowi prawo posiadania, obciążania, zbywania i nabywania majątku oraz rozporządzania nim, jednak na podstawie art. 37 ustawy ograniczył obrót nieruchomościami w ten sposób, że wprowadził tu wymóg uzyskania zgody ze strony właściwego terytorialnie wojewody. W innym miejscu ustawy (art. 39) zdecydowano, że „majątek ruchomy i nieruchomy mający w myśl obowiązującego ustawodawstwa charakter zabytkowy podlegał odnośnym przepisom o opiece nad zabytkami”. W ten sposób zobowiązano władze związku religijnego do właściwego utrzymania głównie obiektów sakralnych i nakazano współdziałanie ze służbami państwowymi odpowiedzialnymi za utrzymanie zabytków w Polsce.

Regulacje wynikające z Ustawy z dnia 21 kwietnia 1936 r. o stosunku Państwa do Karańskiego Związku Religijnego w Rzeczypospolitej Polskiej

Ustawa o stosunku Państwa do Karańskiego Związku Religijnego w Rzeczypospolitej Polskiej była wzorowana na opublikowanej w tym samym Dzienniku Ustaw, ale pod wcześniejszą pozycją, ustawą o stosunku Państwa do Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej. Ta sama data prezydenckiego podpisu nie jest także przypadkowa, gdyż prace parlamentarne i wcześniejsze uzgodnienia w ministerstwie i w parlamencie co do projektów obu ustaw musiały być prowadzone w zasadzie równolegle. Wiele podobieństw wynika także z końcowej redakcji przepisów ustawy dotyczącej wyznawców religii karańskiej. W przypadku Karańskiego Związku Wyznaniowego – ta wspólnota religijna mogła funkcjonować jako wyznanie prawnie uznane dopiero po zatwierdzeniu przez Prezesa Rady Ministrów jego statutu (Rozporządzenie Prezesa Rady Ministrów z dnia 26 sierpnia 1936 r. o uznaniu Statutu Karańskiego Związku Religijnego w Rzeczypospolitej Polskiej). Podobnie jak w przypadku wyznawców religii islamskiej przewidziano kontrolę ze strony państwa w zakresie wyboru hachana (samej procedury jego wyboru, sprzeciwu co do kandydatów na ten urząd, przesłania do ministerstwa pełnej dokumentacji z czynności wyborczych). Poza tym w art. 9 ustawy karańskiej przyjęto niemal identyczną rotę przysięgi hachana jak w przypadku muzulmańskiego muftiego, uwzględniającą wymóg aktu wierności wobec władzy i podporządkowania się jej prawom. Także organ doradczy hachana, czyli Karański Zarząd Duchowny (podobnie jak Najwyższe Kolegium Muzułmańskie), podlegał władzy wojewody i ministerstwa. Na podobieństwo ustawy muzulmańskiej uregulowano kwestie dotyczące majątku tego związku religijnego, w tym nieruchomości, opieki nad zabytkami, dotacji państwowych, cmentarzy wyznaniowych, a także szkolnictwa wyznaniowego, odstępstw ministerialnych od wymogów dla kandydatów na hachanów, modlitw (w świąteczną sobotę) za władze publiczne oraz tworzenia gmin wyznaniowych, ponadto nabywania, zbywania, obciążania, zarządzania i rozporządzania majątkiem. Identycznie jak w przypadku ustawy muzulmańskiej „wykonanie ustawy niniejszej poruczono Ministrowi Wyznań Religijnych i Oświecenia Publicznego w porozumieniu z zainteresowanymi ministrami”.

Podsumowanie

Bezpieczeństwo religijne w kategoriach pojęciowych należy traktować jako zjawisko w miarę nowe. Natomiast biorąc pod uwagę faktycznie realizowane zasady związane z bezpieczeństwem państwa w relacjach ze wspólnotami religijnymi, to bezpieczeństwo religijne miało być od zawsze gwarantem zabezpieczenia interesów państwowych. Dopiero w dalszej perspektywie gwarantowano wolność jednostki oraz wspólnot o charakterze religijnym. Jednak za każdym razem za dobro nadrzędne uznawano porządek i bezpieczeństwo państwa, i to władze państwowe, a nie władze religijne, określały zasady tzw. polityki wyznaniowej. W okresie II RP w obydwu ustawach określono stosunek Państwa do (szeroko rozumianych) wyznawców religii muzułmańskiej i karaimskiej, a nie odwrotnie: Związku Religijnego Muzułmanów i Związku Religijnego Karaimów do Państwa. Gdyby przyjąć odwrotne założenie, wówczas można by domniemywać, że to wspólnoty religijne dyktowały władzy zasady wzajemnych relacji. W rzeczywistości to władza publiczna dokonywała uznania związku religijnego za legalny i nadawała mu określone uprawnienia, także natury majątkowej, regulując w formie ustawowej pozycję formalnoprawną m.in. muzułmanów i wyznawców religii karaimskiej w Polsce.

Analizując zakresłone w tytule zagadnienia, należy odnieść je i zestawić z ówczesnymi realiami politycznymi i prawnymi okresu międzywojnia w Polsce. Trzeba uwzględnić fakt, że polityka bezpieczeństwa w ogólności i polityka wyznaniowa młodego państwa (po latach niewoli) uwarunkowana była przecież spuścizną legislacyjną po zaborczych porządkach prawnych i uwzględniającą dominujące wcześniej w poszczególnych regionach wyznania religijne. Zwłaszcza we wschodnich województwach polityka wyznaniowa państwa była zdecydowanie bardziej radykalna aniżeli gdzie indziej. Z jednej strony pod koniec lat 30. XX wieku prowadzono dyskryminacyjne działania związane z burzeniem cerkwi prawosławnych na Chełmszczyźnie i części Podlasia, a z drugiej strony wyznawcy religii mahometańskiej i karaimskiej w ramach uznania państwowego uzyskali przynajmniej formalne gwarancje (tzn. ustawowe) umożliwiające im swobodę uzewnętrzniania swojej religii. Zresztą postanowienia konstytucyjne zawarte w obu ustawach zasadniczych okresu II RP formalnie gwarantowały swobodę religijną dla wyznawców wszystkich religii, także tzw. mniejszościowych związków religijnych, co w praktyce wcale nie oznaczało, że władze państwowe nie pozostawiły sobie marginesu swobody oceny tego, co może realnie zagrażać interesom publicznym. Można więc zaryzykować tezę, że bezpieczeństwo państwa było nieodłącznie związane z bezpieczeństwem religijnym, jakkolwiek nie podnoszono kwestii wzajemnych relacji pomiędzy poszczególnymi, nawet antagonizującymi się związkami wyznaniowymi. Pomijano, zupełnie niesłusznie, aspekt związany z ewentualnymi sporami o charakterze doktrynalnym, prozelickim czy majątkowym, a nade wszystko eksponowano interes ogólny (państwowy, publiczny). Stąd też organy władzy wojewódzkiej (szczególnie wojewody wileńskiego) oraz centralne (ministerialne) wyposażono w niemałe atrybuty kontrolno-nadzorcze, a te były związane z koniecznością zapewnienia bezpieczeństwa społeczności lokalnej. Co prawda polscy muzułmanie i polscy karaimowie zostali uznani przez państwo za wspólnoty mogące legalnie funkcjonować w obrocie

prawnym, ale szacunek władz w stosunku do nich bardziej był dyktowany obawami przed ewentualnymi rozruchami o podłożu religijnym aniżeli ścisłym realizowaniem funkcji państwa jako gwaranta wolności religijnej wszystkich jego obywateli. Brak zaufania organów władzy do związków religijnych mniejszościowych wcale nie był neutralizowany poprzez wzajemne uczestnictwo władz religijnych w uroczystościach państwowych, i na odwrót – władz państwowych w obchodzeniu świąt muzułmańskich czy karaimskich. Owa nieufność powodowała także konieczność składania lojalnościowych wobec władzy państwowej deklaracji i akceptacji dla państwowych zasad prawnych, w tym niepopadania w konflikt z regułami porządku i bezpieczeństwa określonego w regulacjach wydanych przez władze publiczne, a nie według zasad wynikających z prawa wewnętrznego związków religijnych.

Na koniec należy podkreślić niemal identyczność (wyraźne podobieństwo) redakcyjne obu ustaw i na tej podstawie traktować je jako pakiet prawie bliźniaczych rozwiązań legislacyjnych. Trzeba również zauważyć zbieżność czasową związaną z podpisaniem tych ustaw, przyjęciem również podobną ścieżką legislacyjną i opracowanie ostatecznego tekstu przepisu prawnego według propozycji przedstawionych przez stronę rządową. Brak silnego lobby wyznaniowego zdecydował o takim kształcie obu „wyznaniowych” ustaw pochodzących z dnia 21 kwietnia 1936 roku, który wyraźnie zabezpieczał interes związany z bezpieczeństwem publicznym. W tym znaczeniu obydwie regulacje wpisać należy do katalogu przepisów państwowych będących gwarantami uprawnień „silniejszego”.

Literatura

1. Abramowicz A. (2019), *Naczelne stanowisko wyznania rzymskokatolickiego a równouprawnienie wyznań w prawie II Rzeczypospolitej*, „Przegląd Prawa Wyznaniowego”, 11, s. 5-22.
2. Abramowicz A. (2018), *Równouprawnienie związków wyznaniowych w prawie polskim*, Wydawnictwo KUL, Lublin.
3. Eliade M. (2007), *Słownik religii*, Wydawnictwo Książnica, Warszawa.
4. Harbatski A. (2015), *Tożsamość religijna a bezpieczeństwo konfesyjne: współczesne wyzwania (na przykładzie Republiki Białoruś)*, „Pogranicze. Studia Społeczne”, XXV, s. 135-150.
5. *Konkordat pomiędzy Stolicą Apostolską a Rzeczpospolitą Polską z dnia 25 lutego 1925 r.*, (Dz.U. nr 72 poz. 501).
6. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. nr 78 poz. 483, ze zm.).
7. Łukomski S. (1934), *Konkordat zawarty dnia 10 lutego 1921 roku pomiędzy Stolicą Apostolską i Rzeczpospolitą Polską*, Wydawnictwo Unitas, Łomża.
8. Marczevska-Rytko M. (1997), *Religie niechrześcijańskie w Polsce*, Wydawnictwo UMCS, Lublin.
9. Osuchowski J. (1967), *Prawo wyznaniowe Rzeczypospolitej Polskiej 1918-1939 (Węzłowe zagadnienia)*, Książka i Wiedza, Warszawa.
10. Pietrzak M. (1988), *Prawo wyznaniowe*, PWN, Warszawa.
11. Pokruszyński W. (2012), *Bezpieczeństwo. Teoria i praktyka*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide de Gasperi w Józefowie, Józefów.
12. Rozporządzenie Prezesa Rady Ministrów z dnia 26 sierpnia 1936 r. o uznaniu Statutu Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej (Dz.U. 1936 nr 72 poz. 517).

13. Rozporządzenie Prezesa Rady Ministrów z dnia 26 sierpnia 1936 r. o uznaniu Statutu Karaimskiego Związku Religijnego w Rzeczypospolitej Polskiej (Dz.U. 1936 nr 72 poz. 518).
14. Sawicki J. (1937), *Studia nad położeniem prawnym mniejszości narodowych w Państwie Polskim*, Kasa im. Mianowskiego, Warszawa.
15. Szymonik A. (2011), *Organizacja i funkcjonowanie systemów bezpieczeństwa*, Difin, Warszawa.
16. Świątkowski H. (1962), *Wyznaniowe prawo państwowe*, PWN, Warszawa.
17. Ustawa z dnia 17 marca 1921 r. *Konstytucja Rzeczypospolitej Polskiej* (Dz.U. nr 44 poz. 267, ze zm.).
18. Ustawa Konstytucyjna z dnia 23 kwietnia 1935 r. (Dz.U. nr 30 poz. 227).
19. Ustawa z dnia 21 kwietnia 1936 r. o stosunku Państwa do Muzułmańskiego Związku Religijnego w Rzeczypospolitej Polskiej (Dz.U. 1936 nr 30 poz. 240; Dz.U 1945 nr 48 poz. 271 i 273).
20. Ustawa z dnia 21 kwietnia 1936 r. o stosunku Państwa do Karaimskiego Związku Religijnego w Rzeczypospolitej (Dz.U. 1936 nr 30, poz. 241; Dz.U. 1945 nr 271 i 273).

THE RELIGIOUS SECURITY IN THE SECOND POLISH REPUBLIC. CONSIDERATIONS BASED ON THE ACTS OF APRIL 21, 1936

Abstract: Two laws signed on April 21, 1936: on the relationship of the State to the Muslim Religious Union in the Republic of Poland and on the relationship of the State to the Karaim Religious Union in the Republic of Poland are an example of interests properly secured by the state authorities in relations with so-called minority religious associations. The legislator clearly defined the limits of interference by state organs in the activities of Muslim and Karaim communities in the territory of the Republic of Poland in the interwar period. Maintaining the privileged position of the Catholic Church in Poland resulting from the March Constitution, the authorities also ensured the possibility of conducting business activity to other denominations, but on different terms.

Keywords: the minority denominations, the period of the Second Polish Republic, the religious security, the security

Rozdział 16

THE ELEMENTS OF MANAGEMENT IN DESTRUCTIVE APOCALYPTIC GROUPS ON SELECTED EXAMPLES

Robert Janik²⁴

Abstract: The subject of destructive cults has repeatedly occupied public attention. Often, this has been caused by the dangerous situations caused by spectacular collective suicides, killing those who dare criticise them or the acts of terrorism force one to reflect upon the essence of their activities as well as upon the dangers related to them. What are the characteristic features of these groups and how are they organised also proved to be important. A major place among them is occupied by apocalyptic sects, focusing their attention in a special way on issues connected with the end of the world, in which they are often supposed to play an important role. Among them, one can distinguish following groups: 1) referring to Christianity; 2) drawing inspiration from Far Eastern religions; 3) inspired by the belief in UFO; and 4) related to the New Age. Despite their doctrinal diversity, there are some similarities in their management. Understanding the governance mechanisms of these organisations, forms of leadership as well as disturbing doctrinal features, can help to identify the dangers associated with their activities.

Keywords: apocalyptic sects, destructive cults, governance mechanisms, management, organisations

Introduction

The role of religion in the life of the world is often underestimated. And yet, it was precisely for religious and political reasons that monumental buildings were erected in antiquity, which, as is the case of the pyramids, have become the symbols of the power of the cultures that created them. It can be said without exaggeration that these actions mark the very beginnings of large-scale management (Witzel 2012, pp. 9-22; Wren 1994, pp. 13-21). Also, the further development of this discipline is connected with the activities of various religious organisations, which have been created over the centuries; they were powerful economic structures, which also stimulated the economic development of numerous countries (Nisbet 1976, pp. 221-263). However, the economic interests of religious groups did not always bring

²⁴ Częstochowa University of Technology, Faculty of Management

positive social effects; some of them took advantage of the naivety and good will of their followers to satisfy their own selfish desires.

Nowadays, in religious groups, especially those conventionally referred to as “sects”, one can also encounter the cases of manipulation, cheating, exploitation and depriving people of the possibility of making independent decisions about their life (Gasper, Müller, Valentin 1994, pp. 974-982).

It is particularly important to study the ways in which those religious groups which are infamous for their extreme approach to “the end of the world” act; often, one can observe in them a puzzling mixture of purely earthly managerial practices, combined with leadership tendencies and the cult of leaders, that teachings and behaviour are often marked by self-destructive tendencies.

Despite the importance of the ideology and worship of these religious organisations, they are active in one form or another in societies, and often seeking the ways to influence them. It is not uncommon for them to behave pragmatically, although it is not a rule. It is interesting to know how these groups are managed and how they act in the world that they often perceive as dangerous and “tainted by evil”.

The general characteristics of apocalyptic sects

Among the wide range of contemporary non-orthodox religious groups, so-called “apocalyptic sects” play a special role. This is not because of their numbers, but because of their often strange behaviour, which has led to tragedies many times in the past. These groups try to change the existing world order and refer to the expectations of the “final end”. Not seldom do they try themselves to accelerate the global destruction by use of violence, which poses serious threats to their members and the societies in which they exist (Gallagher 2005). Of course, not all groups showing apocalyptic interests are dangerous; the vast majority of them do not manifest any murderous or terrorist tendencies, nor do they persuade their members to commit suicide or mutilations. Although the groups classified as extreme religious groups with apocalyptic tendencies are, to a large extent, syncretistic, in analysing the sources of their doctrinal concepts, 4 main ideological sections can be distinguished in these regard: 1) referring to Christianity; 2) oriented to Far Eastern religions; 3) inspired by UFOs and 4) connected to the New Age-ideology.

Ad 1. The first one is characterised by faith in the imminent end of the world; as a rule, the faith in the thousand-year reign of Jesus, which is to put an end to the existing order of the world, is invoked are used in this context. The most famous quasi-ecclesial groups, of this type include the **Temple of the People**.

The **Peoples Temple of the Disciples of Christ** was founded in Indianapolis, United States by James Warren (Jim) Jones (1931-1978), in 1956. Its ideology was a mix of Pentecostal doctrine, the concepts of Martin Luther King, Father Divine and Gandhi, as well as the teaching of communists leaders like Marx, Lenin and Castro. Jones managed to rally under dissatisfied with the existing social, political and religious situation in the United States under his banner. The afore-mentioned Father Divine (circa 1876-1965) was a black religious leader and campaigner for racial equality, who ascribed divine powers to himself. J. Jones took some of his teachings and

concepts from Father Divine's social movement, the International Peace Mission. His speeches against racism rendered J. Jones popular with some of the public; he himself adopted children of different races, creating the so-called "Rainbow Family".

Throughout his career, the leader of the Peoples Temple developed close ties with influential people from the American establishment, including politicians. As a rule, the latter showed considerable interest in seeking electoral support from various types of religious leaders. Practice shows that ecclesial communities, having developed organisational structures, can mobilize their followers, as well as influence the public opinion by using the members of their communities as "electoral helpers". Donations, often from sources raising justified suspicions with which the leader of the Peoples Temple supported his "political friends", were also important. In return for this kind of help, they willingly showed themselves in public with Jones, thus giving his "mission" the appearance of seriousness and recognition on the part of those in power. Despite the political success, events inside the Peoples Temple took an increasingly disturbing direction in the 1970s; the members of this community were forced to perform slave labour, subjected to humiliating punishments in the event of insubordination, and often imprisoned against their will. Gradually, J. Jones's eccentric and dictatorial behaviour brought public criticism on the Peoples Temple. Regardless of his initially good contacts with the media, increasingly negative opinions about the "pastor" began to appear in them. The police also began to show interest in the activities of the Peoples Temple, alerted by the concerned families of the members, and began investigating the activities of the community, reaching increasingly disturbing conclusions. James's reaction to this development was not long in coming; feeling confident that his paranoid fears of a "conspiracy" were justified, he decided to disappear from the eyes his "persecutors", leaving the United States and moving the Peoples Temple's headquarter to Guyana, where the group had purchased grounds (in Jonestown).

According to the plan, the community living there should be "autarkic" (self-sufficient), building an ideal society combining the features of communism with the religious doctrine proclaimed by Jones. In practice, it failed in every way, convincing the paranoid leader, who struggled to hold back a "mass desertion" by terror, that "the end is coming". The factor that directly accelerated the tragedy was the arrival at the camp of senator Leo J. Ryan, who was concerned about the news of the abuse in the Peoples Temple. He was murdered on 18th November, 1978, by Jones's men and on his orders, shortly after some members of the Peoples Temple had approached him for help. After this incident, Jones knew he would be held responsible for his actions. Therefore, he decided to annihilate his religious community, using in practice the "variant of voluntary death", which had been practiced with his followers many times before; as a result of this, about 900 of its members took their own lives. The tragic end of the Peoples Temple was associated with the process of the gradual "incapacitation of the adherents" and the psychological degeneration of its leader, who, endowed with the hallmarks of absolute power, transformed from a religious activist, committed to overcoming the effects of social injustice and racial inequality,

into an oppressor of his followers and the perpetrator of their destruction (Kilduff, Javers 1978, pp. 103-188).

Ad 2. The second section, encompassing dangerous apocalyptic groups originating from Far Eastern religions, is composed of those which draw their ideological inspiration mainly from Buddhism, Hinduism, Shinto and many local Asian cults. There have been strong syncretistic accents in it. The most famous, due to the tragic events with its participation, is Aum Shinrikyo (the Supreme Truth) (Wiebus 1997, p. 47). Aum Shinrikyo was founded in Japan on the initiative of Shoko Asahara (real name: Chizuo Matsumoto, 1955-2018), which began its public activity in the 1980s. The doctrine he created contained a mixture of the elements of Buddhism, Hinduism, Nostradamus prophecies, chiliasm, science fiction, fascination with technology, anti-Semitism and esotericism. Asahara, a nearly blind “truth-seeker”, showed great cunning in securing the appearance of “recognition” by respected religious authorities; he even managed to meet the Dalai Lama, which was publicly acknowledged as the acceptance of the religious role of the leader of the Supreme Truth for the part of the head of Tibetan Buddhism. Most likely, the Dalai Lama himself was unaware of Asahara’s plans and his actual teachings. Initially, Soko Asahara dealt with yoga and Chinese medicine, promoting asceticism and disregarding worldly life as *vanitas vanitatum, et omnia vanitas* (Hope, Loon van 2008, pp. 121-135). Soon, however, he felt a messianic vocation, which prompted him to proclaim that mankind was in danger of extinction, from which he wished to save it. A characteristic role in his plans was played by Japan, which was the “chosen” country which the self-proclaimed saviour of mankind wanted to act as a protective sphere, making it a “base for saving the whole world”. There were many indications that Asahara had great political ambitions and wanted to play the role of the state leader (Kaplan, Marshall 1996, pp. 50-499). His stance on his earlier concept of “saving the earth” changed after Aum Shinrikyo’s failure in the Japanese parliamentary elections in 1990, in which the organisation suffered a severe defeat; none of its candidates won the expected mandate. In this situation, the guru of the sect began to proclaim from the mid-1990s that the end of the world was near and that Japan was to be annihilated in the Battle of Armageddon, from which the Millennial Kingdom would emerge with Asahara as a regent, and that which confirmed his interest in having secular power.

The prophecies disseminated by the Supreme Truth turned out to be only a screen behind which there were hidden secret plans for Asahara to gain the earthly power. In fact, Aum Shinrikyo planned a coup in Japan, which was to be preceded by a landing of its militants arriving across the sea—from Russia.

The action plan assumed entering Tokyo by the armed formations of the sect; simultaneously, a gas attack should take place and important military points be taken over by loyal “guru’s soldiers”. The members of the lawful government were to be exterminated, and Asahara was planned to be declared the leader of the nation and the founder of theocracy. A specific accelerator was the earthquake that destroyed the Japanese city of Kobe on 17th January, 1995, and killed 5,500 people. Asahara recognised the above event as a result of the United States’ use of a previously unknown weapon against Japan and announced that “the war has already begun”. Initially, he limited himself only to verbal attacks on “enemies”, without taking any

radical actions. However, when news spread that the Japanese police were planning to search the Aum Shinrikyo buildings on 21st March, the sect's chief ordered a strike; on 18th March, he gave the cult chemist Seiichi Endo the appropriate instructions, which resulted in a series of attacks using poisonous gas (sarin) on non-military targets in Japan. In the first of the genocidal attacks, which took place on 20th March, 1995, a crowd of innocent victims using the Tokyo city train was targeted; 9 people died and 5,200 were injured. After another attack, on 19th April, 1995, conducted at the Yokohama railway station, 300 people had to seek medical attention. Moreover, the Supreme Truth tried to intimidate those investigating its ease and organised attacks against them. The sect's murderous activities were finally brought to an end by the arrest of its leaders, along with the guru Asahara, on 16th May, 1995, and sentencing them to many years of prison. A few days before the capture of the head of Aum Shinrikyo (5th May), an attempt was made by his supporters to attack the Tokyo collector's station again by using the gloomy World War II cyclone B, and it was only thanks to the vigilance of passers-by that it was possible to prevent the catastrophe. The police said the attack used enough poison to kill 10,000 people (Nordhausen, Billerbeck 1999, pp. 522-533).

The fall of the sect in Japan entailed its banning in other countries, including Russia, where a large number of parents had already tried to regain their children, who had fallen into the hands of a bloodthirsty "saviour". Although as a result of the police actions, the Aum Shinrikyo organisation suffered a heavy blow, yet, many of its structures survived as not all senior activists were punished for their actions by the judiciary. Formally, Aum Sinrikyo was dissolved in February, 1996, and its chief leader, Asahara, was tried and sentenced to death by hanging; the execution was carried out in 2018.

Ad 3. The third section, inspired by UFOs, is predictably fascinated by the subject of extra-terrestrial intelligences that are supposed to interfere with human life. It includes the Heaven's Gate, a group founded by Marshall Herff Applewhite (1931-1997) (Hussey 2006). Born in a Christian environment as the son of a Presbyterian pastor, he earned money as a church musician for many years, and endeavoured to persevere in "the faith of his father". Yet, his own homosexual inclinations stood in his way. As a traditional Christian, he considered "sodomy" a grave sin, which led him to great mental tension and frustration. It can be presumed that it was this factor that contributed to his conflict with official religious groups, which, in turn, resulted in the formulation of his own doctrinal concept and the establishment of an organisation that was to help him implement his ideological plans. He was dismissed from his official job due to "emotional health problems" in 1970. The following year, he underwent unsuccessful treatment in the hope of eradicating his homosexual tendencies. The nurse Bonnie Nettles (1927-1985), whom Applewhite met during his treatment of heterosexuality, collaborated with him in the field of religion until her death. Together, they developed the concepts of belief compiling the elements of reincarnation, spiritism, astrology, as well as belief in extra-terrestrial intelligence. Applewhite showed a talent for organisation and an ability to gain supporters; perhaps, the ability to work with people he acquired as a church organist helped him.

His group devoted a lot of time and resources to cultivating its image on the internet, posting a lot of video material about itself.

The members of the Heaven's Gate believed that the Earth in its present shape had no future; it had to be cleansed, which, in fact, meant means the extinction of life on the planet. From their point of view, the only way to save themselves was to leave this place. Simultaneously, they were convinced that their bodies were only a kind of "vessels". When the Hale-Bopp comet appeared in November, 1996 (the closest approach to the Earth was expected to take place in 1997), the Heaven's Gate members saw in it the sign from a "higher civilisation" they were waiting for, enabling them to achieve a higher stage of development. On 26th March, 1997, the bodies of 39 members of Heaven's Gate, including the founder of the organisation, were found at the group's property (Santa Fe ranch) north of San Diego, California. The mass suicide of the members of the group occurred while the comet was approaching. It was caused by the conviction of Applewhite of the need to get onto the spacecraft, which was to be behind the comet, by "leaving the vessels" of own bodies of the sect members (Melton, 18.09.2021).

Ad 4. The fourth section is connected with the New Age ("New Era") ideology, a kind of set of beliefs created in the 1960s and encompassing multiple concepts in the field of esotericism, occultism and spiritism. This direction is represented in the extreme form by the group of the Order of the Solar Temple (*Ordre du Temple Solaire*). This organisation referred to the "Knights of the Temple", and was founded by Joseph Di Mambro and Luc Jouret in Geneva in 1984, although there are indications that some preceding structure might have existed before. The central soteriological concept was the expectation of the second coming of Jesus Christ as the solar "god-king". The belief in the final victory of "eternal powers" over "temporal matters" was emphasised. The group's beliefs were a mixture of New Age (e.g. reincarnation), Christianity, and Masonic rituals. There were centres in Switzerland, Canada, Australia and Martinique. The Order of the Temple of the Sun was divided into lodges and had a rich ceremony involving the use of altars, costumes, swords and crusader coats, as well as a number of technical devices with which long deceased religious leaders (e.g. prophets from the Old Testament) were "materialised" and "miracles" were performed.

The tragic "breakthrough" in the group's career was the spectacular series of suicides in 1994, and there are reasons to believe that some followers did not want to part with their lives voluntarily; for example, some of the dead had their hands tied behind their backs. The tragic events took place after the so-called "last Supper", during which 15 people took poison or were poisoned, 38 died from bullets or were killed in a different way (Thaler Singer, Lalich 1997). Drugs, presumably ingested to limit the logical judgment of the situation, were discovered in the bodies of the dead members. In Switzerland, 48 bodies of the followers of the Order of the Solar Temple were found (Hussey 2006). They were "equipped" with mirrors and other items related to the symbolism of the group, and were dressed in ceremonial costumes, with plastic bags on their heads, supposedly to symbolize the ecological catastrophe happening the world. On 23rd March, 1997, in Quebec, Canada, a similar discovery was made; five people died there. The sect's motivation was twisted:

the members of this group identified death with a “journey to planet Sirius”, which they considered their “home”. Also in this case, there were elements of “suicide management” related to attempts to shape the image of the sect.

Conclusions (in the context of sect management practice)

The examples given above illustrate the forms of operation of some extreme apocalyptic religious groups. Repeated dramatic events force render it necessary to analyse the essence of this issue, which is an indispensable condition for effective counteraction. The following characteristic features of the activities of extreme religious groups with an apocalyptic orientation seem to deserve the special attention:

- The method of acquiring followers. Above all, they recruit lonely, needy and lost people. Often, in addition to salvation, they are promised to acquire skills needed in their earthly life, and to get rid of addictions.
- Soteriological exclusivism. As a rule, these groups maintain that they have a monopoly on salvation; outside of them, it cannot be obtained. Since their leaders are practically regarded as saviours, they are the chief ministers of grace in the eyes of their believers.
- Black and white optics of perceiving the world. These groups do not recognize compromises and ideological “grey area”. From their perspective, the world is made up of “good” people, that is, members of their own organisation, and the “bad” people and this means all the rest of the mankind.
- The requirement of absolute obedience. The faithful are obliged to strictly follow orders, which are often unable to fulfil their leadership satisfactorily. This usually ends with slave labour and permanent surveillance.
- Isolation from the world. The members of extreme religious groups have strictly rationed social contacts, usually limited to “their own ranks”. An interesting phenomenon is also the formation of the forms of communication specific to individual groups; a significant role is played by a specific “newspeak”, which enables “thought control”, and in which facts and words are assigned meanings different from the accepted ones. Cutting off contacts with the outside world is important from financial point of view as it de facto leads to taking over the property of the followers by the sects leaders.
- Leader cult. It usually takes on monstrous dimensions. A characteristic feature is the ability to make any changes within the doctrine by a “guru prophet” or “guru god”.
- Total control over the sexual behaviour of the supporters. Sexual life in extreme apocalyptic religious groups is usually under strict control.
- Gathering weapons, most often “in order to defend against the forces of evil”. In general, the number of weapons and their type indicate the aggressive nature of the people collecting them. Only those belonging to the inner circle of power have access to the arsenal in question it.
- Using drugs and technical gadgets to build up the ambience of group ceremonies. In the case of narcotic drugs, the control of group management in charge of the

distribution is clear. It is not about the use of drugs as such, but about the correlation of their consumption with the reception of the group's teachings. The use of "technical aids" also serves to strengthen the effectiveness of teaching.

- Concentrating on the "end of the world", with a focus on the group's role in the event. This favours the creation of an atmosphere of danger in which voicing homicidal or suicidal suggestions is particularly effective.

The leaderships of all the groups described above attached great importance to the material side of their functioning (Ritzer 2010, pp. 134-135). Practice proves that most organisations of this type show great concern for increasing their financial condition, which often contradict with the 'expectation of the end of the world' which they publicly promote. They have rich bank deposits, buy and sell shares, enjoy the financial privileges of being religious organisations, including, *inter alia*, being exempt from taxes.

The enslavement of their members (achieved in various ways) had also significant economic aspects. The management of these sects generally means using them for selfish goals by the leaders. The rank and file are basically people who are deprived of their own will, being *de facto* slaves. They are used for various purposes, for work or for collecting money for a group by streets the begging.

The leaderships of such sects are able to develop strategically plans and to manage the human resources of sects in ways that suit their purposes. In the management of such sects, one can see the main elements of "classical Fayol's management theory", albeit in a deformed form. One can see also the "product placement" in the form of their ideologies. They use marketing, attracting new followers. Some of these organisations were able to function for a relatively long time, achieving significant economic successes. Unfortunately, this was usually at the expense of their followers.

References

1. Gallagher E.V. (2005), *Branch Davidians*, [w:] *Encyclopedia of Religion*, Encyclopedia.com (dostęp: 19.07.2021).
2. Gasper H., Müller, Valentin F. (1994), *Lexikon der Sekten, Sondergruppen und Weltanschauungen*, Verlag Herder, Freiburg.
3. Hope J., Loon van B. (2008), *Intruding Buddha*, Gutenberg Press, Malta.
4. Hussey A. (2006), *The Beast at Heaven's Gate*, <https://www.mewsie.org/textbook/The-Beast-at-Heaven%E2%80%99s-Gate> (dostęp: 13.09.2021).
5. Kaplan D.E., Marshall A. (1996), *AUM – Eine Sekte greift nach der Welt*, München.
6. Kilduff M., Javers R., (1978), *Suicide Cult*, Bantham Books Edition, New York.
7. Melton J.G., *Heaven's Gate*, <https://www.britannica.com/topic/Heavens-Gate-religious-group> (dostęp: 18.09.2021).
8. Nisbet R.A. (1976), *The Sociological Tradition*, Heinemann, London.
9. Nordhausen F., von Billerbeck L. (1999), *Psycho-Sekten*, Fischer, Frankfurt.
10. Ritzer G. (2010), *Enchanting Disenchanted World*, SAGE, London.
11. Thaler Singer M., Lulich J. (1997), *Sekten*, AUER, Kempten.
12. Wiebus H.O. (1997), *Lexikon Jugendkulte*, Wilhelm Heyne Verlag, Hamburg.

13. Witzel M. (2012), *A History of Management Thought*, Routledge, London, New York.
14. Wren D.A. (1994), *The Evolution of Management Thought*, John Wiley & Sons, New York.

ELEMENTY ZARZĄDZANIA W DESTRUKTYWNYCH GRUPACH APOKALIPTYCZNYCH NA WYBRANYCH PRZYKŁADACH

Streszczenie: W rozdziale ukazano działalność destruktywnych sekt apokaliptycznych. Odgrywają one szczególną rolę wśród organizacji religijnych, wykazując się specyficznymi formami organizacyjnymi. Można wśród nich wyróżnić 4 rodzaje: 1) ugrupowania o proweniencji chrześcijańskiej; 2) czerpiące inspirację z religii Dalekiego Wschodu; 3) pozostające pod wpływem wiary w UFO oraz 4) związane z New Age. Pomimo ich różnorodności doktrynalnej, istnieją pewne podobieństwa w formach ich działania. W rozdziale poświęcono również uwagę managementowi, który jest w ich działaniach dostrzegalny.

Słowa kluczowe: destrukcyjne sekty, sekty apokaliptyczne, organizacje, mechanizmy zarządzania, management

VI

Inne formy bezpieczeństwa pozamilitarnego

Rozdział 17

STRATEGIA ROZWOJU ZRÓWNOWAŻONEGO A BEZPIECZEŃSTWO EKOLOGICZNE NA OBSZARACH PRZYRODNICZO CENNYCH

Ewa Albińska²⁵

Streszczenie: W działaniach na rzecz ochrony środowiska i bezpieczeństwa ekologicznego duże znaczenie ma opracowanie strategii rozwoju zrównoważonego dla obszaru o uznanych walorach przyrodniczych. Rozdział ukazuje proces przygotowywania takiej strategii. Dokonane analizy zwracają uwagę m.in. na kwestie: 1) uwzględnienia bezpieczeństwa ekologicznego w Lokalnej Agendzie 21; 2) zaangażowania mieszkańców gminy w działania na rzecz bezpieczeństwa ekologicznego; 3) konfliktów społecznych dotyczących realizacji strategicznych celów na obszarze parku narodowego.

Słowa kluczowe: bezpieczeństwo ekologiczne, *Lokalna Agenda 21* (ekostrategia), obszar przyrodniczo cenny, park narodowy, rozwój zrównoważony, społeczność lokalna, strategia rozwoju zrównoważonego

Wprowadzenie

Problematyka rozwoju zrównoważonego może być rozpatrywana z różnej perspektywy badawczej. Interesująca jest perspektywa społeczna, która łączy rozwój zrównoważony z bezpieczeństwem ekologicznym oraz uwzględnia tereny o szczególnych walorach przyrodniczych. Wobec powyższego problemem badawczym jest kwestia, czy lokalna strategia rozwoju zrównoważonego gwarantuje mieszkańcom obszarów przyrodniczo cennych utrzymanie bezpieczeństwa ekologicznego.

W rozdziale analizowane są wyzwania oraz trudności dotyczące realizacji celów strategicznych w kontekście oczekiwań społeczności lokalnej funkcjonującej na terenie parku narodowego. Przyjęto pięć hipotez:

- 1) Złożoność procesu opracowania *Lokalnej Agendy 21* utrudnia jej praktyczną realizację.
- 2) Bezpieczeństwo ekologiczne jest słabo zaznaczone w ekostrategii terenu przyrodniczo cennego.
- 3) Partycypacja mieszkańców w działaniach na rzecz bezpieczeństwa ekologicznego jest znikoma.

²⁵ Uniwersytet Pedagogiczny im. KEN w Krakowie, Instytut Filozofii i Socjologii

- 4) Często występują konflikty społeczne dotyczące rozbieżności pomiędzy oczekiwaniami społeczności a wymogami strategicznymi ochrony środowiska, bezpieczeństwa ekologicznego.
- 5) Praktyczne zastosowanie *Lokalnej Agendy 21* w parku narodowym jest utrudnione. Do uzyskania odpowiedzi na podane kwestie zastosowano metodę analizy danych zastanych, dostępnych materiałów źródłowych (akty normatywne i dokumenty) oraz publikacji naukowych w tytułowym zakresie. Rozdział ma charakter przeglądowy. Zaproponowane ujęcie rozwoju zrównoważonego w zestawieniu z bezpieczeństwem ekologicznym ukazuje sytuację społeczno-przyrodniczą mieszkańców terenów o szczególnych walorach przyrodniczych w nowej perspektywie badawczej.

Bezpieczeństwo ekologiczne

Bezpieczeństwo jest poczuciem pewności, szansą na przyszły rozwój oraz gwarancją jego zachowania. To obiektywna pewność nienaruszalnego przetrwania, swobód rozwojowych (Lis 2020, s. 25-26). W kontekście strategii rozwoju zrównoważonego warto odnieść się do bezpieczeństwa ekologicznego, będącego brakiem zagrożeń ekologicznych oraz pewnością życia społeczeństw w środowisku przyrodniczym (Gierszewski 2013; Ściborek i in. 2020). Taki stan stosunków społecznych promuje zrównoważone działania społeczne. Zatem bezpieczeństwo ekologiczne:

- odwołuje się do antropogennego charakteru zagrożeń ekologicznych i możliwości przeciwdziałania im w kreowanych zachowaniach społecznych;
- akcentuje znaczenie ekologicznej aktywności ludzi, w tym międzynarodowej współpracy;
- eksponuje wartości społeczne w zestawieniu z wartościami przyrodniczymi;
- uwzględnia eliminowanie napięć i konfliktów społeczno-ekologicznych.

Dla rozwoju zrównoważonego istotne znaczenie ma aspekt społeczny bezpieczeństwa ekologicznego, ujmowany w różnych wymiarach (Pietras 2000), m.in.: politycznym, ekonomicznym, technicznym.

Spółeczny aspekt bezpieczeństwa ekologicznego

Spółeczństwo rozwija się w konkretnej przestrzeni: ekonomicznej, kulturowej, technicznej itp. Wytwory człowieka w tych przestrzeniach tworzą środowisko społeczno-przyrodnicze. Z tego powodu wszelkie modyfikacje: administracyjne, gospodarcze itd. wywołują perturbacje w przyrodzie, które zmieniają pozostałe podsystemy, od technicznego, poprzez finansowy, do politycznego.

By zapewnić bezpieczeństwo ekologiczne podejmuje się próby zbudowania zrównoważonej relacji między ludźmi a przyrodą. Nie polega to tylko na zorganizowaniu parku czy rezerwatu ochrony. W imię bezpieczeństwa ekologicznego dąży się do transformacji społeczeństwa w kierunku powstrzymania procesów degradacji przyrody. Oczekuje się, że transformacja wystąpi we wszystkich płaszczyznach, które wywierają presję na środowisko: w stylu życia, konsumpcji, rolnictwie, kształtowaniu przestrzeni, turystyce, codziennych wyborach jednostki oraz grupy,

funkcjonowaniu społeczności lokalnej oraz globalnej, pokoleń współczesnych oraz przyszłych generacji. Bezpieczeństwo ekologiczne polega na utrzymaniu takiego stanu środowiska, w którym realizowane będą założenia rozwoju zrównoważonego.

Rozwój zrównoważony

W raporcie pod kierunkiem G.H. Brundtland istotę rozwoju zrównoważonego stanowi zapewnienie trwałej poprawy jakości życia obecnych i przyszłych pokoleń poprzez kształtowanie proporcji między kapitałem przyrodniczym, ludzkim i ekonomicznym (Brundtland 1991; Piątek 2002, s. 27). W definicji rozwoju zrównoważonego nie ma odniesienia do bezpieczeństwa ekologicznego, które wyraża porządek i występowanie równowagi społeczno-ekologicznej w skali lokalnej oraz globalnej. Bezpieczeństwo nie jest zatem kategorią antagonistyczną wobec równoważenia rozwoju przyrodniczego, społecznego, gospodarczego.

Dla odmiany w koncepcji zrównoważonego rozwoju podkreśla się potrzebę realizowania rozwoju gwarantującego bezpieczeństwo ludzi oraz przyrody (Kozłowski 2000; *Integracja...* 2000). Podstawową siłą sprawczą stanowią tutaj mechanizmy rynkowe, prawa rządzące zachowaniami społecznymi oraz prawa związane z warunkami przyrodniczymi (Markowski 2008, s. 26). Z kolei rozwój zrównoważony analizowany jako strategia poprawy jakości życia pomija zagadnienie bezpieczeństwa ekologicznego. Zawężając pojęcie rozwoju zrównoważonego do strategii na poziomie gminy, kluczowe będzie przeanalizowanie procedury przygotowania *Lokalnej Agendy 21*.

Przygotowanie Lokalnej Agendy 21

Gminy są zobligowane do opracowania i realizowania tzw. *Lokalnej Agendy 21*. Ta strategia ma wzorować się na *Globalnym Programie Działań – Agenda 21* i zawierać wytyczne do opracowania kompleksowego, miejscowego planu zagospodarowania przestrzennego. Tworzenie dokumentu obejmuje konkretne elementy oraz wymaga zachowania kolejności etapów (Giordano 2005; Albińska 2008)²⁶. W toku konstruowania ekostrategii ma powstać całościowy program zrównoważonego rozwoju gminy. Podczas opracowania planów i programów strategicznych konieczne jest ujęcie zasad zrównoważonego rozwoju w celach strategicznych. Każde z zaplanowanych działań zarówno ogólnych, jak i szczegółowych ma nawiązywać do idei ekorozwoju. Tymczasem działania z zakresu lokalnej ekopolityki realizowane są na podstawie wybranych i chaotycznie konstruowanych opracowań. W przyjętych strategiach nie ma spójności. Brakuje długookresowych wskazań dotyczących ochrony, zarządzania lokalnymi zasobami środowiska, bezpieczeństwa ekologicznego. Ponadto nie uwzględnia się współzależności społecznych, ekonomicznych, przestrzennych i instytucjonalnych. Tylko trzy opracowania są wykonywane przez

²⁶ 1) Inwentaryzacja przyrodnicza gminy; 2) Program ekorozwoju (rozwoju zrównoważonego); 3) Plan zagospodarowania przestrzennego.

gminy obowiązkowo²⁷. Pozostałe dokumenty mają charakter fakultatywny, uzależniony od posiadanych środków finansowych. Profesjonalnie wykonana ekostrategia nie gwarantuje automatycznie sukcesu, ale umożliwia społeczności lokalnej osiągnięcie określonych przemian w gminie. Z przemianami tymi łączą się przykładowe korzyści: poczucie stabilizacji społeczno-gospodarczej, możliwość realizowania oczekiwań mieszkańców gminy, łagodzenie konfliktów (społecznych, politycznych, gospodarczych itp.).

Ważną kwestią jest formułowanie ekostrategii dostosowanej do obszarów przyrodniczo cennych. Rozwój zrównoważony może stanowić szansę dla terenów o szczególnych walorach przyrodniczych i z tego powodu objętych ochroną prawną. Obecnie trwa dyskusja nad zakresem działań, które należy przeprowadzić na takich obszarach (m.in. w otulinie parku narodowego), by wdrożyć rozwój zrównoważony.

Park narodowy jako obszar przyrodniczo cenny

Regulacje prawne wskazują na obszary przyrodniczo cenne, w których ograniczona jest działalność człowieka. Są nimi np. rezerваты przyrody, parki krajobrazowe, obszary chronionego krajobrazu, obszary Natura 2000 (Ustawa... 2001; Ustawa... 2004). W tej grupie wyróżniają się parki narodowe. Strategia rozwoju zrównoważonego musi uwzględniać potrzebę ochrony środowiska na terenie przyrodniczo cennym. Znajduje to swoje uzasadnienie w ustawie zasadniczej, łączącej ochronę środowiska z ideą rozwoju zrównoważonego (*Konstytucja...* 2010, art. 5). Odnosząc ustawowe regulacje do terenów o szczególnych walorach przyrodniczych, należy uznać parki narodowe za rejony pionierskiej realizacji ekostrategii (Sychut, Chmielewski 1990, s. 9).

Powołanie parku narodowego na obszarze zamieszkanym przez określoną społeczność jest wyzwaniem stanowiącym społeczny eksperyment. Wdrażanie ekostrategii na wydzielonym terenie umożliwia obserwację organizowania w praktyce różnych form i płaszczyzn funkcjonowania społeczności lokalnych w środowisku przyrodniczym. Zwolennicy ekorozwoju przyjmują, że możliwy jest zrównoważony rozwój społeczno-gospodarczy, który zabezpieczy teren objęty ochroną przed dalszą degradacją przyrody i pozwoli na racjonalne wykorzystanie jej zasobów. Przeciwnicy i osoby sceptycznie odnoszące się do powyższych kwestii przyjmują, że na terenie parku narodowego nie uda się zrealizować celów ekostrategii. Ze względu na specyfikę przyrodniczego terenu, na którym wprowadza się ekostrategię, kluczowe jest wyszczególnienie z czynnika społecznego m.in. oczekiwań w życiu mieszkańców parku narodowego.

Dylematy mieszkańców parku narodowego

W społeczeństwie funkcjonują układy wartości powiązane z różnymi potrzebami oraz interesami społecznymi. Oznacza to, że działania, które dla jednej grupy są

²⁷ Są to: 1) Program ochrony środowiska; 2) Studium uwarunkowań i kierunków zagospodarowania przestrzennego gminy; 3) Miejscowy planu zagospodarowania przestrzennego.

„pożądane”, dla innych mogą stać się „niepożądane” (Nowak 1985, s. 451). W procedurach powoływania parków narodowych przeważnie nie uwzględnia się zbiorowości społecznych, które mieszkają na tym terenie. Dyrekcja parku nie przewiduje też konieczności organizowania na chronionym obszarze życia społeczności lokalnej. Tymczasem w dotychczasowych warunkach życia lokalnej społeczności pojawiają się narzucone „z zewnątrz” zakazy i nakazy, do których w krótkim czasie należy się dostosować. Realia funkcjonowania chronionego obiektu wymuszają na osobach przebywających na jego terenie przyjęcie regulacji prawnych, a także konieczność powołania instytucji represyjnych (strażników) w celu egzekwowania prawa. Wywołuje to oczywiście niezadowolenie i niepokój wśród mieszkańców takiego obszaru. Granice terytorialne parku są „odgórnie” ustalone przez urzędników na podstawie wytyczonych zasięgów występowania rzadkich i cennych gatunków flory, fauny, układów geologicznych, krajobrazowych itp. Często parki są tworzone w rejonach kultur tradycyjnych, miejscach historycznych, których mieszkańcy nie są przygotowani do zmian i natychmiastowej asymilacji. Problemem społecznym staje się wówczas nieprzystosowanie struktury administracyjnej parku do społecznych oczekiwań. Pojawiają się konflikty między mieszkańcami a urzędnikami, inwestorami i turystami. Mają one przyczynę urbanizacyjną, finansową, a także emocjonalną. Narastanie postaw wrogich i roszczeniowych lokalnej społeczności zagraża wówczas istnieniu parku narodowego.

Inną przyczyną niechęci miejscowej ludności wobec tworzonego parku narodowego jest traktowanie go jako rejonu gospodarki podporządkowanej konserwatorskiej ochronie przyrody (Sychut, Chmielewski 1990, s. 8). Zachowanie takiego obszaru wymaga realizacji przedsięwzięć gospodarczych, ale w minimalnym zakresie – ściśle podporządkowanym potrzebom ochrony środowiska (*Parki narodowe...* 1992, s. 10). Ponieważ obszar jest wyłączony z działalności przemysłowej, aby zapewnić źródła finansowania, podejmowana jest działalność o charakterze usługowym, skoncentrowana na realizacji funkcji turystyczno-wypoczynkowej. Oznacza to ograniczenie dotychczasowych możliwości rozwojowych dla społeczności. Brak ofert alternatywnych związanych z funkcjami takiego terenu nasila negatywny stosunek mieszkańców do parku narodowego.

Niepokoje społeczne mają także źródło w opiniach, stereotypach i postawach, które kształtowały się przed powołaniem parku. Obszar chroniony nie spełnia oczekiwanych przez społeczność lokalną funkcji inspiracyjnych i kreatywnych, szczególnie finansowych. Mieszkańcy ponoszą m.in. straty materialne (np. w uprawach) związane z faktem zamieszkania na obszarze chronionym albo w jego sąsiedztwie. Nie zawsze straty te są rozliczane. Ponadto lokalni gospodarze chcą mieć prawo do nieograniczonej działalności w swoim gospodarstwie domowym, rolnym itp. Szczególnie dotyczy to ograniczania prawa własności (wyrębu drzew w swoim lesie, dowolnego dysponowania gruntami, prawa budowy).

Wśród przyczyn konfliktów społecznych wymienia się ponadto niską świadomość ekologiczną. Badania socjologiczne w tym zakresie, przeprowadzone w latach 80. i 90. XX wieku (Grabowski, Marmuszewski 1985; *Ochrona przyrody...* 1990; Osiniak, Poskrobko, Sadowski 1993), potwierdzają przejawianą również po 2000 roku niechęć społeczności lokalnych do mieszkania na terenie parku

narodowego. Negatywne postawy odnoszą się do niespełnionych oczekiwań poprawy warunków życia, dobrobytu, wzrostu stopy życiowej, a także braku rekompensat za straty materialne i utrudnienia związane z zamieszkiwaniem obszaru przyrodniczo cennego. Podobna sytuacja występuje obecnie.

Wobec powyższego szczególną rangę należy nadać możliwościom zrównoważonego postępu społecznego, który sprowadza się do zaspokajania potrzeb ludzi, zapewnienia im równych szans rozwoju oraz zagwarantowania ładu ekologicznego.

Perspektywy dla społeczności lokalnej

Mieszkańcy gminy nie dysponują propozycjami rozwiązywania problemów cywilizacyjnych, w tym również ekologicznych. Z tego powodu poszukują różnych modeli życia, zasad organizowania stosunków społecznych wewnątrz „małej ojczyzny”, przede wszystkim poszukują bezpiecznego miejsca do życia. Obserwacje dotyczące aktywności ludzi na rzecz ochrony środowiska przyrodniczego czy zapewnienia bezpieczeństwa ekologicznego wskazują, że „chcieliby coś zrobić, ale nie wiedzą jak”. W codziennym funkcjonowaniu przeciętny Polak jest skupiony na „zwykłych sprawach i problemach” i nie martwi się kwestiami ekologicznymi. Przykłady uczestnictwa społecznego w rozwiązywaniu problemów ekologicznych znacznie częściej wiążą się z protestem przeciw niebezpieczeństwom natury zdrowotnej oraz ekonomicznej, rzadziej dotyczą bezpiecznej aktywności w środowisku przyrodniczo cennym. Sterowanie zachowaniami społecznymi mieszkańców parku poprzez przedstawianie argumentów naukowych jest niewystarczające. Ludzie powinni odczuwać korzyści oraz dumę z faktu egzystencji na terenie objętym ochroną prawną. W tym celu wskazane jest zorganizowanie mechanizmów gospodarczych pozwalających na zagwarantowanie społeczności lokalnej odpowiedniego poziomu dobrobytu²⁸.

Potencjał środowiska społecznego, znajdującego się na terenie parku narodowego, nie jest w pełni wykorzystany. Brakuje wzorców życia społeczno-gospodarczego na terenach przyrodniczo cennych. Przestrzegania reguł zachowań na obszarze objętym ochroną nie uzyska się bez zmiany osobowości ludzi, ich uświadomienia ekologicznego, przebudowy całokształtu życia społeczności lokalnych, co łączy się z relacjami w ramach szerszych struktur społecznych. Czasami mieszkańcy parku narodowego podejmują działania związane z ekorozwojem lub bezpieczeństwem ekologicznym, nie czekając na pomoc z instytutów badawczych, ministerstwa, władz samorządu terytorialnego itp. Takie inicjatywy oddolne są przejawem zaangażowania społecznego, jednak wciąż o minimalnym zasięgu terytorialnym. Jeżeli społeczności lokalne mieszkające na terenie np. parku narodowego nie będą mieć perspektyw rozwojowych, możliwości bogacenia się, wówczas obszar ten przeobrazi się w skansen bez ludzi. Zapewniając mieszkańcom różne formy aktywnej pomocy i doradztwa, z których będą oni mogli skorzystać, umożliwi się im bezpieczny i zrównoważony rozwój.

²⁸ Przykładowo: 1) kreowanie form wypoczynku i ruchu turystycznego, które nie kolidują z funkcją ochrony zasobów przyrodniczych; 2) ekoturystyka, gospodarstwa biodynamiczne, ekologiczne.

Ciekawą perspektywą jest regionalizm ekologiczny. U jego podstaw znajduje się dążenie mieszkańców do zaspokojenia bezpieczeństwa poprzez działania uwzględniające specyfikę obszaru przyrodniczego w „małej ojczyźnie”. Taka działalność będzie korzystnym elementem podczas wdrażania efektywnej strategii rozwoju zrównoważonego na obszarze przyrodniczo cennym.

Efektywność ekostrategii na obszarze chronionym

Wdrażanie rozwoju zrównoważonego w gminie znajdującej się w obszarze chronionym jest determinowane:

- stanem równowagi między gospodarką, środowiskiem i społeczeństwem;
- świadomością ekologiczną władz samorządowych i mieszkańców;
- gotowością społeczności do partycypacji w zarządzaniu gminą.

Lokalna Agenda 21 zostanie zrealizowana przez gminę, gdy użyte zostaną odpowiednie narzędzia prawne, ekonomiczne i organizacyjne. Należą do nich przede wszystkim: efektywna struktura organów zarządzających ochroną środowiska, mechanizmy ekonomiczne wymuszające i wspierające działalność inwestycyjną służącą ochronie przyrody, skuteczne prawo ekologiczne wraz z systemem kontroli jego przestrzegania (Nowicki 1993, s. 145). Dobre współrzędzenie zapewni gminie sprawna administracja, partnerstwo w rozwiązywaniu problemów oraz współpraca między władzami a mieszkańcami. Poprawnie skonstruowane plany rozwoju zrównoważonego na poziomie gminy zaspokoją potrzeby bezpieczeństwa finansowego, społecznego, ekologicznego. Natomiast zrównoważona relacja społeczeństwa i gospodarki do przyrody rozwiąże lokalne problemy ochrony środowiska oraz zagwarantuje stabilizację ekonomiczną gminy.

Ważne jest dążenie do osiągnięcia postępu społecznego poprzez wykorzystanie geograficznego położenia regionu oraz jego walorów przyrodniczych. Chcąc zapewnić realizację ekostrategii na obszarze cennym przyrodniczo, należy spełnić przynajmniej dwa warunki. Pierwszy łączy się z trafnym, praktycznym wykorzystaniem walorów przyrodniczych. Warunek drugi to partycypacja społeczności lokalnej. Parki narodowe dysponują obok kadry specjalistów mieszkańcami, których warto pozyskać do zadań wskazanych w strategii rozwoju zrównoważonego. Obszary przyrodniczo cenne, w tym parki narodowe, mogą stać się wzorcowymi terenami dla praktycznej realizacji założeń rozwoju zrównoważonego, uwzględniającego bezpieczeństwo ekologiczne.

Podsumowanie

Do aktywności gminnych władz samorządowych należy opracowanie strategii zrównoważonego rozwoju. Jej wieloetapowe przygotowanie ma szczególnie charakter w zakresie obszarów cennych przyrodniczo. Na terenach o uznanych walorach przyrodniczych proces konstruowania *Lokalnej Agendy 21* oraz jej wdrażanie ograniczają działania na płaszczyźnie terytorialnej, instytucjonalnej, finansowej, gospodarczej, środowiskowej i społecznej.

Na podstawie przeprowadzonych w rozdziale analiz stwierdza się, że lokalna ekostrategia nie daje mieszkańcom parku narodowego gwarancji na utrzymanie bezpieczeństwa ekologicznego. Przyczyniają się do tego następujące fakty:

- 1) Nieujednolicony, niespójny proces opracowania dokumentu utrudnia jego praktyczne zastosowanie.
- 2) W ekostrategii gminy marginalizowane jest bezpieczeństwo ekologiczne.
- 3) Słabo zaznacza się partycypacja mieszkańców gminy w działaniach na rzecz ochrony środowiska, bezpieczeństwa ekologicznego itp. aktywności.
- 4) Występują konflikty interesów, potrzeb społeczności lokalnej oraz konieczności wprowadzenia prawnych ograniczeń ochronnych dotyczących środowiska, bezpieczeństwa ekologicznego czy zadań o charakterze społeczno-ekonomicznym.
- 5) Trudności w praktycznym zastosowaniu *Lokalnej Agendy 21* na obszarze parku narodowego.

Sytuację może poprawić m.in. działalność uaktywniająca i uświadamiająca w zakresie ochrony środowiska i bezpieczeństwa ekologicznego, skierowana do mieszkańców parku narodowego, organów władzy samorządowej, turystów itd. Proponując mieszkańcom różne formy partycypacji społeczno-gospodarczej, dostosowanej do wymogów funkcjonowania terenu objętego ochroną, można zapewnić rozwój zrównoważony oraz zadbać o bezpieczeństwo społeczno-ekologiczne. Istotne jest, by w ekostrategii uwzględnić obszar chroniony, lokalną społeczność i gospodarkę. Efektem bezpiecznego i zrównoważonego rozwoju będzie proces tworzenia na szczeblu gminy miejsc pracy, usług i dóbr zaspokajających lokalny i ponadlokalny popyt, walorów użytkowych oraz przyrodniczych.

Dokumentem określającym dzisiaj kierunki polityki rozwoju zrównoważonego jest przyjęta w 2017 roku *Strategia na Rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*. Formułuje ona rozwój odpowiedzialny, który m.in. ma zapewnić udział oraz korzyści wszystkim grupom społecznym zamieszkującym różne miejsca w kraju (*Strategia...* 2017, s. 7). W dokumencie dostrzega się rangę mieszkańców w ekorozwoju „małych ojczyzn”.

Literatura

1. Albińska E. (2008), *Organizacja funkcjonowania gminy zgodnie z zasadą rozwoju zrównoważonego*, [w:] Partycki S. (red.), *Kultura a rynek*, t. 2, Wydawnictwo KUL, Lublin.
2. Brundtland G.H. (1991), *Nasza wspólna przyszłość. Raport Światowej Komisji do Spraw Środowiska i Rozwoju*, PWE, Warszawa.
3. Gierszewski J. (2013), *Bezpieczeństwo społeczne. Studium z zakresu teorii bezpieczeństwa narodowego*, Difin, Warszawa.
4. Giordano K. (2005), *Planowanie zrównoważonego rozwoju gminy w praktyce*, Wydawnictwo KUL, Lublin.
5. Grabowski T., Marmuszewski S. (1985), *Świadomość ekologiczna górali i ich postawy wobec tatrzańskiego parku Narodowego*, „*Studia Socjologiczne*”, 1, 96, s. 241-258.
6. *Integracja polityk sektorowych Unii Europejskiej z polityką ekologiczną. Jak Unia Europejska traktuje ekorozwój* (2000), Instytut na rzecz Ekorozwoju, Warszawa.
7. *Konstytucja Rzeczypospolitej Polskiej* (2010), Lexis Nexis, Warszawa.
8. Kozłowski S. (2000), *Ekorozwój. Wyzwanie XXI wieku*, Wydawnictwo Naukowe PWN, Warszawa.

9. Lis S. (2020), *Struktura społeczna a typy bezpieczeństwa*, [w:] Szylar A., Maciaszczyk P. (red.), *Bezpieczeństwo a perspektywy przemian globalizującego się świata*, Wydawnictwo Państwowej Uczelni Zawodowej im. prof. Stanisława Tarnowskiego w Tarnobrzegu, Tarnobrzeg.
10. Markowski T. (2008), *Teoretyczne podstawy rozwoju lokalnego i regionalnego*, [w:] Strzelecki Z. (red.), *Gospodarka regionalna i lokalna*, s. 13-28, Wydawnictwo Naukowe PWN, Warszawa.
11. Nowak S. (1985), *Metodologia badań społecznych*, PWN, Warszawa.
12. Nowicki M. (1993), *Strategia ekorozwoju Polski*, Agencja Reklamowo-Wydawnicza A. Grzegorzczak, Warszawa.
13. *Ochrona przyrody i krajobrazu w systemie samorządów gmin* (1990), Polski Klub Ekologiczny, Kraków.
14. Osiniak T., Poskrobko B., Sadowski A. (1993), *Wigierski Park Narodowy a jego mieszkańcy*, Wydawnictwo Ekonomia i Środowisko, Białystok.
15. *Parki narodowe w Polsce. Sprawozdanie roczne 1991* (1992), Krajowy Zarząd Parków Narodowych, Izabelin – Białowieża.
16. Piątek B. (2002), *Koncepcja rozwoju zrównoważonego i trwałego Polski*, Wydawnictwo Naukowe PWN, Warszawa.
17. Pietraś M. (2000), *Bezpieczeństwo ekologiczne w Europie. Studium politologiczne*, Wydawnictwo UMCS, Lublin.
18. *Strategia na Rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*, przyjęty uchwałą Rady Ministrów w dniu 14 lutego 2017 r., Warszawa.
19. Sychut W., Chmielewski T.J. (1990), *Świadomość ekologiczna mieszkańców obszarów chronionych*, IGPIK, Lublin.
20. Ściborek Z. i in. (2020), *Bezpieczeństwo wewnętrzne. Podręcznik akademicki*, Wydawnictwo Adam Marszałek, Toruń.
21. Ustawa z dnia 27 kwietnia 2001 r. *Prawo ochrony środowiska* (Dz.U. 2008 nr 25 poz. 150, ze zm.).
22. Ustawa z dnia 16 kwietnia 2004 r. o ochronie przyrody (Dz.U. 2004 nr 92 poz. 808).

SUSTAINABLE DEVELOPMENT STRATEGY AND ECOLOGICAL SAFETY IN REGIONS OF NATURAL PROTECTION

Abstract: This chapter looks – with ecological and sociological perspective – at the situation of local community in Poland. In this context, the chapter concern at: 1) sustainable development strategy, 2) ecological security, 3) discussion about the sustainable development in national park territory, 4) human activities for the local environment. In short analysis, this chapter present: 1) relations between ecological development and security, 2) social situation in regions of natural protections, 3) the role of local community in strategy of sustainable development and ecological security.

Keywords: ecological security, *Local Agency 21*, local community, national park, region of natural protection, sustainable development, sustainable development strategy

Rozdział 18

BEZPIECZEŃSTWO SOCJALNE RODZINY POPRAWKĄ ZASIŁEK WYCHOWAWCZY 500+ A WPŁYW NA WZROST ZAMOŻNOŚCI RODZINY

Tomasz Odzimek²⁹

Streszczenie: Rozwój społeczno-gospodarczy w XX i XXI wieku wiąże się m.in. z dużą interwencją państw w pomaganiu rodzinom i ich dzieciom. Pomoc ta przybrała postać zasiłków rodzinnych. Państwo zaangażowało się w poprawę warunków życia i pracy jednostek oraz całych grup społecznych. Jednym z głównych celów działań państwa na rzecz bezpieczeństwa socjalnego obywateli jest bezpieczeństwo rodziny. Znaczną rolę w ograniczaniu zasięgu ubóstwa odgrywają transfery społeczne w postaci świadczeń pieniężnych, w tym też w postaci świadczeń rodzinnych. W rozdziale przedstawiono pomoc materialną państwa dla polskich rodzin ze szczególnym uwzględnieniem wspierania finansowego rodzin wielodzietnych w aspekcie bezpieczeństwa socjalnego. Szczególną uwagę poświęcono sprawie ubóstwa w rodzinach wielodzietnych. Za pomocą porównawczych badań własnych przedstawiono działalność państwa polskiego w relacji do innych krajów Unii Europejskiej na przestrzeni lat od wejścia Polski do UE do roku 2021. W szczególności pokazano wpływ programu 500+ na poziom bezpieczeństwa socjalnego rodzin w Polsce i porównano aktywność finansową państwa po wprowadzeniu programu 500+ z aktywnością państw Zachodniej Europy.

Słowa kluczowe: bezpieczeństwo socjalne rodzin, pomoc finansowa dla rodzin, program 500+, zasiłek rodzinny,

Wprowadzenie

Bezpieczeństwo socjalne definiowane jest jako: „stan wolności od braku lub niedostatku środków utrzymania, to stan zaspokojenia potrzeb socjalnych, a więc podstawowych potrzeb bytowych. Bezpieczeństwo jest stanem wolności od zagrożeń i może być odnoszone do różnych sfer życia człowieka” (Pacud 2002, s. 14). Zaspokajanie potrzeb bytowych może być postrzegane w kategoriach bezpieczeństwa społecznego i socjalnego. W literaturze często pojęcia te traktowane są zamiennie. Określenie „socjalny” dotyczy podstawowych spraw bytowych, najbardziej istotnych dla każdej jednostki, i często łączone jest z udzielaniem wsparcia. „Społeczny”

²⁹ Politechnika Częstochowska, Wydział Zarządzania

ma szerszy kontekst znaczeniowy niż „socjalny” i obrazuje wszechstronny rozwój fizyczny (zdrowie, rekreacja, ubezpieczenia społeczne) oraz duchowy (kultura) człowieka (Zamorska 2010, s. 26).

Należy pamiętać, że wraz z rozwojem cywilizacyjnym, w szczególności z wcześniej niespotykanym wzrostem warunków socjalnych społeczeństw zachodnich, bezpieczeństwo socjalne odnosi się także do standardów gwarantowanych w systemie prawa państwa demokratycznego. Źródła prawa nie definiują pojęcia „bezpieczeństwa socjalnego”, ale próbują wytyczać jego granice poprzez normowanie zadań państwa, zwłaszcza w zakresie dostarczania świadczeń i odpowiadających im uprawnień obywateli. W aktach prawnych czy urzędowych dokumentach bezpieczeństwo socjalne opisywane jest przez zwroty prawnie niedookreślone typu: „odpowiedni poziom”, „godne warunki życia”, „godziwa płaca” itp. Takimi pojęciami posługują się często międzynarodowe czy europejskie źródła prawa, pozostawiając poszczególnym państwom swobodę w konkretyzacji poziomu bezpieczeństwa socjalnego (Sierpowska 2009, s. 117-118). Zwroty te są podstawą do określania w systemach prawnych standardów zabezpieczenia bytu jednostki, takich jak minimalna płaca krajowa, próg interwencji socjalnej, kryteria dochodowe uprawniające do świadczeń.

Współcześnie bardzo ważną rolę w polityce społecznej państwa pełni zapewnienie podstawowych warunków do godnego życia rodziny. Szczególnie ważnym aspektem jest dbanie państwa o zrównoważony rozwój rodzin wielodzietnych. Temu służy różnego rodzaju pomoc państwa na rzecz rodzin wychowujących dzieci. Na plan pierwszy wybijają się zasiłki rodzinne dedykowane rodzinom, w których są dzieci. Dotyczy to zarówno pełnych rodzin, jak i osób samotnie wychowujących dzieci. Temu poświęcona jest dalsza część rozdziału.

Bezpieczeństwo materialno-socjalne rodziny punktem odniesienia do rozwoju społecznego państwa

Rodzina nadrzędną wartością społeczeństwa

Bezpieczeństwo socjalne wraz z rozwojem cywilizacyjnym w świecie zachodnim XX wieku zajęło czołową pozycję wśród wartości społecznych i na trwale wpisało się w katalog podstawowych praw obywatelskich w systemie demokratycznym. W nowoczesnych, demokratycznych systemach politycznych oznacza to, że państwo i jego struktury przejęły współodpowiedzialność za poziom bezpieczeństwa socjalnego narodu.

Początek XX wieku nie wskazywał na to, iż ten wiek właśnie wiek zapisze się w historii jako okres budowy państw opiekuńczych wobec swoich obywateli. Obowiązywały reguły, według których dopóki społeczne konsekwencje nierównego dostępu do instytucji i urzędów gwarantujących bezpieczeństwo socjalne były akceptowane jako uzasadnione normami moralnymi i religijnymi, dopóty odpowiedzialność za stan i stopień poczucia bezpieczeństwa socjalnego spoczywała na rodzinie. Rozwój systemu politycznego w kierunku demokracji sprawił, że to, co możliwe, stało się konieczne. Przejęcie dużo wcześniej przez państwo

odpowiedzialności za poziom bezpieczeństwa socjalnego obywateli stało się konieczne, ponieważ na tym obszarze pojawiło się narastające zapotrzebowanie na legitymizowanie na zasadzie dobrowolności i wolności demokratycznych systemów politycznych. Motywacją państwa jako aparatu zarządzającego do angażowania się w poprawę warunków życia i pracy jednostek oraz całych grup społecznych była nie tylko presja potrzeb społecznych, ale także odnosząca się do sukcesji wyborczych konieczność dostosowywania politycznych i administracyjnych struktur do całkowicie nowych żądań instytucjonalnych i procesów rozwoju gospodarczego (Dziewiącka-Bokun 2003, s. 131-132).

Według badania Centrum Badania Opinii Społecznej (CBOS 2020) z 2019 roku, dotyczącego najważniejszych wartości dla polskich obywateli, na pierwszym miejscu znalazło się szczęście rodzinne (najważniejsze dla ponad 4/5 Polaków – 83%), a na drugim (69%) – zachowanie dobrego zdrowia (tak jak w 2013 roku). Na trzecim miejscu znalazł się spokój, wybrany przez 27% badanych, a na czwartym uczciwe życie, wskazane przez 19% respondentów (w 2013 roku uczciwe życie plasowało się na trzecim, a spokój – na piątym miejscu).

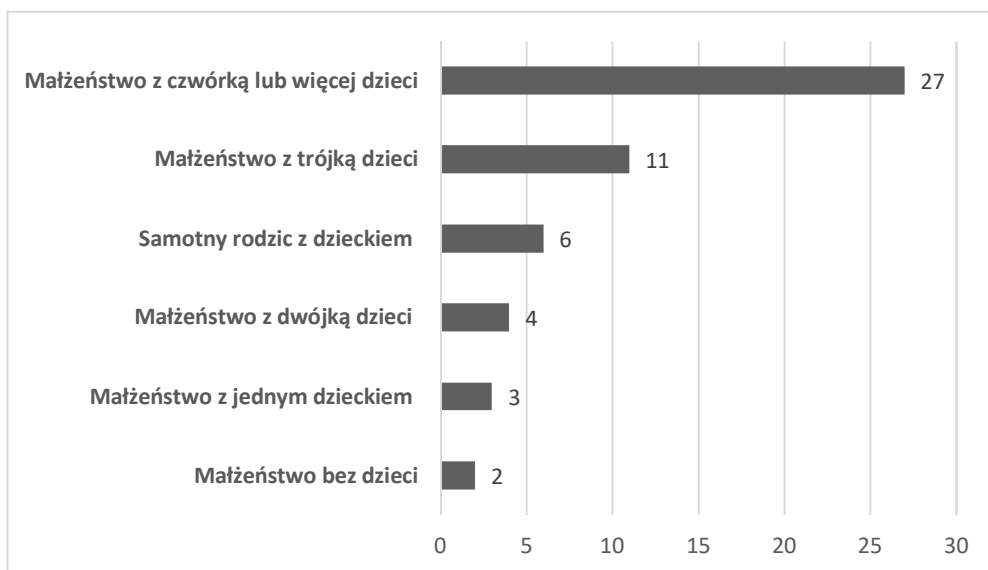
Jednym z głównych celów działań państwa na rzecz bezpieczeństwa socjalnego obywateli jest bezpieczeństwo rodziny. Podstawę do takiego postrzegania roli państwa w tym zakresie dają m.in. publikowane od 2000 roku raporty o stanie społeczeństwa *Diagnoza społeczna*, z których wynika, że rodzina i praca zawodowa niezmiennie należą do podstawowych wartości społeczeństwa polskiego. Według raportu *Diagnoza Społeczna* w 2015 roku 67% badanych dorosłych Polaków uważało zdrowie za wartość najważniejszą jako warunek udanego i szczęśliwego życia (Czapliński, Panek (red.) 2015). Na drugim miejscu znalazło się udane małżeństwo (50,3%), dzieci (48,7%), praca (30,0%), pieniądze (28,3%), opatrność, Bóg (13,1%), przyjaciele (11,6%) (Czapliński, Panek (red.) 2015, s. 140-145).

Bezpieczeństwo socjalne rodziny w wymiarze materialnym

Problem pomocy materialnej rodzinie był ciągle aktualny zarówno w badaniach, jak i działaniach rządów zmierzających przede wszystkim do zwiększenia ochrony rodzin znajdujących się w trudnej sytuacji życiowej. Pieniądze wydawane na świadczenia przez budżet państwa, mimo pokażnej sumy, nie uchroniły jednak dostatecznie polskich rodzin przed ubóstwem. Uwagę zwraca fakt, że wraz ze wzrostem gospodarczym w Polsce nie zawsze poprawiała się sytuacja gospodarstw domowych. Zgodnie z *Diagnozą społeczną* z 2013 roku (Czapliński, Panek (red.) 2013) było tak np. w latach 2011-2013, kiedy wystąpiła przewaga gospodarstw domowych, które weszły do sfery skrajnego ubóstwa (3,13%), nad tymi, które w tym czasie z tej sfery wyszły (2,09%). Podobną tendencję zaobserwowano w przypadku przynależności gospodarstw domowych do sfery niedostatku. Sytuacja 5% gospodarstw domowych z tej grupy polepszyła się na tyle, że wyszły z tej sfery, natomiast ponad dwa razy więcej gospodarstw (11%) do niej weszło (Czapliński, Panek (red.) 2013, s. 354). Zadziwiające wobec powyższych danych jest to, że w latach 2011-2013 mieliśmy w Polsce dodatni wzrost gospodarczy (średnio o ok. 3% PKB), a więc sytuacja powinna być odwrotna.

Od 2015 roku utrzymuje się spadkowa tendencja zagrożenia ubóstwem. O ile jeszcze w 2015 roku poziom skrajnego ubóstwa wynosił 6,5%, a poziom ustawowej linii ubóstwa obejmował 12,2% społeczeństwa, to w 2019 roku według danych GUS minimum egzystencji wynosiło 4.2%, natomiast poziom ustawowej linii ubóstwa 9% (GUS 2019). Na przestrzeni tych kilku lat zaobserwowano wyraźny spadek niekorzystnych stanów zagrażających godnemu życiu w społeczeństwie.

Według innych, pochodzących z 2015 roku, badań sondażowych GUS w 2012 roku w porównaniu z poprzednimi latami zanotowano zwiększenie zagrożenia skrajnym ubóstwem niemal we wszystkich grupach gospodarstw domowych. Grupę gospodarstw, w których istnieje największe zagrożenie ubóstwem, stanowią rodziny wielodzietne wychowujące czwórkę lub więcej dzieci. W rodzinach bezdzietnych oraz w rodzinach z jednym dzieckiem sytuacja jest najlepsza. W nich zagrożeniem objęta jest co 50. osoba. Natomiast zagrożenie wyraźnie wzrasta wraz z liczbą dzieci na utrzymaniu. W rodzinach z co najmniej czwórką dzieci ubóstwo skrajne zagraża przynajmniej co 4. osobie (Kubów 2014, s. 31-32). Rysunek 18.1 przedstawia poziom ubóstwa w zależności od dzietności rodziny.



Rysunek 18.1. Poziom ubóstwa w zależności od dzietności rodziny w Polsce w 2015 r. (w %)

Źródło: opracowanie własne na podstawie (GUS 2015)

Znaczącą rolę w ograniczaniu zasięgu ubóstwa odgrywiają transfery społeczne w postaci świadczeń pieniężnych, w tym też w postaci świadczeń rodzinnych. Jak wynika z badań GUS w 2011 roku, pozbawienie rodzin tego typu dochodów zwiększyłoby zasięg ubóstwa relatywnego w Polsce o ok. 6%, a więc wyniosłoby ono nie 16,9%, lecz ok. 23% (GUS 2011). W przypadku dzieci i młodzieży do lat 18 transfery społeczne redukowały ubóstwo o 8,1%. W Polsce, w porównaniu do Unii

Europejskiej, zwraca uwagę mniejszy wpływ transferów społecznych na ograniczanie ubóstwa, gdyż w Unii w 2011 roku ograniczyły one ubóstwo o ok. 9%, a wśród osób poniżej 18. roku życia aż o ok. 14% (GUS 2013, s. 18).

Powstaje zatem pytanie, w jakim stopniu polityka rodzinna, zwłaszcza świadczenie rodzinne w postaci zasiłków rodzinnych, sprzyja umacnianiu bezpieczeństwa socjalnego rodziny. W tym celu należy dokonać przeglądu aktywności państwa polskiego w tym zakresie w okresie przedakcesyjnym do Unii Europejskiej aż do roku 2019³⁰, a więc do momentu działania przez trzy lata programu rządowego Rodzina 500+. Przegląd jest o tyle uzasadniony, że Polska, wstępując do UE, znalazła się w gronie państw o dużej aktywności finansowej na rzecz rodziny. Ponadto w celu ukazania roli państwa w zakresie bezpieczeństwa socjalnego rodziny należy porównać wysokości finansowych transferów w Polsce do innych krajów UE, będących głównym celem emigracji polskich obywateli.

Program 500+ przełomowym krokiem w pomocy finansowej państwa we wspieraniu bezpieczeństwa socjalnego polskiej rodziny w świetle innych krajów UE

Program 500+ a wpływ na obniżenie ubóstwa w rodzinach w świetle badań własnych

W 2016 roku doszło w Polsce do przełomowego wydarzenia pod względem pomocy państwa dla rodzin z dziećmi. Stało się tak za sprawą wprowadzenia programu 500+. Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Ustawa... 2016) wprowadziła najdroższy w III RP instrument polityki rodzinnej. Jest nim świadczenie wychowawcze w wysokości 500 zł (ok. 120 euro) miesięcznie przysługujące bez kryterium dochodowego na drugie i kolejne dziecko do ukończenia przez nie 18. roku życia oraz na pierwsze dziecko w rodzinach, w których dochód netto w przeliczeniu na osobę nie przekraczało 800 zł (lub 1200 zł w przypadku dziecka niepełnosprawnego). Od lipca 2019 roku zasiłek ten przysługuje na każde dziecko do uzyskania pełnoletności, a więc świadczenie to stało się całkowicie powszechne dla wszystkich.

W 2016 roku do świadczenia uprawnionych było około 3,8 mln dzieci wychowujących się w około 2,7 mln rodzin, a więc łącznie 63% rodzin z niepełnoletnimi dziećmi. W całym roku 2016 program kosztował 17 mld zł, w kolejnych zaś latach – 23 mld. Od pełnego 2020 roku wydatki państwa na ten cel stanowią rocznie ok. 40 mld zł, uprawnionych jest ponad 4 mln rodzin i ok. 5 mln dzieci. W tabeli 18.1. została przedstawiona pomoc państwa dedykowana dzieciom w rodzinach do 2016 roku i po tym okresie, licząc już razem skumulowane zasiłki: dotychczasowy rodzinny i wychowawczy 500+.

³⁰ Lata 2020 i 2021 są w cieniu pandemii COVID-19 i z tego względu państwa koncentrowały się na pomocy skierowanej na ratowanie firm przed upadłościami, a jednocześnie pomoc skierowana ku rodzinie w postaci zasiłków nie odpowiadała standardowej sytuacji planowania takiej polityki. Z tego powodu analiza obejmuje okres do 2019 łącznie.

**Tabela 18.1. Wysokość zasiłku rodzinnego w Polsce przed i po 2016 r.
(miesięcznie – w zł)**

Polska	Na jedno dziecko	Na dwójkę dzieci	Na trójkę dzieci	Na czwórkę dzieci
Przed 2016 r. Liczone powyżej 5. roku życia do ukończenia 18. roku życia	124	148	272	396
Program 500+	500	1000	1500	2000
Od 2016 r. liczone łącznie z programem 500+	724	1148	1772	2396

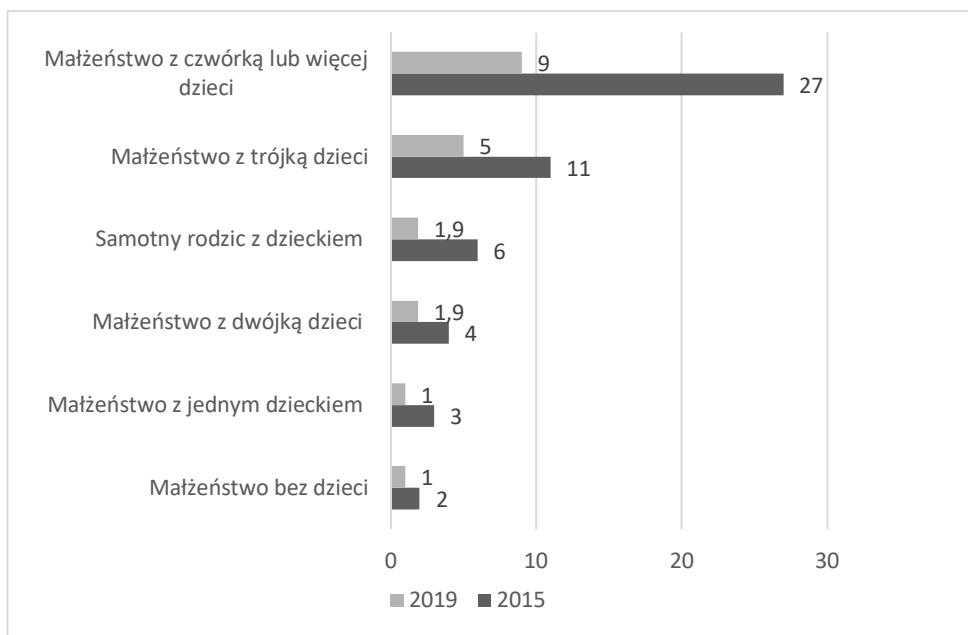
Źródło: opracowanie własne

Interesującym aspektem zasiłków na rzecz rodziny jest porównanie tejże pomocy państwa polskiego do pomocy udzielanej w innych krajach Unii Europejskiej. Odnosząc się do przedstawionego na rysunku 18.2 poziomu ubóstwa w zależności od dzietności rodziny w 2015 roku, należy stwierdzić, że wprowadzenie programu 500+ doprowadziło do wzrostu zamożności polskiej rodziny i jednocześnie do obniżenia ubóstwa w rodzinach posiadających dzieci. W szczególności zauważalny jest spadek ubóstwa w rodzinach wielodzietnych.

Porównując zasiłki rodzinne w kilku bogatych krajach Europy Zachodniej do sytuacji w Polsce, zaznaczyć należy, że w Polsce do 2016 roku istniał zasiłek rodzinny będący odpowiednikiem takiego samego zasiłku w UE. Natomiast od 2016 roku istnieją dwa zasiłki: zasiłek rodzinny oraz zasiłek wychowawczy w ramach programu 500+, jednakże obydwa pełnią tę samą rolę i można w celach porównawczych stosować ich łączną wartość jako zasiłek na rzecz rodzin z dziećmi lub osób samotnie wychowujących dzieci.

Odnosząc się do rysunku 18.2, należy podkreślić, że w latach 2015-2019 nastąpiła zdecydowana poprawa życia materialnego rodzin wielodzietnych. Poziom ubóstwa w rodzinach z czwórką i więcej dzieci obniżył się odpowiednio z 27% do 9%. Oznacza to, że w 2019 roku już tylko 9 na 100 rodzin znajdowało się w ubóstwie, podczas gdy w 2015 roku blisko jedna trzecia cierpiała z tego powodu. Również duży spadek zauważyć należy w grupie małżeństw z trójką dzieci oraz samotnie wychowujących dziecko. Tutaj redukcja rodzin żyjących w ubóstwie wynosiła odpowiednio z 11% do 5% w przypadku rodzin z trójką dzieci oraz z 6% do 1,9% w przypadku osób wychowujących dzieci samotnie. Najmniejszy wpływ obydwa zasiłki na rzecz rodzin miały na małżeństwa z jednym dzieckiem. To jednak nie dziwi, gdyż zazwyczaj małżeństwa z jednym dzieckiem w porównaniu do rodzin wielodzietnych w mniejszym stopniu potrzebują pomocy państwa.

Rysunek 18.2 pokazuje więc, iż wprowadzenie zasiłku wychowawczego na dziecko w postaci 500+ doprowadziło do sporych zmian jakości życia wielu setek rodzin w Polsce, co należy odnotować jako bardzo korzystne zjawisko, przybliżające Polskę do standardów Europy Zachodniej.



Rysunek 18.2. Poziom ubóstwa w zależności od dzietności rodziny w % lata 2015 i 2019

Źródło: opracowanie własne na podstawie (GUS 2015; GUS 2019)

Program 500+ jako element polityki zasiłków rodzinnych w porównaniu do innych krajów UE w świetle badań własnych

Do 2016 roku funkcjonował system świadczeń rodzinnych w Polsce wprowadzony 1 maja 2004 roku na mocy ustawy o świadczeniach rodzinnych z dnia 28 listopada 2003 roku. Podstawowym rodzajem świadczeń rodzinnych był zasiłek rodzinny. W pierwszych latach jego funkcjonowania, tj. od 1 maja 2004 roku do 31 sierpnia 2006 roku był on przyznawany w wysokości zależnej od liczby dzieci na utrzymaniu osoby uprawnionej i wynosił miesięcznie: 43 zł na pierwsze i drugie dziecko, 53 zł na trzecie dziecko oraz 66 zł na czwarte i kolejne dziecko. Począwszy od 1 września 2006 roku zasiłek rodzinny jest przyznawany w zależności od wieku dziecka pozostającego na utrzymaniu osoby uprawnionej i obowiązuje przez 3 lata. W tabeli 18.2 przedstawiono, jak kształtowała się wysokość zasiłku rodzinnego w Polsce na przestrzeni lat 2006-2021.

Zasiłek rodzinny jest to jedna z form wsparcia dla rodzin, przede wszystkim o niskich dochodach, wielodzietnych czy wychowujących niepełnosprawne dzieci. Ma na celu częściowe pokrycie kosztów utrzymania dziecka. Wymiar zasiłku rodzinnego, mimo niemal podwojenia jego kwoty w latach 2005-2012, jest w Polsce nadal niewielki, jeśli spojrzeć na inne kraje UE. Niski poziom pomocy państwa dla utrzymania rodziny był do 2016 roku jednym z głównych powodów emigracji Polaków za granicę do krajów dużo bogatszych, w których zasiłki rodzinne są kilkukrotnie wyższe.

Tabela 18.2. Wysokość zasiłku rodzinnego w Polsce w latach 2006-2021 (w zł)

Wiek dziecka	Wysokość zasiłku rodzinnego			
	2006-2009	2009-2012	2012-2015	2015-2021
Do 5. roku życia	48	68	77	95
Powyżej 5. roku życia do ukończenia 18. roku życia	64	91	106	124
Powyżej 18. roku życia do ukończenia 24. roku życia	68	98	115	135

*daty obowiązywania każdorazowo od 1 września do 30 października danego roku

Źródło: opracowanie własne na podstawie przeglądu nowelizacji Ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych

Aby zobrazować różnice w wysokości zasiłku rodzinnego w stosunku do obowiązujących w Polsce do 2016 roku (tab. 18.2), warto przytoczyć przykłady krajów, do których emigrują Polacy, zwłaszcza młodzi, chcący zakładać rodzinę, m.in. z powodu dużo lepszego poczucia bezpieczeństwa socjalnego. Tymi krajami są Wielka Brytania, Niemcy, Irlandia. W tabeli 18.3. przedstawiono wysokość zasiłku rodzinnego w tych krajach w euro, co pokazuje istotne różnice w stosunku do zasiłków w Polsce do 2016 roku.

Tabela 18.3. Wysokość zasiłku rodzinnego w krajach UE w roku 2016 w euro (miesięcznie)

Kraj	Na jedno dziecko	Na dwójkę dzieci	Na trójkę dzieci	Na czwórkę dzieci
Irlandia Zasiłek pobierany jest do 16. r.ż. dziecka lub do 18. r.ż. w przypadku, gdy dziecko się uczy lub jest niesamodzielne z powodu niepełnosprawności	140	280	420	560
Niemcy Przysługuje na każde dziecko do 18. r.ż. Wypłacany miesięcznie na każde niepełnoletnie lub studiujące dziecko	190	380	576	797
Szwecja Przysługuje na każde dziecko do 18. r.ż. Wypłacany miesięcznie na każde niepełnoletnie lub studiujące dziecko	110	236	362	488
Wielka Brytania* Przysługuje na dzieci do 18 r.ż. Wypłacany cotygodniowo	26,3	43,71	61,12	78,53

*W Wielkiej Brytanii zasiłek rodzinny wypłacany jest cotygodniowo, co należy to uwzględnić, przeliczając na liczbę tygodni w roku. Nie zawsze to oznacza, że miesięcznie równa się 4 razy, jest to ok. 4,12 tygodni w miesiącu.

Źródło: opracowanie własne na podstawie (PWC Polska 2017)

Z kolei tabela 18.4 jest podsumowaniem porównania polskich zasiłków na rzecz rodzin wychowujących dzieci. Dla porównania ich wartości przyjęto najpierw polski złoty oraz walutę euro po kursie obowiązującym w ostatnim badanym roku 2019, przy czym należy zaznaczyć, że skumulowano obydwa już wówczas istniejące zasiłki pełniące tę samą rolę, tj. zasiłek rodzinny oraz zasiłek wychowawczy 500+.

Tabela 18.4. Wysokość skumulowanego zasiłku rodzinnego i wychowawczego 500+ jako odpowiednika zasiłku rodzinnego w krajach EU w euro (miesięcznie)

	Na jedno dziecko	Na dwójkę dzieci	Na trójkę dzieci	Na czwórkę dzieci
Polska – zasiłek rodzinny w euro (kurs 4,4)	28,1	56,3	84,5	112,7
Polska – łącznie zasiłek rodzinny i wychowawczy w zł	624	1248	1872	2496
Polska łącznie zasiłek rodzinny i wychowawczy w euro (kurs 4,4)*	141,8	283,6	425,4	567,2

*W krajach EU istnieje jeden zasiłek dedykowany wychowywaniu dzieci w rodzinach – zasiłek rodzinny. W Polsce od 2016 roku oprócz zasiłku rodzinnego istnieje wychowawczy 500+ . Z tego powodu w tabeli połączono obydwa zasiłki w Polsce dla porównania ich wartości do odpowiedników w krajach EU.

Źródło: opracowanie własne na podstawie przeglądu nowelizacji Ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych oraz Ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci

Porównywanie zasiłków dedykowanych rodzinie w Polsce i krajach Europy Zachodniej do 2016 roku wypadało zdecydowanie na korzyść krajów zachodnich. To zmieniło się od 2016 roku wraz z wprowadzeniem zasiłku wychowawczego 500+, który skumulowany ze standardowym zasiłkiem rodzinnym zaczął stanowić wartość już tylko niewiele mniejszą od jego odpowiedników w bogatych krajach tzw. starej UE. Jednocześnie należy zauważyć, że od 2016 roku, który w tej kwestii był przełomowy w Polsce, w krajach zachodnich następował powolny wzrost tych zasiłków dopasowujący ich wartość m.in. do inflacji, a wartość nominalna polskich zasiłków nie zmieniła się. Przykładem będą tutaj Niemcy, w których od 2021 roku wartość zasiłku rodzinnego, tzw. *Kindergeld*, wynosi odpowiednio 219 euro na pierwsze i drugie dziecko, na każde trzecie dziecko 225 euro oraz na każde czwarte i następne dziecko 250 euro. W stosunku do 2016 roku oznacza to wzrost o ok. 15%. Z każdym rokiem wartość polskiego odpowiednika, chociaż wciąż oznacza dużą pomoc państwa, w porównaniu do zachodnich odpowiedników spada. Istnieją szacunki (wciąż nieautoryzowane oficjalnie), że po uwzględnieniu inflacji w połowie 2021 roku zasiłek wychowawczy 500+ powinien wynosić już 620 zł, aby spełniał swoją rolę sprzed kilku lat. Czas pokaże, czy wartość tej pomocy państwa w zapewnieniu bezpieczeństwa socjalnego ulegnie podwyższeniu w ciągu najbliższych kilku lat.

Podsumowanie

Po 2016 roku w Polsce doszło do istotnego przełomu w obszarze wspierania finansowego rodzin, zwłaszcza rodzin wielodzietnych. Wprowadzenie zasiłku wychowawczego (rozumianego również jako rodzinnego) w wysokości 500 zł miesięcznie na każde dziecko do ukończenia 18. roku życia przesunęło Polskę z pozycji jednego z najmniej wspierającego rodziny kraju w Europie do grona państw hojnych pod tym względem. Można stwierdzić, że do najbogatszych państw Europy w tej kwestii już wiele nie brakuje. Porównując średnie zarobki w Polsce i państw Zachodniej Europy, należy uznać, że wprowadzenie zasiłku wychowawczego 500+ jest dużym podniesieniem poziomu materialnego rodzin w Polsce, zwłaszcza tych wielodzietnych. Nie będzie dużą przesadą stwierdzenie, że obserwowana dotychczas tylko w krajach Europy Zachodniej pomoc finansowa dla rodzin ze strony państwa została w dużej mierze zapewniona.

Literatura

1. CBOS (2020), *System wartości Polaków 2019*, <https://www.cbos.pl/PL/publikacje/news/2020/02/newsletter.php> (dostęp: 20.07.2021).
2. Czaplński J., Panek T. (red.) (2013), *Diagnoza Społeczna. Warunki i jakość życia Polaków*, <http://rops-opole.pl/wp-content/uploads/publikacje/Warunki%20i%20jakość%20życia%20Polakow.pdf> (dostęp: 20.07.2021).
3. Czaplński J., Panek T. (red.) (2015), *Diagnoza Społeczna. Warunki i jakość życia Polaków*, http://www.diagnoza.com/pliki/raporty/Diagnoza_raport_2015.pdf (dostęp: 20.07.2021).
4. Dziewięcka-Bokun L. (2003), *Bezpieczeństwo socjalne jako podstawa spokoju społecznego*, „Prace Naukowe/Akademia Ekonomiczna w Katowicach”, t. *Bezpieczeństwo socjalne*, s. 11-26.
5. GUS (2011), *Zasięg ubóstwa ekonomicznego w Polsce w 2011 r.*, https://stat.gov.pl/cps/rde/xbcr/gus/WZ_ubostwo_w_polsce_2011.pdf (dostęp: 22.07.2021).
6. GUS (2015), *Zasięg ubóstwa ekonomicznego w Polsce w 2015 r.*, <https://stat.gov.pl/obszary-tematyczne/warunki-zycia/ubostwo-pomoc-spoleczna/zasieg-ubostwa-ekonomicznego-w-polsce-w-2015-r-,14,3.html> (dostęp: 22.07.2021).
7. GUS (2019), *Zasięg ubóstwa ekonomicznego w Polsce w 2019 r.*, <https://stat.gov.pl/obszary-tematyczne/warunki-zycia/ubostwo-pomoc-spoleczna/zasieg-ubostwa-ekonomicznego-w-polsce-w-2019-roku,14,7.html> (dostęp: 20.07.2021).
8. Kubów A. (2014), *Znaczenie świadczeń rodzinnych w kształtowaniu poziomu życia rodziny*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu”, 364: *Polityka rodzinna w Polsce z perspektywy wybranych aspektów polityki społecznej i ekonomii. Doświadczenia innych państw europejskich*, s. 26-43.
9. Pacud R. (2002), *Standard bezpieczeństwa socjalnego jako kategoria normatywno-wzorcowa polityki zabezpieczenia społecznego*, „Polityka Społeczna”, 9, s. 14-18.
10. PWC Polska (2017), *Ulgi podatkowe i świadczenia rodzinne w UE 2016*, <https://www.pwc.pl/pl/pdf/ulgi-podatkowe-2017.pdf> (dostęp: 25.07.2021).
11. Sierpowska I. (2009), *Zasada bezpieczeństwa socjalnego w świetle zjawiska ekskluzji społecznej w Europie* [w:] Z. Pulka (red.), *Wybrane zagadnienia teorii i praktyki prawa europejskiego*, Państwowa Wyższa Szkoła Zawodowa w Legnicy, Legnica.
12. Zamorska K. (2010), *Prawa społeczne jako program przebudowy polityki społecznej*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław.
13. Ustawa z dnia 11 lutego 2016 roku o pomocy państwa w wychowywaniu dzieci (Dz.U. 2016 poz. 195).

14. Ustawa z dnia 28 listopada 2003 r. o świadczeniach rodzinnych (Dz.U. 2003 nr 228 poz. 2255, ze zm.).

FAMILY SOCIAL SECURITY THROUGH THE 500+ CHILD BENEFIT AND THE INFLUENCE ON THE INCREASE OF THE WEALTH OF THE FAMILY

Abstract: Socio-economic development in the 20th and 21st centuries is associated with a large intervention of states in helping families and their children. This assistance took the form of family benefits. The state committed itself to improving the living and working conditions of individuals and entire social groups. One of the main goals of the state's activities for the social security of citizens is the security of the family. Social transfers in the form of financial benefits, including family benefits, play a significant role in reducing the scope of poverty. The chapter presents the financial assistance of the state for Polish families, with particular emphasis on financial support for large families in terms of social security. Particular attention was paid to poverty in large families. With comparative own research, the activity of the Polish state in relation to other European Union's countries over the years from Poland's accession to the EU until 2021 was presented. Especially including the Polish child benefit 500+ with the similar activity of Western European countries was also presented.

Keywords: family allowance, financial assistance for families, 500+ program, social security for families

Rozdział 19

SŁUŻBY SPECJALNE UCZESTNIKAMI WALKI Z TERRORYZMEM NA POCZĄTKU XXI WIEKU (WYBRANE ASPEKTY)

Andrzej Żebrowski³¹, Izabela Szkurtat³²

Streszczenie: Walka z terroryzmem to złożony i trudny proces, w którym rozpoznanie i systematyczny monitoring stanowią podstawę prowadzonych działań ofensywnych i defensywnych. Skala i dynamika tego negatywnego zjawiska, a także trudności w prowadzeniu działań wyprzedzających wymagają ze strony służb specjalnych dostosowywania się do zmieniających się warunków. Terrorysty, wykorzystując zachodzące procesy w otoczeniu państw, a także przemiany cywilizacyjne, adoptują się do jakościowo nowych warunków. Wykorzystują wszelkie dostępne narzędzia pozwalające na destrukcyjne działania. Obok klasycznych przestrzeni, jakościowo nową przestrzenią konfrontacji jest cyberprzestrzeń, gdzie wykorzystuje się jej właściwości. W tych przestrzeniach działania ofensywne i defensywne podejmują służby specjalne, których potencjały operacyjne pozwalają na walkę z tym zagrożeniem. Prowadzą aktywne działania w osobowej i technicznej przestrzeni informacyjnej, gdzie człowiek nadal odgrywa podstawową rolę. Człowiek i technika, przy wsparciu prawnym, finansowym, a także władzy politycznej, sprawiają, że walka z terroryzmem wymaga poszukiwania skutecznych form, metod i środków destrukcji. Kompleksowe podejście i zaangażowanie służb specjalnych przy racjonalnej polityce i działaniu może skutkować neutralizowaniem tego negatywnego zjawiska, jakim jest terroryzm.

Słowa kluczowe: służby specjalne, terroryzm, walka

Wprowadzenie

Terroryzm zdominował przemiany cywilizacyjne, wykorzystując wszelkie możliwości pozwalające na przeprowadzenie ataku ukierunkowanego na zadanie jak największych start wśród ludności. Wspierany jest przez media, które zapewniają nie tylko rozgłos, ale poprzez przekaz opatrzone komentarzem zabezpieczają potrzeby informacyjne terrorystów, wskazując m.in. działania podmiotów sił policyjnych. Procesy związane z globalizacją dotyczą wszystkich funkcji państwa (państw). Ich monitorowanie pozwala terrorystom na swobodne poruszanie się w globalnym środowisku bezpieczeństwa. Skala, dynamika, zorganizowanie i znajomość obiektów

³¹ Uniwersytet Pedagogiczny im. KEN w Krakowie, Instytut Nauki o Bezpieczeństwie

³² Akademia Pomorska w Słupsku, Instytut Bezpieczeństwa i Zarządzania

pozwalają na dokonywanie spektakularnych ataków z wykorzystaniem niekiedy niekonwencjonalnych środków destrukcji. W obliczu istniejących zagrożeń i dostosowywania się organizacji terrorystycznych do zmieniających się warunków funkcjonowania, państwa podejmują wiele złożonych decyzji i działań, których celem jest zwalczanie organizacji terrorystycznych. Państwa dysponujące wyspecjalizowanymi podmiotami do walki z terroryzmem wyposażają m.in. służby specjalne w uprawnienia umożliwiające walkę z terroryzmem zarówno na własnym terytorium, jak i poza jego granicami. W materiale zostały poruszone kwestie dotyczące walki z terroryzmem ze wskazaniem na działalność służb specjalnych, których potencjały operacyjne pozwalają na realizowanie wielu złożonych przedsięwzięć. Służby specjalne, z uwagi na możliwość niejawnego penetrowania osobowej i technicznej przestrzeni informacyjnej, wpisują się w trwającą globalną wojnę informacyjną, w której prowadzone operacje informacyjne ukierunkowane są na rozpoznawanie organizacji terrorystycznych. Celem rozdziału jest ukazanie, jaki wpływ na bezpieczeństwo międzynarodowe mają służby specjalne względem zwalczania terroryzmu w dobie globalnej wojny informacyjnej.

Charakterystyka problemu

Globalne środowisko bezpieczeństwa międzynarodowego to miejsce ogólnoświatowej wojny informacyjnej, gdzie jej uczestnicy mają zróżnicowane cele strategiczne, operacyjne i taktyczne. Zalicza się do nich również międzynarodowe organizacje terrorystyczne, które wykorzystują trwający globalny konflikt informacyjny dla swoich partykularnych interesów. Generalnie jednak celem strategicznym jest przejęcie kontroli nad człowiekiem i jego środowiskiem.

Podmioty państwowe i pozapaństwowe podejmują wiele złożonych decyzji ukierunkowanych na uderzenie w przeciwnika wewnętrznego i zewnętrznego, gdzie agresja informacyjna jest domeną przede wszystkim wyspecjalizowanych jednostek (komórek) organizacyjnych sektora państwowego i prywatnego, międzynarodowego i narodowego, także organizacji terrorystycznych, które dysponują narzędziami pozwalającymi na realizację przyjętych celów. Cel to kontrola zarówno w osobowej, jak i technicznej przestrzeni informacyjnej, gdzie motorem postępu są osiągnięcia nauki i techniki. W obecnych czasach szczególną uwagę zwraca się na rozwój środków wykorzystywanych na potrzeby podmiotów, w których agresja informacyjna zajmuje kluczową pozycję w trwającej kooperacji negatywnej. Coraz większą uwagę zwraca się na kwestie związane z dominacją informacyjną nad przeciwnikiem. W dobie rewolucji w technikach komunikacyjnych i teleinformatycznych, które zdominowały współczesne konflikty w sferach militarnej i pozamilitarnej, pokonanie przeciwnika w sferze informacyjnej jest czynnikiem decydującym o ogólnym sukcesie w trwającej wojnie informacyjnej. Należy przyjąć, że obecnie wojna jest najbardziej nadużywanym pojęciem w polityce uprawianej przez wszystkich uczestników stosunków międzynarodowych, a także podmioty pozapaństwowe naruszające zasady prawa krajowego i międzynarodowego. Z uwagi na to, że bardzo często konflikty międzynarodowe i wewnętrzne wzajemnie się przenikają, wszystko jest nazywane wojną. Określenie przemocy jako wojny, bez względu na jej podłoże, zawsze wiąże się z ryzykiem.

Globalna wojna informacyjna i jej wpływ na bezpieczeństwo

Wojna informacyjna to jednak przemoc na ogromną skalę, do której dochodzi na całym świecie, a obiektem ataku jest społeczność międzynarodowa. Agresja informacyjna bardzo często jest elementem szerszego konfliktu w sferach materialnej i duchowej, gdzie (Gawliczek, Pawłowski 2003, s. 12-13):

- 1) w sferze materialnej przyjmuje postać konfrontacji informacyjnej, obejmującej wszelkie działania informacyjne w odniesieniu do przeciwnika, prowadzone z zamiarem promowania określonego celu politycznego, gospodarczego lub wojskowego, przy równoczesnym zapewnieniu odpowiedniej ochrony własnym systemom informacyjnym;
- 2) w sferze duchowej przejawia się w formie:
 - wojny kulturowej,
 - wojny religijnej,
 - konfrontacji etycznej.

Uczestnicy stosunków międzynarodowych w procesie realizacji swoich partykularnych interesów na użytek wewnętrzny i zewnętrzny posiłkują się pojęciem „wojna”, wskazując m.in. na wojny z terroryzmem, przestępczością zorganizowaną o charakterze transnarodowym, państwami upadłymi, opozycją wewnętrzną, parlamentarną i pozaparlamentarną, wrogimi reżimami, nielegalną migracją, narkotykami, pandemią, kobietami czy religią, a także wojny o dostęp do naturalnych surowców energetycznych lub zasobów bezpiecznej wody pitnej. Przy właściwej analizie i argumentacji praktycznie każdy konflikt, bez względu na podłoże, można potraktować jako „wojnę”.

Warto mieć na uwadze to, że taka retoryka stanowi drogę do hysterii, która w dobie pandemii COVID-19 narusza istniejące reżimy bezpieczeństwa w stosunkach międzynarodowych. Stanowi ona podatny grunt dla wszelkiego rodzaju decyzji politycznych. Przykładem jest np. oficjalna decyzja Stanów Zjednoczonych (22.11.2020 r.) o wycofaniu się z międzynarodowego traktatu „o otwartym niebie”, który umożliwia identyfikowanie ruchów wojsk, organizacji terrorystycznych i przestrzegania układów o ograniczaniu broni przez państwa – sygnatariuszy. Walka informacyjna koncernów farmaceutycznych o skuteczność produkowanych szczepionek przeciwko COVID-19, która dla strony wygranej przyniesie bliżej nieokreślone korzyści finansowe, może być wykorzystywana przez silnych uczestników w trwającym globalnym konflikcie informacyjnym. Na uwadze należy mieć także, obok trwającego konfliktu zbrojnego na Ukrainie, wojnę w Górskim Karabachu. Kolejna ważna kwestia to zamach terrorystyczny w Nicei (Francja), który można uznać za rozpoznanie pola konfrontacji – walkę. Jednym z celów mogło być sprawdzenie reakcji władz (centralnych, lokalnych) i zdolności służb do walki z zagrożeniami terrorystycznymi. Nie można także zapominać o trwającej migracji (w tym nielegalnej), którą należy traktować nie tylko jako wsparcie dla rynku pracy i rozwoju przedsiębiorstw, ale także jako potencjalna baza werbunkowa dla organizacji terrorystycznych i przestępczych, droga przenikania członków organizacji terrorystycznych, a ponadto jako zagrożenie związane z trwającą globalną pandemią COVID-19. „Można założyć, że hakerzy po prostu wykorzystują okno możliwości związane z wybuchem tzw. pandemii koronawirusa nowego typu. Gdy wszyscy

zajęli się walką z nim, mogą osłabiać działania związane z ochroną sieci informacyjnych” (Kramarski 2021, s. 27).

Można założyć, że pandemia COVID-19 w 2020 roku spowolniła, a nawet zahamowała dynamikę ataków terrorystycznych i działań zorganizowanych grup przestępczych o charakterze transnarodowym w stosunku do ich skali sprzed pandemii. Przebieg, zasięg i dynamika rozprzestrzeniania się koronawirusa, a także niewydolność państw w jego zwalczaniu, pozwalają dostosować się organizacjom terrorystycznym i zorganizowanym grupom przestępczym do jakościowo nowej rzeczywistości. To również czas na poszukiwanie nowych form ataków, przy jednoczesnym minimalizowaniu własnych strat. Warto mieć na uwadze to, że realizacji celów przez organizacje terrorystyczne sprzyjają masowe wystąpienia społeczeństw demonstrujących swoje niezadowolenie o zróżnicowanym podłożu. Obserwowana i analizowana jest także reakcja władz, która niekiedy eskaluje pojawiające się zagrożenia. Takie prowokacyjne działania sprawujących władzę w stosunku do społeczeństwa jest wykorzystywane przez różne podmioty, w tym i organizacje terrorystyczne. Przeprowadzenie ataku terrorystycznego w takich warunkach to bliżej nieokreślona liczba ofiar wśród demonstrujących, a także organów (właściwych w sferze bezpieczeństwa i porządku publicznego) zabezpieczających przebieg demonstracji.

Media, będące narzędziem w trwającej globalnej wojnie informacyjnej, obok spraw związanych z walką z koronawirusem wskazują na istniejące zagrożenia dotyczące wielu zjawisk, których kumulacja zwiększa rozprzestrzenianie się wirusa, co bezpośrednio przekłada się na liczbę zarażonych i śmiertelność. Należą do nich np. migracja i lekceważenie zakazów przy braku szczepionki pozwalającej na walkę z COVID-19, a także kierowanie się partykularnymi interesami zorientowanymi na korzyści polityczne, ideologiczne, ekonomiczne i finansowe. W tym globalnym konflikcie człowiek jest najmniej ważny, ważne są cele – bez względu na ponoszone straty.

Pandemia to szczególnie czas dla wszystkich, również dla terrorystów i zorganizowanych grup przestępczych. Podmioty naruszające prawo międzynarodowe i krajowe, realizując swoje cele polityczne, ekonomiczne itp., wykorzystują nieudolność władzy wykonawczej, w tym ograniczenia w działalności służb, organizacji i instytucji w zapewnieniu bezpieczeństwa wewnętrznego państwa. Ponadto warto mieć na uwadze, że terrorizm czasu pandemii COVID-19 jest kolejnym (po zamachu terrorystycznym z 11 września 2001 roku w Stanach Zjednoczonych), jakościowo nowym pod względem warunków, przejawem aktów przemocy w środowisku bezpieczeństwa międzynarodowego.

Pandemia, z uwagi na swój charakter, jest bardzo poważnym wyzwaniem nie tylko dla jednostki, grupy społecznej, narodu czy państwa, ale także dla organizacji terrorystycznych i zorganizowanych grup przestępczych o charakterze transnarodowym. Dotyczy to również wyspecjalizowanych podmiotów władzy wykonawczej, właściwych w walce z terroryzmem międzynarodowym. Na uwadze należy mieć służby policyjne (cywilne i wojskowe), wywiad, kontrwywiad, wyspecjalizowane jednostki kontrterrorystyczne i antyterrorystyczne, służby finansowe, służby ochrony granic i celno-skarbowe, prokuraturę, sądy, siły zbrojne, jednostki walki elektronicznej, jednostki wojny informacyjnej, jednostki wojny psychologicznej itp.

Historia i aktualny stan stosunków międzynarodowych pokazują, że rozpad bipolarnego podziału świata, a tym samym zanik wszelkich barier, skutkuje tym, iż

„wraz z postępującą globalizacją nastąpił gwałtowny wzrost zagrożeń, których skala, zasięg i perspektywa urzeczywistnienia ma szerszy, ponadpaństwowy i ponadregionalny wymiar, a ponadto permanentny charakter” (Barcz, Libera 2007, s. 165).

Terroryzm międzynarodowy i jego wpływ na bezpieczeństwo

Tymi zagrożeniami są niewątpliwie: terroryzm międzynarodowy, terroryzm wewnętrzny, cyberterroryzm i transgraniczna przestępczość zorganizowana (w tym przestępczość komputerowa), które wspierane są przez operacje informacyjne i sytują się w globalnym konflikcie informacyjnym (wojnie informacyjnej). Należy podkreślić, że w społeczności międzynarodowej dominują procesy związane z globalizacją, które stanowią źródło wielu złożonych zagrożeń o charakterze asymetrycznym zarówno ze strony podmiotów pozapaństwowych (międzynarodowych organizacji terrorystycznych), jak i państwowych (władzy wykonawczej, która dysponuje wyspecjalizowanymi agendami posiadającymi możliwości wykonawcze do prowadzenia zamachów terrorystycznych). Ten rodzaj działalności władzy jest ukierunkowany na wszelkie podmioty wewnętrzne będące przeciwnikami partii sprawującej władzę, a także na własnych zwolenników, aby poprzez propagandę i manipulację poszukiwać u nich wsparcia dla realizowanej polityki (zagranicznej i wewnętrznej). Działaniom tego typu najczęściej towarzyszy podsycanie i wyzyskiwanie społecznego niezadowolenia, co może być niebezpieczne dla państwa i jego otoczenia zewnętrznego. „Może bowiem doprowadzić do kryzysu, a nawet konfliktu wewnętrznego lub konfliktu z innymi państwami (w tym graniczącymi). [...] Wykorzystuje się niezadowolenie społeczeństwa, wszelkiego rodzaju manipulacje, co wspiera przede wszystkim istniejące rozbieżności między realiami dnia codziennego a oczekiwaniami wynikającymi z wcześniejszych porozumień i obietnic wyborczych” (Dworecki 1996, s. 33). Obecna tu jest koniunkturalna retoryka elit politycznych, łączona z obietnicami pozwalającymi na pozyskanie wsparcia w utrzymaniu i/lub zdobyciu władzy. Najczęściej dominuje kolizja ideologii i sposobu sprawowania władzy z indywidualnymi ambicjami politycznymi członków elit władzy (i przywódców) (Dworecki 1996, s. 33). Rządzący posługują się zróżnicowanymi narzędziami, „począwszy od prostego kłamstwa, aż po czystą prawdomówność, która niekiedy bywa tragiczna w skutkach (często bywa, że powiedzenie prawdy kończy prowadzoną grę polityczną i zapoczątkowuje działania wojenne). Do instrumentarium tego należą również: przemilczenie, protokół dyplomatyczny, promocja, obłuda, propaganda, posunięcia i argumenty gospodarcze, oszustwo, dementi, manipulacja i intryga” (Chudy 2004, s. 14), a ponadto: wprowadzanie w błąd, zatajenie, ukrywanie, kręcenia, fabrykowanie, maskowanie, dwuznaczność, zmyślanie, unikanie, opóźnianie, wywieranie wpływu itp. (Walters 2004, s. 14). W skrajnych przypadkach, uzasadnianych rozwojem sytuacji i celem (celami), strona ofensywna stosuje również przemoc w postaci ataku terrorystycznego (np. ekonomicznego – obniżanie poziomu życia społeczeństwa, wykluczenie, bieda).

Podsumowanie

Terroryzm jest złożonym zjawiskiem, które rozwija się, wykorzystując procesy związane m.in. z procesami towarzyszącymi globalizacji. Kieruje się ideami o zróżnicowanym podłożu, a celem ataku jest najczęściej bezbronna ludność. Mimo wysiłków podejmowanych przez państwa dysponujące rozbudowanym aparatem walki z terroryzmem – straty są poważne, a walka niezmiernie trudna. Na szczególną uwagę zasługują służby specjalne, które są wyposażone w rozbudowany aparat zasilający w informacje, a także aparat wykonawczy pozwalający na prowadzenie walki z terroryzmem. Osobowe i techniczne środki pracy operacyjnej pozwalają na monitorowanie tego złożonego środowiska, pamiętając, że świat jest niebezpieczny i wymaga racjonalnych decyzji i działań.

Literatura

1. Chudy W. (2004), *Kłamcy profesjonalni? Praca dyplomaty i szpiega w ujęciu etyki*, Maternus Media, Tychy.
2. Dworecki S. (1996), *Od konfliktu do wojny*, Wydawnictwo Buwik, Warszawa.
3. Gawliczek P., Pawłowski J. (2003), *Zagrożenia asymetryczne*, Wydawnictwo AON, Warszawa.
4. Kramarski I. (2021), *Cyberatak na Amerykę*, „Raport. Wojsko. Technika. Obronność”, 1, s. 26-29.
5. Libera B. (2007), *Rodzaje zagrożeń w środowisku międzynarodowym*, [w:] Barcz J., Libera B. (red.), *Urzędnik i biznesmen w środowisku międzynarodowym. Wybrane aspekty pragmatyki zawodowej*, s. 165-176, Wolters Kluwer, Kraków.
6. Walters S.B. (2003), *Kłamstwo cała prawda o... Jak wykryć kłamstwo i nie dać się oszukać*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk.

INTELLIGENCE AGENCIES AS PARTICIPANTS IN THE FIGHT AGAINST TERRORISM AT THE BEGINNING OF THE 21ST CENTURY (SELECTED ASPECTS)

Abstract: The fight against terrorism is a complex and difficult process, where reconnaissance and systematic monitoring constitute the basis of offensive and defensive activities. The scale and dynamics of this negative phenomenon, as well as difficulties in conducting pre-emptive interventions, require the Intelligence Agencies to adapt to changing conditions. Terrorists use the processes taking place in the environment of states, as well as civilization changes, to adapt to qualitatively new conditions. They use all available tools that allow for destructive actions. In addition to classical spaces, cyberspace is a new qualitative confrontation space, where its properties are used. In these areas, offensive and defensive actions are taken by Intelligence Agencies, whose operational potentials allow them to fight this negative threat. They are active in the personal and technical information space, where the human still plays the basic working tool. Man and technology, with the support of legal, financial and political power make that the fight against terrorism requires searching for effective forms, methods and means of destruction. A comprehensive approach and involvement of Intelligence Agencies with rational policy and action may result in neutralizing this negative phenomenon of terrorism.

Keywords: secret services, fight, terrorism

Rozdział 20

BEZPIECZEŃSTWO SŁUŻB SPECJALNYCH WYBRANE ASPEKTY

Andrzej Żebrowski³³

Streszczenie: Służby specjalne, usytuowane w strukturze władzy wykonawczej, wykonują wiele złożonych zadań wywiadowczych i kontrwywiadowczych. Z uwagi na ich niejawny charakter, posiadany potencjał operacyjny pozwalający na realizację zadań w otoczeniu wewnętrznym i zewnętrznym państwa – znajdują się w zainteresowaniu przeciwnika. Cel to przejęcie władztwa nad ich zasobami informacyjnymi. Tym samym służby znajdują się w sferze aktywności informacyjnej przeciwnika wewnętrznego i zewnętrznego państwa. Ta aktywność to atak informacyjny (zdobycie informacji) i zakłócanie informacyjne. Są to kompleksowe działania prowadzone w osobowej i technicznej przestrzeni informacyjnej. Wspierane są przez techniki teleinformatyczne, komunikacyjne i Internet, a także nowoczesne technologie produkcji. Służby specjalne są aktywnymi uczestnikami trwającego ogólnoswiatowego konfliktu informacyjnego, prowadząc ofensywne i defensywne operacje informacyjne na niejawnym froncie konfrontacji. Skala i dynamika zachodzących procesów w globalnym środowisku bezpieczeństwa to ewoluujące zagrożenia, angażujące służby specjalne do ich rozpoznawania.

Słowa kluczowe: bezpieczeństwo, zagrożenia, służby specjalne

Wprowadzenie

Służby specjalne zawsze związane są z władzą wykonawczą, co wynika z charakteru realizowanych zadań i posiadanych uprawnień (praca operacyjna w kraju i za granicą). Będąc wyspecjalizowanymi agendami rządowymi, zabezpieczają potrzeby informacyjne uprawnionych podmiotów cywilnych i wojskowych, a także własne. Uprawnienia do prowadzenia czynności operacyjno-rozpoznawczych w globalnym środowisku bezpieczeństwa, a także w otoczeniu wewnętrznym państwa, niejawne metody ich prowadzenia, posiadane środki pracy ze szczególnym wskazaniem na tzw. agenturę, penetrację osobowej i technicznej przestrzeni informacyjnej, posiadane bazy danych i kierunki zainteresowań operacyjnych sprawiają, że wywiad i kontrwywiad znajdują się w operacyjnym zainteresowaniu obcych służb specjalnych. Oznacza to, że służby muszą prowadzić aktywną politykę bezpieczeństwa

³³ Uniwersytet Pedagogiczny im. KEN, Instytut Nauki o Bezpieczeństwie w Krakowie, Instytut Nauki o Bezpieczeństwie

własnej infrastruktury, chroniąc przed zewnętrznymi i wewnętrznymi atakami informacyjnymi i zakłócaniem informacyjnym. W materiale przedstawione zostały: charakterystyka środowiska działania służb specjalnych, zagrożenia i działania defenzywne ukierunkowane na zminimalizowanie skutków ataku.

Służby specjalne

Służby specjalne są tajnymi agendami rządowymi, usytuowanymi w strukturach władzy wykonawczej, organizacyjnie samodzielными lub wchodzącymi w skład innych jednostek państwowych, cywilnych i wojskowych instytucji, uprawnionymi do prowadzenia zakonspirowanych działań o charakterze niejawnym (potencjał operacyjny, czynności operacyjno-rozpoznawcze, metody i środki pracy operacyjnej) mających na celu (Larecki 2017, s. 797):

- ochronę interesów narodowych, bezpieczeństwa państwa oraz jego instytucji politycznych i obywateli przed różnymi zagrożeniami ze strony sił zewnętrznych i wewnętrznych, m.in. takich jak szpiegostwo, działania przeciw polityce zagranicznej, działania antypaństwowej opozycji, zamachy, terroryzm, sabotaż, proliferacja broni masowej zagłady, międzynarodowa przestępczość zorganizowana itp. (przedmiot działań cywilnych i wojskowych służb wywiadu, służb kontrwywiadu, służby bezpieczeństwa, policji politycznej lub odrębnej policji ds. cudzoziemców), ujawniania i zwalczanie szczególnie groźnych przestępstw, zabezpieczanie tajemnic państwowych;
- zdobywanie, opracowywanie i dostarczanie uprawnionym podmiotom władzy państwowej, niedostępnymi innymi sposobami, wiarygodnych informacji o sytuacji (zdarzeniach i procesach) politycznej, społecznej, gospodarczej i militarnej w innych państwach, regionach czy miejscach świata lub o osobach – pod kątem interesów i zagrożeń dla własnego państwa (w głównej mierze cele te realizują cywilne i wojskowe służby wywiadu);
- prowadzenie operacji specjalnych przeciw różnym innym aktualnym i potencjalnym źródłom zagrożeń dla bezpieczeństwa państwa.

Do podstawowych, specyficznych cech działania służb specjalnych zalicza się (Larecki 2017, s. 797):

- pozyskiwanie, przygotowywanie wykorzystywanie specjalnie dobranych współpracowników (osobowe źródła informacji) pod kątem nakreślonych celów i zadań oraz obiektów zainteresowań;
- zbieranie i wykorzystywanie materiałów kompromitujących;
- przestrzeganie zasad konspiracji (m.in. stosowanie kryptonimów, pseudonimów, wykorzystywanie legend, przykryć);
- stosowanie specyficznych metod pracy operacyjnej i specjalnych środków techniki operacyjnej.

Należy mieć na uwadze to, że służby specjalne, które stosują w swych działaniach niejawne metody i formy pracy operacyjnej, pełnią funkcje: informacyjne (dostarczanie niejawnych informacji i materiałów), procesowe, ochronne, kontrwywiadowcze (ofensywne rozpoznanie obcych służb specjalnych), akcje niejawne, aktywne przedsięwzięcia, dezinformacja, manipulacja, dywersja, sabotaż, szantaż.

Służby zawsze znajdują się na pierwszej linii konfrontacji w czasie pokoju, stanie kryzysu i konfliktu zbrojnego. W tych jakościowo nowych warunkach (dyktowanych przez poszczególne stany) muszą zmierzać się z przeciwnikiem w warunkach turbulentnego środowiska bezpieczeństwa międzynarodowego. Asymetryczne środowisko działania służb specjalnych to systematyczna konfrontacja w tzw. rozregulowanym otoczeniu, gdzie istniejące problemy związane z koniecznością ich rozwiązywania przez służby mają związek m.in.:

- ze stałym poszerzaniem się przestrzeni działania państw, a w związku z tym i służb wywiadu i kontrwywiadu;
- z ewoluującymi zmianami w środowisku międzynarodowym, gdzie rośnie zakres wzajemnych zależności, a procesy społeczne, polityczne, ekonomiczne, narodowościowe, religijne czy wojskowe stale się komplikują, co sprawia, że wiele państw posiada trudności w zaadoptowaniu się do tej rzeczywistości;
- z postępującym procesem umiędzynarodowienia działalności gospodarczej, której towarzyszy zmiana reguł w odniesieniu do przepływu surowców, finansów, towarów, usług, ludności oraz informacji;
- z rozwijaniem się międzynarodowej przestępczości zorganizowanej, której działalność przekracza granice państwowe, a tożsamość i określenie kraju pochodzenia staje się trudne nie tylko do zidentyfikowania, ale i zwalczania;
- z rozwijaniem się międzynarodowego terroryzmu, jego nieprzewidywalnością co do wyboru obiektu ataku, stosowanych form i metod, a także stosowanych środków fizycznej destrukcji;
- z ekspansją innych wzorców, co sprawia, że tradycje, doświadczenie, wizerunek i pochodzące z odmiennych kultur stanowi poważne zagrożenie dla bezpieczeństwa środowiska międzynarodowego;
- z rozwojem epidemii i pandemii, które dominują w globalnej przestrzeni bezpieczeństwa i wyznaczają zachowania władz i społeczeństw;
- z rozwojem masowego przemieszczania się ludności, co stanowi wyzwanie dla państw dotkniętych tym zjawiskiem oraz organizacji międzynarodowych.

To niewątpliwie zmiana w filozofii podejścia służb specjalnych do realizowanych zadań w otoczeniu państwa w skali globalnej, co wpływa na rozwiązywanie takich problemów, jak (Małara 2006, s. 15):

- poszukiwanie wartościowych źródeł informacji, nie ograniczając się tylko do własnego kraju i tych obiektów, które znajdują się (bądź znajdują) w ich operacyjnym zainteresowaniu, a także poszukiwanie partnerów wśród zagranicznych służb wywiadowczych i kontrwywiadowczych;
- identyfikowanie sytuacji i wynikających z nich szans oraz zagrożeń w otoczeniu, a także antycypowanie rzeczywistości organizacyjnej w perspektywie strategicznej;
- wykorzystywanie metod analizy i planowania umożliwiających gromadzenie informacji, tworzenie planów i programów realizacji w wymiarze globalnym;
- stosowanie zasad elastyczności w opracowywaniu planów i wola ustawicznej zmiany obszarów i sposobów działania w miarę zmieniania się warunków działania wywiadu i kontrwywiadu;

- rozwijanie umiejętności podejmowania ryzyka i godzenia się na niepewność, jaką niesie przyszłość;
- zdolność wykorzystywania źródeł przewagi informacyjnej w skali lokalnej, regionalnej i globalnej;
- wprowadzanie nowych koncepcji i metod zarządzania, zwłaszcza dotyczących umiejętności zarządzania zmianami w celu osiągnięcia ogólnie pojmowanej sprawności organizacyjnej służb, niezbędnej do prowadzenia bieżącej działalności w wielonarodowym i multikulturowym otoczeniu.

Służby specjalne były i są strategicznym uczestnikiem wojny informacyjnej, a wywiad postrzegany jest jako wyspecjalizowana i odpowiednio zorganizowana służba państwowa, której podstawowym zadaniem jest zbieranie informacji o przeciwniku i prowadzenie operacji informacyjnych. Z kolei analogiczne działania, ale o charakterze defensywnym, wykonują służby kontrwywiadu. W trakcie operacji informacyjnych prowadzą m.in. bitwy na bity, co sprowadza się do niszczenia zasobów informacyjnych przeciwnika, jego sieci: teleinformatycznych, telekomunikacyjnych, elektrycznych, finansowych czy ruchu powietrznego. Pojawia się bowiem tzw. nowe pokolenie „wojowników wiedzy”, intelektualistów w mundurach i bez, wyznających zasadę, że wiedza pozwoli na zapobieganie lub wygranie wojny.

Do ważniejszych obszarów aktywnego zainteresowania operacyjnego służb specjalnych, gdzie są lub będą podejmowane przedsięwzięcia rozpoznawcze, należą (Larecki, 2017, s. 439):

- analizy i oceny długofalowych kierunków politycznych;
- problemy gospodarcze w skali globalnej;
- polityczne i ekonomiczne procesy integracyjne w Europie i na świecie;
- rzeczywiste i potencjalne kryzysy i konflikty rzutujące na bezpieczeństwo poszczególnych państw i środowiska międzynarodowego, ich przyczyny i charakter;
- nielegalna proliferacja broni ABC i środków do jej produkcji;
- terroryzm, ekstremizm i fundamentalizm religijny we wszystkich formach;
- międzynarodowa przestępczość zorganizowana (w tym handel bronią i narkotykami);
- korupcja i pranie brudnych pieniędzy;
- nielegalna migracja ludności (zorganizowane siatki przerzutu);
- czystki etniczne;
- ambicjonalne działania lokalnych dyktatorów;
- rozpoznawanie nowoczesnych zabezpieczeń systemów informacyjnych (cyberbezpieczeństwo) stosowanych dla przeciwdziałania obcej penetracji szpiegowskiej;
- ochrona środowiska naturalnego w związku z możliwością skażeń w efekcie działań człowieka lub samoistnych klęsk ekologicznych.

Jeżeli chodzi o nowe zadania służb bezpieczeństwa i kontrwywiadu, to są one uzupełniane przez obowiązujące i tradycyjne kierunki działania. Stanowią one coraz większe zagrożenia zarówno dla bezpieczeństwa wewnętrznego państw, jak i dla całego środowiska międzynarodowego. Do najważniejszych z nich należy m.in.:

- zwalczanie krajowego i międzynarodowego terroryzmu;
- rozpoznawanie i redukcja zagrożeń wynikających z fundamentalizmu religijnego i ekstremizmu politycznego;
- ujawnianie i przeciwdziałanie działalności międzynarodowej przestępczości zorganizowanej w świetle postanowień państw – członków ONZ;
- przeciwdziałanie handlowi narkotykami, nielegalnemu obrotowi bronią, materiałami wybuchowymi i rozszczepialnymi oraz związanym z tym procederem prania brudnych pieniędzy;
- zwalczanie handlu ludźmi;
- ujawnianie aktów destabilizujących gospodarkę kraju (szpiegostwo, korupcja, niekorzystne dla firm decyzje kierownictw krajowych czy korporacji spółek zagranicznych itp.);
- zwalczanie obcego szpiegostwa, w tym komputerowego i innych przestępstw komputerowych, a także ochrona systemów i sieci informatycznych i informacyjnych przed atakami w cyberprzestrzeni (wojna informacyjna).

W epoce społeczeństwa cybernetycznego, w której postęp naukowo-techniczny i technologiczny decyduje o rozwoju poszczególnych państw, ochrona informacji istotnych dla bezpieczeństwa państwa nabiera szczególnego znaczenia. Na podkreślenie zasługuje bezpieczeństwo systemów i sieci teleinformatycznych oraz sieci komunikacyjnych, które wykorzystywane są zarówno przez podmioty państwowe, jak i pozapaństwowe. Szczególne zadania służb to zapobieganie i przeciwdziałanie terroryzmowi, ochrona zdolności obronnych i ekonomicznych państwa, które kształtują jego międzynarodową pozycję, eliminują zagrożenia dla bezpieczeństwa wewnętrznego i porządku konstytucyjnego oraz korupcji, a także przeciwdziałanie penetracji obcych służb wywiadowczych i kontrwywiadowczych. Służby kontrwywiadu cywilnego i wojskowego zapewniają kontrwywiadowczą ochronę państwa, szczególnie w aspekcie właściwego funkcjonowania elementów infrastruktury krytycznej, gospodarki państwa i jego systemu obronnego.

Istotnym obszarem zainteresowania wywiadu i kontrwywiadu każdego państwa jest inwigilowanie osób i organizacji, których działalność wymierzona jest w podstawowe interesy ekonomiczne i społeczne, w tym zwalczanie korupcji osób pełniących ważne funkcje publiczne oraz zaangażowanych w działania zorganizowanych grup przestępczych. Służby specjalne współuczestniczą również w eliminowaniu szczególnie ciężkich form przestępczości, m.in. związanych z produkcją towarów, technologii i usług o strategicznym znaczeniu (tzw. podwójnego zastosowania) oraz obrotem nimi, nielegalnym wytwarzaniem broni, amunicji i materiałów wybuchowych, ich posiadaniem i handlem, przestępstw związanych ze środkami odurzającymi i narkotykami, środkami radioaktywnymi itp.

Skuteczność polityki i strategii bezpieczeństwa państwa wymaga ze strony egzekutywy i legislatywy dbania o solidne zaplecze zasilania w informacje z otoczenia wewnętrznego i zewnętrznego państwa, jakie stanowią cywilne i wojskowe służby wywiadu i kontrwywiadu z uwagi na posiadane potencjały operacyjne.

Zagrożenia

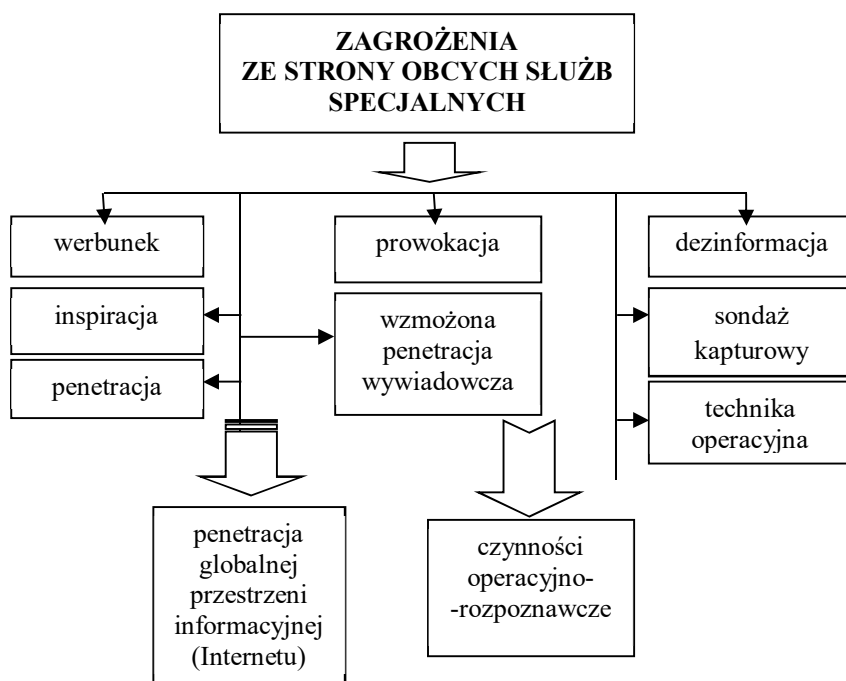
Współczesne zagrożenia wkroczyły w nową fazę i stanowią poważny problem dla każdego państwa (w tym i dla służb specjalnych), a w konsekwencji całego środowiska międzynarodowego. Inny jest ich cel, skala oraz dynamika. Służby specjalne i ich potencjały operacyjne znajdują się w zainteresowaniu nie tylko obcych służb specjalnych, ale także organizacji przestępczych o charakterze transnarodowym, organizacji terrorystycznych i innych podmiotów zagrażających bezpieczeństwu państwa. Zagrożenie to stan zmniejszonego poczucia bezpieczeństwa w toku prowadzenia działań konspiracyjnych, stwarzający ryzyko możliwej dekonspiracji oficera operacyjnego lub agenta czy grupy osób, np. siatki szpiegowskiej. Powstanie zagrożenia sygnalizują pewne symptomy, takie jak np.: zwiększone zainteresowanie i aktywność operacyjna wrogiej służby kontrwywiadu wobec danej osoby lub osób czy wpadka jednego z ogniw siatki (łącznika czy radiotelegrafisty) itp. (Larecki 2017, s. 950).

Szpiedzy cisną się ze wszystkich stron, starając się uzyskać dostęp do najistotniejszych sfer życia nie tylko państw czy organizacji międzynarodowych, ale i organizacji przestępczych. Taką wiedzę posiadają zarówno podmioty państwowe, jak i pozapaństwowe, szczególnie te, które wykonują zadania związane z bezpieczeństwem państwa, a więc są nośnikami informacji o charakterze niejawnym. „Szpiegostwo stanowi zakulisową i prowadzoną nielegalnymi środkami walkę o władzę, która rozgrywa się na całym świecie w sferze politycznej, militarnej i gospodarczej (naukowej – przyp. autora). Co roku coraz większą część światowego produktu globalnego pochłania opłacanie niezliczonych tysięcy tajnych agentów oraz wyposażenie służb specjalnych w wysokiej klasy sprzęt techniczny” (Piekalkiewicz 1999, s. 10).

„Krótko mówiąc, [...] stolice państw stanowią prawdziwe targowisko agentów, informatorów, donosicieli, instruktorów, doradców i radiotelegrafistów. [...] Znajdują się tam reprezentanci każdej specjalności szpiegowskiego rzemiosła; szpiedzy kłębią się przede wszystkim [...] w salonach i na koktajlach oraz wszędzie tam, gdzie można spotkać wpływowe towarzystwo. Hazardziści i szarlatani próbują na własną rękę handlować pożądanym towarem, jakim jest informacja, co prowadzi do ich szybkiego zdemaskowania. Innych boją się nawet starzy wywiadowczy wyjadacze: tych mianowicie, którzy pracują na dwa lub więcej frontów, to znaczy jako podwójni agenci sprzedający swą wiedzę i przyjaciołom, i wrogom. Jeszcze inni wraz ze zmianami sytuacji na frontach cichej wojny zmieniają też barwy” (Kaltefleiter, Oschwald 2007, s. 50).

Globalna wojna informacyjna jest środowiskiem, które jest i producentem, i odbiorcą znacznych ilości informacji. „Ich zdobywaniem, przetwarzaniem i dystrybucją zajmują się wyspecjalizowane elementy struktury systemu rozpoznawczego, do którego zalicza się wywiad i kontrwywiad (cywilny i wojskowy). Służby tego charakteru są silnym orężem w kooperacji negatywnej. Z uwagi na posiadane uprawnienia, w jakie wyposażył je ustawodawca, posiadają możliwości zdobywania informacji (w tym charakteru niejawnego) w kraju i poza jego granicami, w sposób jawny i tajny” (Żebrowski 2005, s. 76). Służby specjalne w coraz większym stopniu

wykorzystują globalną przestrzeń informacyjną i inne technologie służące planowaniu, wspieraniu i prowadzeniu działalności wywiadowczej i kontrwywiadowczej. Penetracja Internetu pozwala m.in. na poznanie sfer zainteresowania przeciwnika, a także technik, jakimi się on posługuje. Wzrost umiejętności strony ofensywnej niesie ze sobą korzyści pozwalające na zachowanie bezpieczeństwa państwa, poznanie form i metod działania przeciwnika, zaangażowanych sił i środków, a także zaoszczędzenie znacznych aktywów finansowych. Obok penetracji technicznej przestrzeni informacyjnej aktywność służb ma miejsce także w osobowej przestrzeni informacyjnej, która szczególnie narażona jest na zagrożenia z ich strony (zob. rys. 20.1).



Rysunek 20.1. Zagrożenia ze strony obcych służb specjalnych

Źródło: (Libera 2007, s. 186)

Systemy informacyjne i teleinformatyczne wykorzystywane przez służby specjalne traktowane są jako infrastruktura krytyczna, która stanowi kluczowy element systemu bezpieczeństwa państwa. Jest ona bogatym źródłem informacji znajdujących się w zainteresowaniu służb specjalnych. Warto mieć świadomość tego, że w trakcie penetracji technicznej przestrzeni informacyjnej wywiadu i kontrwywiadu, przeciwnik prowadzi zakłócanie informacyjne. Obejmuje ono wszystkie poziomy działań na informacjach, tzn. zdobywanie, przetwarzanie (działalność analityczno-studyjną), przechowywanie i przesyłanie. Oznacza to, że zakłócanie obejmuje zarówno penetrację bierną, jak i czynną.

Penetracja bierna stanowi zagrożenie dla poufności zasobów informacyjnych. Dotyczy dostępu przeciwnika do danych, a w sieciach komputerowych do monitorowania ich przepływu lub ustalenia struktury sieci. Penetracja bierna może być prowadzona w formie (Janczak 2001, s. 137-139):

- przeglądania – polega na przeszukiwaniu sieci komputerowej w celu pozyskania danych;
- przenikania – dotyczy przepływu danych do nieuprawnionych użytkowników;
- wnioskowania – dotyczy procesów ustalenia danych niejawnych na podstawie ogólnie dostępnych lub jawnych informacji.

Penetracja aktywna zagraża autentyczności znajdujących się tam danych. Dotyczy ochrony własnych zbiorów lub strumieni danych przed rozmyślnym ich modyfikowaniem przez przeciwnika. Przy zakłócaniu penetracji aktywnej należy uwzględnić (Janczak 2001, s. 137-139):

- zniekształcanie (modyfikowanie) danych;
- podszywanie, które jest odpowiednikiem dywersyjnych działań dezinformacyjnych w kanałach łączności;
- niszczenie danych – dotyczy zamierzonego zamazania lub usunięcia części lub całych plików lub programów.

Zakłócanie rozpoznania informatycznego będzie polegało m.in. na:

- ataku fizycznym mającym na celu niszczenie infrastruktury zasadniczej (komputery, bazy danych, oprogramowanie, środki łączności, układy sterowania i monitorowania) oraz infrastruktury pomocniczej (budynki, urządzenia sterowania zasilaniem, klimatyzacją itp.), a także fizycznym ataku na personel obsługujący urządzenia;
- ataku za pośrednictwem programu komputerowego na elementy infrastruktury teleinformatycznej, komputery sterujące pracą innych urządzeń, zbiory danych (niszczenie lub ograniczenie dostępu).

Szczególnym obszarem zainteresowania przeciwnika jest niewątpliwie zakłócanie działalności analityczno-studyjnej. Jego następstwem jest błędna prognoza zagrożenia (zagrożeń) przedstawiana uprawnionym podmiotom cywilnym i wojskowym właściwym sferze bezpieczeństwa państwa. Tego rodzaju działalność ma negatywny wpływ na przetwarzanie danych przez obiekt znajdujący się w zainteresowaniu służb (obiekt ataku) oraz wytwarzanie informacji przydatnych w procesie przygotowania i prowadzenia działań w sferze zarówno militarnej, jak i pozamilitarnej. W związku z tym zakłócanie rozpoznania studyjnego ma dwoisty charakter: z jednej strony dezorganizuje proces zasilania komórki analityczno-studyjnej w dane rozpoznawcze, z drugiej utrudnia funkcjonowanie ogniw rozpoznania danego szczebla organizacyjnego (personel, osoby funkcyjne) (Janczak 2001, s. 150-151).

Należy zaznaczyć, że zasoby informacyjne wywiadu i kontrwywiadu zawsze znajdują się w zainteresowaniu uczestników konfliktu, dlatego służby specjalne obcego państwa będą dążyły do ich penetracji, modyfikacji lub zniszczenia. Służby specjalne w procesie wykonywania swoich ustawowych zadań będą m.in. podejmowały działania ukierunkowane na konkretny obiekt zainteresowania operacyjnego, mające na celu w szczególności:

- prowokowanie uczestnika (uczestników) kooperacji negatywnej do podejmowania działań, które w istocie będą dla niego niekorzystne – zarówno w sferze militarnej, jak i pozamilitarnej;
- przeciążanie grup analizy danych uczestnika (uczestników) kooperacji negatywnej nadmiarem bezwartościowych danych;
- sugerowanie uczestnikowi (uczestnikom) kooperacji negatywnej określonych wzorców zdarzeń, które powodować będą małą skuteczność ich działania;
- obniżenie zdolności bojowej uczestnika (uczestników) kooperacji negatywnej na skutek występowania opóźnień lub podejmowania niewłaściwych działań.

Niebezpieczeństwo tych działań polega m.in. na tym, że uczestnik (uczestnicy) kooperacji negatywnej (Janczak 2001, s. 152-153):

- nie będzie w stanie odróżnić danych prawdziwych od fałszywych;
- po analizie sytuacji oceni działania mylące jako prawdziwe;
- podejmie działania przeciwko pozorowanym celom i sytuacjom.

Zagrożenia ze strony obcych służb specjalnych dla bezpieczeństwa wywiadu i kontrwywiadu państwa zainteresowania są wielopłaszczyznowe i dotyczą niemal każdej sfery ich działalności, przy czym jedne kierunki są dominujące, a inne marginalizowane jako niemające istotnego wpływu na poziom bezpieczeństwa własnego i państwa, co jednak nie oznacza, że w określonych warunkach nie znajdują się w sferze zainteresowania wywiadu i/lub kontrwywiadu. Szczególne zagrożenie dla służb specjalnych stanowi jednak agentura, która z uwagi na posiadane możliwości dotarcia do informacji znajdujących się w operacyjnym zainteresowaniu służb przeciwnika, przez swoją aktywność narusza ich system bezpieczeństwa wewnętrznego. Rozpoznanie agenturalne jest jednym z najstarszych, a jednocześnie najtrudniejszym rodzajem zdobywania informacji. Agentura stanowi podstawowy środek pracy służb specjalnych, których zadaniem jest zdobywanie informacji o przeciwniku drogą ściśle zakonspirowanych operacji wywiadowczych i kontrwywiadowczych. W ramach prowadzonych działań operacyjno-rozpoznawczych, służby każdego państwa dążą do umieszczenia w strukturach służb specjalnych swojej agentury, co stanowi naturalne warunki do nawiązania bezpośredniego kontaktu ze służbami państwa zainteresowania i podjęcia gry wywiadowczej/kontr-wywiadowczej.

Służby specjalne z uwagi na swój charakter, wykonywane zadania w kraju i poza jego granicami, posiadane uprawnienia (w tym do wykonywania czynności operacyjno-rozpoznawczych), ze szczególnym wskazaniem na anonimowość, wielość obiektów rozpoznawanych, wykorzystywanie nowoczesnych technik teleinformatycznych i komunikacyjnych, Internetu (gdzie brak przestrzennych granic, brak politycznych granic, brak geograficznych granic, brak doraźnych granic, proste technologie, niejasne prawo, niejasna odpowiedzialność, słabo określone przedsięwzięcia zaradcze, akt kryminalny, akt wojny (Szpyra 2003, s. 91)) – czynią je szczególnie niebezpiecznymi. Na tym tle wyróżnia się praca operacyjna jako szczególna aktywność uprawnionych pracowników wywiadu i kontrwywiadu, opatrzona najwyższymi klauzulami niejawności praktycznie w każdym państwie. Stanowi ona zagrożenie z uwagi na realizowane cele, polegające na (Larecki 2017, s. 667-668):

- 1) uzyskiwaniu informacji będących przedmiotem zainteresowania służb specjalnych;
- 2) rozpoznawanie i rozpracowywanie osób, organizacji lub instytucji pod kątem ich dalszego operacyjnego wykorzystania (przy działaniach wywiadowczych) lub ujawnienia, rozpoznania i zneutralizowania ich wrogiej działalności (przy działaniach kontrwywiadowczych);
- 3) dokumentowanie badanych faktów do dalszego operacyjnego lub procesowego ich wykorzystania.

Różnorodność metod operacyjnych i ich ochrona to czynniki stanowiące zagrożenie nie tylko dla samych służb, ale także dla kierunków zainteresowania operacyjnego i pracy operacyjnej. Czynności wymienione w tabeli 20.1 pozwalają służbom specjalnym na dostęp do wiedzy prawnie chronionej, co już stanowi zagrożenie dla podmiotów będących jej dysponentami.

Tabela 20.1. Metody pracy operacyjnej

METODY PRACY OPERACYJNEJ	
POZNAWCZE	MANIPULACYJNE
<ul style="list-style-type: none"> – współpraca z osobami (z osobowymi źródłami informacji) – wywiad – rozmowa operacyjna – sondaż kapturowy – wywiad środowiskowy – ustalenie – penetracja terenu – eksperyment operacyjny – analiza operacyjna – inwigilacja operacyjna – zakup kontrolowany – przesyłka niejawnie kontrolowana – kontrola operacyjna (kontrolowanie treści korespondencji, kontrolowanie treści przesyłek, stosowanie środków technicznych umożliwiających uzyskiwanie w sposób niejawnie informacji i dowodów oraz ich utrwalanie — w szczególności obrazu, treści rozmów telefonicznych i innych informacji przekazywanych przy pomocy sieci telekomunikacyjnych) – tajne przeszukanie – tajne otwarcie zamka (zamek) – tajne zatrzymanie – penetracja technicznej przestrzeni informacyjnej (cyberprzestrzeni) 	<ul style="list-style-type: none"> – rozmowa operacyjna – legendowanie – przykrycie – legalizowanie – zasadzka – inspiracja operacyjna – dezinformacja operacyjna – dezintegracja operacyjna
	KOMPLEKSOWE
	<ul style="list-style-type: none"> – kombinacja operacyjna – gra operacyjna – operacja specjalna – penetracja technicznej przestrzeni informacyjnej (cyberprzestrzeni)

Źródło: opracowanie własne na podstawie dostępnej literatury

Z uwagi na to, że służby specjalne walczą na niejawnym froncie, praca operacyjna zawsze jest prowadzona w warunkach ryzyka. Ryzyko działania służb wywiadu i kontrwywiadu można rozpatrywać na trzech płaszczyznach:

- 1) ryzyko związane z prowadzeniem rozpoznania obszarów zainteresowania w kraju i poza jego granicami;
- 2) ryzyko prowadzenia działalności wywiadowczej i kontrwywiadowczej (gry operacyjne);
- 3) ryzyko związane z barierami wyjścia służb z prowadzonej gry wywiadowczej/kontrwywiadowczej.

Dla współczesnych służb specjalnych szczególnym rodzajem zagrożenia jest jednak globalna wojna informacyjna, w której wykorzystywane i modernizowane są metody pracy operacyjnej wspieranej przez naukę i nowoczesne technologie produkcji. Ma to istotne znaczenie dla bezpieczeństwa państwa (państw), które od końca 2019 roku realizują swoje funkcje wobec pandemii COVID-19. W ten scenariusz wpisują się także służby specjalne wszystkich państw, dla których jest to wyzwanie, gdzie dominują jednak zagrożenia spowodowane wspomnianą pandemią, ale także koniecznością dostosowania się do jakościowo nowego środowiska wewnętrznego i zewnętrznego w skali globalnej.

System ochrony

Potencjał operacyjny, zasoby informacyjne (bazy danych), kierunki zainteresowania operacyjnego, zadania i ich charakter, kadrowi pracownicy, a przede wszystkim osobowe źródła informacji sprawiają, że służby specjalne stanowią atrakcyjny obiekt zainteresowania przeciwnika i czyni je podatnymi na atak w osobowej i technicznej przestrzeni informacyjnej.

Służby specjalne penetrujące osobowe i techniczne przestrzenie informacyjne zawsze są narażone na atak informacyjny przeciwnika (obecne służby specjalne, organizacje terrorystyczne, zorganizowane grupy przestępcze o charakterze transnarodowym), gdyż zdobywanie i zakłócanie informacji to kluczowe elementy aktywności informacyjnej służb specjalnych każdego państwa. Te złożone warunki, ewoluujące w globalnej przestrzeni bezpieczeństwa międzynarodowego, sprawiają, że służby specjalne (każda w zakresie swojej właściwości) muszą wypracować i wdrażać politykę bezpieczeństwa własnej infrastruktury (w tym i informacyjnej). Infrastruktura ta traktowana jest jako element infrastruktury krytycznej państwa, co wymaga szczególnej ochrony.

Służby specjalne w procesie budowania własnego systemu bezpieczeństwa muszą uwzględniać procesy zachodzące w otoczeniu zewnętrznym (bliższym i dalszym) i wewnętrznym państwa. Uwzględniając wykonywane zadania, muszą posiadać rozbudowany system alarmowania i powiadamiania, gdzie tzw. agentura ostrzegająca sygnalizuje oznaki niebezpieczeństwa dla realizacji zadań wywiadowczych i/lub kontrwywiadowczych w środowisku działania, a także dla rozbudowanej własnej infrastruktury. Sygnały powiadamiania i alarmowania obok agentury mogą być pozyskiwane w trakcie penetracji technicznej przestrzeni informacyjnej. Należy także mieć na uwadze oficjalne (półoficjalne) kontakty kadrowych pracowników służb specjalnych i agentury z przedstawicielami środowisk znajdujących się w ich operacyjnym zainteresowaniu w kraju i poza jego granicami. Tym bardziej, że wielu pracowników służb specjalnych realizuje swoje zadania na niejawnych etatach

(głęboko zakonspirowanych), co pozwala im na swobodne poruszanie się w środowiskach zainteresowania operacyjnego.

Bezpieczeństwo służb specjalnych jest złożonym procesem, a do aktywności w tej sferze zobowiązanych jest wiele podmiotów, w tym władzy ustawodawczej, wykonawczej i sądowniczej. Każdy z nich podejmuje tę aktywność w zakresie swojej właściwości:

- 1) władza ustawodawcza:
 - funkcja ustawodawcza i kontrolna Sejmu;
- 2) władza wykonawcza:
 - zapewnia wykonanie ustaw m.in. dotyczących działalności służb specjalnych;
 - wydaje rozporządzenia m.in. dotyczących działalności służb specjalnych;
 - uchwała projekt budżetu państwa, w tym działu dotyczącego działalności służb specjalnych (np. wielkość funduszu operacyjnego);
 - zapewnia bezpieczeństwo wewnętrzne i zewnętrzne państwa;
 - sprawuje ogólne kierownictwo w dziedzinie obronności kraju;
 - sprawuje ogólne kierownictwo w dziedzinie stosunków z innymi państwami i organizacjami międzynarodowymi.
- 3) władza sądownicza zapewnia ochronę prawną, dzięki obowiązującym przepisom prawa.

Obowiązujące regulacje prawne, istniejące struktury organizacyjne (w tym wyspecjalizowane komórki bezpieczeństwa wewnętrznego), przestrzeganie zasad ograniczonego zaufania i ograniczonego dostępu, przyjęta i ewoluująca polityka bezpieczeństwa informacyjnego, polityka doboru kwalifikowanego, postępowania sprawdzające, system monitoringu, system powiadamiania i alarmowania, system szkolenia oraz przyjęte rozwiązania bezpieczeństwa w osobowej i technicznej przestrzeni informacyjnej pozwalają na stworzenie skutecznej bariery dostępu dla nieuprawnionych podmiotów (w tym i obcych służb specjalnych). Obowiązujące rozwiązania muszą być monitorowane i modyfikowane pod kątem uwzględniania wszelkich procesów mających wpływ na poziom bezpieczeństwa infrastruktury krytycznej służb wywiadu i kontrwywiadu.

Kluczowym elementem jest zabezpieczenie służb przed niekontrolowanym ulotem informacji (i kontrolowanym przez służby specjalne obcego państwa), zarówno w osobowej, jak i technicznej przestrzeni informacyjnej. Do środków bezpieczeństwa (oprócz postępowań sprawdzających) zalicza się ochronę sieci i systemów informacyjnych i teleinformatycznych, zabezpieczenie pomieszczeń przed podsłuchem i podglądem, ochronę kadrowych pracowników (i ich rodzin), a także wiele innych przedsięwzięć o charakterze kontrwywiadowczym.

Jednym z celów polityki bezpieczeństwa informacyjnego jest także wprowadzenie przeciwnika w błąd poprzez dezinformację, manipulację, kłamstwo, maskowanie (w tym i elektroniczne) czy dezintegrację, realizowane w ramach zakłócających ofensywnych operacji informacyjnych. Przedsięwzięcia pasywne mają na celu ukrycie obiektów, instalacji, jednostek wywiadu i kontrwywiadu (cywilnego i wojskowego), ich zamiarów i planów, kierunków zainteresowania operacyjnego,

prowadzonej pracy operacyjnej, stosowanych form i metod (ofensywnych i defensywnych), agentury poprzez maskowanie operacyjne i techniczne.

Zdobywanie i ochrona informacji znajdujących się w zainteresowaniu służb wywiadu i kontrwywiadu zarówno w działaniach ofensywnych, jak i defensywnych ma kluczowe znaczenie dla zarządzania bezpieczeństwem służb i państwa. Pozwala to na wyciągnięcie następujących wniosków (Band 1993a, s. 66; Band 1993b, s. 114):

- jeżeli punkt ciężkości jest przesunięty w stronę defensywy, to wzrasta na znaczeniu zdobywanie informacji (tym samym służb wywiadu);
- jeżeli punkt ciężkości jest przesunięty w stronę ofensywy, to wzrasta rola bezpieczeństwa (czyli służb kontrwywiadu).

W polityce bezpieczeństwa informacyjnego służby muszą przestrzegać ściśle określonych i współzależnych zasad, m. in.:

- pokonywać bariery związane z procesem uczenia się,
- zarządzać procesem pozyskiwania niezbędnej wiedzy i jej udostępnianie uprawnionym podmiotom politycznym i wojskowym;
- prognozować rozwój potencjału operacyjnego dla skutecznego działania;
- efektywnie zarządzać zmianami w służbach, co wymaga przemyślanego stymulowania procesów przekształceń, wynikających ze świadomego dążenia do zwiększania lub też zachowania na niezmiennym poziomie możliwości realizacji powierzonych zadań.

Bezpieczeństwo służb specjalnych to także działania ofensywne, przybierające postać gry (wywiadowczej/kontrwywiadowczej), to pewne reguły postępowania, dzięki którym kierownictwo służb, poszczególnych pionów funkcjonalnych i komórek organizacyjnych posiada możliwości wyboru i podejmowania określonych działań, co pozwala na zwiększenie prawdopodobieństwa na realizację przyjętych celów przy jednoczesnej minimalizacji niepewności (z którą *de facto* muszą się liczyć). Aby taka gra mogła pozwolić na osiągnięcie założonych celów, podejmujący ją powinni dążyć do poszukiwania odpowiedzi na pytania dotyczące czynników obiektywnych i subiektywnych tak, aby nie były one oderwane od rzeczywistości i dających się przewidzieć zdarzeń, zjawisk i procesów mających wpływ na poziom bezpieczeństwa państwa i zadania wykonywane przez wywiad i kontrwywiad.

Przy poszukiwaniu odpowiedzi na te pytania służby specjalne muszą rozpoznawać środowisko bezpieczeństwa państwa, ale i własne, wskazywać i identyfikować źródła zagrożeń i niepewności. Ważna umiejętność to dostrzeganie słabych i mocnych sygnałów, aby radzić sobie z jakościowo nowymi problemami. Ich rozwiązywanie wiąże się niejednokrotnie z koniecznością dostosowania się do nowych warunków, co pozwala niekiedy na zbudowanie pod względem jakościowym i ilościowym innej służby wywiadu i kontrwywiadu.

Warto mieć na uwadze to, że trwająca wojna informacyjna jest podstawowym, a jednocześnie szczególnym przypadkiem działania służb wywiadu i kontrwywiadu, które są jej aktywnymi uczestnikami. Celem tej walki, obok zdobywania i ochrony własnego potencjału, jest neutralizowanie lub fizyczna destrukcja przeciwnika przy użyciu informacji. Informacja, jako narzędzie wojny informacyjnej, spełnia różne funkcje:

- osłabia potencjał przeciwnika w procesie przekazywania informacji w relacji jego komórki decyzyjnej i wykonawcy;
- wprowadza do systemów informacyjno-sterujących przeciwnika błędne algorytmy decyzyjne, a niekiedy i analogiczne algorytmy działania, które go osłabiają, a w pewnych sytuacjach prowadzą do samozniszczenia.

Służby specjalne w obronie informacyjnej muszą wykorzystywać elementy właściwe propagandzie. Skuteczną metodą dywersji jest inspirowanie przeciwnika do podejmowania błędnych decyzji przy jednoczesnym wykorzystywaniu ich wyników. Stanowi to specyficzny rodzaj manipulacji, której istota polega na ukrytym sterowaniu przeciwnikiem w celu samodestrukcji.

Obrona służb specjalnych to także, a może przede wszystkim, przejęcie kontroli nad torami informacyjnymi obcych służb specjalnych. Zwalczenie wywiadu, kontrwywiadu i sił specjalnych przeciwnika, terrorystów i innych form przestępczości zorganizowanej poprzedzone powinno być rozpoznaniem ich kanałów informacyjnych, co niekiedy jest niezmiernie trudne. Kanały przepływu informacji mogą być rozpoznawane w trakcie penetracji osobowej i technicznej przestrzeni informacyjnej przeciwnika oraz kontroli systemu bezpieczeństwa wewnętrznego własnych służb bezpieczeństwa. Odpowiednio uplasowana agentura stanowi zasadniczy element systemu powiadamiania i alarmowania. Niekiedy obserwacja uczestnicząca kadrowych pracowników służb specjalnych pozwala wychwycić sygnały będące zagrożeniami dla ich infrastruktury. Sygnalizować zagrożenia, ostrzegać w umówiony, ale niezauważalny dla przeciwnika sposób o wystąpieniu niekorzystnej sytuacji utrudniającej lub uniemożliwiającej realizację planowych czynności (np. spotkanie, błyskawiczne przekazanie materiałów) bądź obecność funkcjonariuszy obcych służb specjalnych (kocioł, zasadzka, dekonspiracja, praca pod kontrolą, obserwacja zewnętrzna) (Larecki 2017, s. 650).

Służby wywiadu i kontrwywiadu, uczestnicząc w totalnej wojnie informacyjnej, realizują przedsięwzięcia ochronno-obronne. Prowadzą aktywne operacje informacyjne ukierunkowane na neutralizację (w tym i fizyczną) podmiotów zagrażających niezakłóconemu funkcjonowaniu służb specjalnych. Na szczególną uwagę zasługuje bezpieczeństwo operacyjne, których zakłócanie przez przeciwnika prowadzi do naruszenia realizowanych funkcji przez służby wywiadu i kontrwywiadu. Bezpieczeństwo operacyjne to wszelkie środki podjęte dla ochrony przygotowywanych i realizowanych tajnych operacji przed ewentualną penetracją przeciwnika (Larecki 2017, s. 75). Z kolei bezpieczeństwo operacji to wszelkie działania ochronne, zabezpieczające i maskujące, które mają zagwarantować tajność zamierzeń, planów, przedsięwzięć, stosowanych technik i technologii, a w konsekwencji powodzenie i skuteczność podejmowanych operacji, oraz uniemożliwić jakkolwiek niejawną penetrację przez służby przeciwnika lub sprzymierzeńca (Larecki 2017, s. 75). Warto mieć na uwadze to, że bezpieczeństwo operacji zależy m.in. od bezpieczeństwa informacyjnego, bezpieczeństwa łączności, fizycznej ochrony funkcjonowania i kierowania (system przepustkowy), zabezpieczenia obiektów i kadry, ochrony przepływu dokumentów i informacji oraz dostępu do nich, działań o charakterze profilaktycznym (szkolenia, listy zagrożeń, kontrole) (Larecki 2017, s. 75). Bezpieczeństwo

informacyjne służb specjalnych stanowi element bezpieczeństwa państwa. Realizowany jest przez (Larecki 2017, s. 74):

- a) stosowanie różnego rodzaju działań zabezpieczających systemy komputerowe centrów decyzyjnych i obiektów strategicznych przed atakami sieciowymi hakerów amatorów lub profesjonalistów, działających na zlecenie organów państw wrogich bądź organizacji terrorystycznych, poprzez:
 - fizyczną i osobową ochronę miejsc ich dyslokacji, dokumentów i osób przed możliwymi zagrożeniami (szpiegostwo, atak terrorystyczny),
 - bezpieczeństwo łączności,
 - różne sposoby maskowania i minimalizowania możliwości rozpoznania,
 - systemy antypodsłuchowe,
 - szkolenia personelu i kształtowanie właściwych zachowań;
- b) wykazywanie i likwidację działań obcych służb specjalnych:
 - paraliżowanie działań obcego aparatu zdobywającego przez aktywne i skuteczne przeciwdziałanie kontrwywiadu wewnętrznego i kontrwywiadu ofensywnego;
- c) różnego rodzaju działania mylące (osłonowe, maskujące):
 - wykorzystywanie agentów podwójnych,
 - przekazywanie obcym służbom materiałów dezinformujących.

Bezpieczeństwo łączności służb specjalnych to systemy i procedury ochrony łączności używane przez służby wywiadu i kontrwywiadu w danym państwie. Mają one uniemożliwić osobom niepowołanym dostęp (przechwytywanie emisji, analizę ruchu w sieciach łączności) do informacji przekazywanych przy jej wykorzystaniu. Stosowane systemy i procedury obejmują takie elementy jak: stosowanie metod steganograficznych, ochronę kryptograficzną, bezpieczeństwo transmisji, elektroniczną kontrolę funkcjonowania łączności, stosowanie kontrprzeciwdziałania radioelektronicznego, zabezpieczenie fizyczne sprzętu wykorzystywanego do przekazywania informacji danych (Larecki 2017, s. 75).

Globalna przestrzeń bezpieczeństwa sprawia, że konfrontacja na niejawnym froncie to stały element działalności służb wywiadu i kontrwywiadu. Oznacza to, że aktywność informacyjna towarzyszy jej uczestnikom na każdym etapie prowadzonej walki. Szczególną rolę przypisuje się działaniom o charakterze kontrwywiadowczym, które w przedsięwzięciach defensywnych zajmują kluczową pozycję. Procesowi zwalczania i rozpoznawania przeciwnika muszą towarzyszyć ofensywne operacje informacyjne, ukierunkowane na neutralizację przeciwnika. Powinny to być działania wyprzedzające, co pozwala na niedopuszczenie do ataku informacyjnego przeciwnika.

Bezpieczeństwo służb specjalnych to przede wszystkim działalność kontrwywiadowcza, która każdorazowo powinna być poprzedzona czynnościami określanymi jako cykl kontrwywiadowczy. Jest to zespół czynności, który obejmuje (Larecki 2017, s. 131):

- a) poszukiwanie sygnałów o obcej działalności szpiegowskiej za pomocą:
 - nasłuchów, RKW dla wychycenia nieznanych sygnałów transmisji radiowych, mogących stanowić środek łączności wywiadowczej przeciwnika;

- agenturalnej penetracji środowisk narażonych na zainteresowanie obcego wywiadu;
 - informacji od własnej agentury działającej wewnątrz lub na styku z obcymi służbami specjalnymi;
 - danych z zabezpieczonych obiektów ochraniających kontrwywiadowczo;
 - selekcyjnej kontroli korespondencji w poszukiwaniu, np. tajnopisu;
 - danych uzyskanych w ramach współpracy od służby zaprzyjaźnionych;
 - przypadkowych informacji (zgłoszenia z instytucji, od obywateli, inne sygnały);
- b) weryfikacja uzyskanych informacji i materiałów, które potwierdzają fakt obcej działalności szpiegowskiej;
- c) wszczęcie rozpracowania operacyjnego celem ustalenia agenta obcego wywiadu i udokumentowania jego działań, które może być sfinalizowane w dwojaki sposób:
- przewerbowanie go na własnego agenta podwójnego;
 - kontynuowanie rozpracowania dla procesowego zebrania dowodów winy, aresztowanie szpiega i przekazanie sprawy sądowi.

Rozwój technik teleinformatycznych i komunikacyjnych sprawia, że ochrona przed penetracją osobowej i technicznej przestrzeni informacyjnej służb specjalnych jest niezmiernie trudna i wymaga złożonych przesiedzieć natury prawnej, organizacyjnej i technicznej. Tym działaniom muszą towarzyszyć przedsięwzięcia z zakresu zakłócenia informacyjnego i maskowania. Przeciwnik, prowadząc złożone i agresywne operacje informacyjne, będzie wykorzystywał najnowsze osiągnięcia naukowo-techniczne i technologiczne wspierające jego ofensywne działania. Analogiczne przedsięwzięcia powinny być podejmowane w procesie defensywnych operacji informacyjnych.

Podsumowanie

Służby wywiadu i kontrwywiadu stanowią podstawę aparatu zasilania w informacje uprawnionych użytkowników. Są to działania o charakterze wywiadowczym i kontrwywiadowczym realizowane w otoczeniu wewnętrznym i zewnętrznym państwa. Trwająca globalna wojna informacyjna stanowi szczególne wyzwanie dla państw i organizacji międzynarodowych właściwych w sferze bezpieczeństwa, w tym i dla służb specjalnych. Służby wykonujące swoje ustawowe zadania narażone są na wiele złożonych zagrożeń, pochodzących z otoczenia wewnętrznego i zewnętrznego państwa. Na szczególną uwagę zasługują zagrożenia celowe, których źródłem jest człowiek, w tym podmioty obcych państw, podmioty wewnętrzne naruszające porządek konstytucyjny państwa, organizacje przestępcze, państwa upadłe itp. Strategicznym celem wskazanych organizacji, służb i instytucji jest przejęcie kontroli nad zasobami informacyjnymi służb wywiadu i/lub kontrwywiadu państwa zainteresowania operacyjnego. Zagrożenie tego rodzaju zawsze towarzyszy służbom specjalnym w każdym państwie. Oznacza to, że na bezpieczeństwo służb składa się wiele złożonych i wzajemnie powiązanych przedsięwzięć prawno-organizacyjnych, ludzkich, finansowych i materiałowych, co powinno bezpośrednio przekładać się na

istniejący system ochrony. Ważna jest przyjęta i modyfikowana polityka bezpieczeństwa służb, która stanowi kluczowy element ich ochrony. Bezpieczeństwo służb to nie tylko wspomniane działania, ale także wsparcie ze strony legislatywy, egzekutywy i sądownictwa – jako elementu odstrasającego.

Literatura

1. Band J.F. (1993a), *Nachrichtendienste im Wandel*, „Allgemeine Schweizerische Militärschrift”, 2, s. 66-72.
2. Band J.F. (1993a), *Nachrichtendienste im Wandel*, „Allgemeine Schweizerische Militärschrift”, 3, s. 114-117.
3. Larecki J.H. (2017), *Wielki leksykon tajnych służb świata*, Oficyna Wydawnicza Rytm, Warszawa.
4. Janczak J. (2001), *Zakłócanie informacyjne*, Wydawnictwo AON, Warszawa.
5. Kaltefleiter W., Oschwald H. (2007), *Szpiedzy w Watykanie*, Wydawnictwo Wołoszański, Warszawa.
6. Libera B. (2007), *Zagrożenia ze strony obcych służb specjalnych*, [w:] Barcz J., Libera B. (red.), *Urzędnik i biznesmen w środowisku międzynarodowym*, s. 186-194, Wolters Kluwer, Kraków.
7. Malara Z. (2006), *Przedsiębiorstwo w globalnej gospodarce. Wyzwania współczesności*, Wydawnictwo Naukowe PWN, Warszawa.
8. Piekalkiewicz J. (1999), *Dzieje szpiegostwa*, Spółdzielnia Wydawnicza Czytelnik, Warszawa.
9. Szpyra R. (2003), *Militarne operacje informacyjne*, Wydawnictwo AON, Warszawa.
10. Żebrowski A. (2005), *Ewolucja Polskich służb specjalnych. Wybrane obszary walki informacyjnej (wywiad i kontrwywiad w latach 1989-2003)*, Abrys. Oficyna Wydawnicza, Kraków.

SECURITY OF SECRET SERVICE (SELECTED ASPECTS)

Abstract: Secret services, situated within the structure of the executive power, perform many complex intelligence and counterintelligence tasks. Due to their classified nature, the possessed operational potential allowing for the implementation of tasks in the internal and external environment of the state – are of interest to the opponent. The goal is to take over their information resources. Thus, the services are in the sphere of information activity of the internal and external opponent of the state. This activity is an information attack (information capture) and information disruption. These are comprehensive activities carried out in the personal and technical information space. They are supported by ICT, communication and the Internet, as well as modern production technologies. Secret services are active participants in the ongoing global information conflict, where they conduct offensive and defensive information operations on the covert front of the confrontation. The scale and dynamics of the processes taking place in the global security environment are evolving threats that engage special services to recognize them. Effective performance of tasks by intelligence/counterintelligence requires active defensive actions directed not only at the state, but also at its own critical infrastructure, including information resources.

Keywords: security, secret service, threats