e-ISSN 2451-0718
ISSN 1899-6264

Kwartalnik
Krakowskiej Akademii
im. Andrzeja Frycza Modrzewskiego

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA

PODNOSZENIE POZIOMU BEZPIECZEŃSTWA. METODY I NARZĘDZIA

redakcja
Andrzej Chodyński

numer 4 (XXXVII) Kraków 2019

Kwartalnik
Krakowskiej Akademii
im. Andrzeja Frycza Modrzewskiego

SECURITY
THEORY AND PRACTICE

IMPROVING THE LEVEL OF SECURITY: METHODS AND TOOLS

edited by
Andrzej Chodyński

number 4 (XXXVII), October–December, Krakow 2019

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA

PODNOSZENIE POZIOMU BEZPIECZEŃSTWA. METODY I NARZĘDZIA

redakcja
Andrzej Chodyński

numer 4 (XXXVII), październik–grudzień, Kraków 2019

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA
Kwartalnik
Krakowskiej Akademii
im. Andrzeja
Frycza Modrzewskiego

Adres redakcji
ul. Gustawa Herlinga-Grudzińskiego 1, A, pok. 219
30-705 Kraków
tel. (12) 25 24 666
e-mail: biuro@kte.pl
btip.ka.edu.pl

Czasopismo punktowane w rankingu Ministerstwa Nauki i Szkolnictwa Wyższego
oraz indeksowane w następujących bazach:
Repozytorium eRIKA. Repozytorium Instytucjonalne Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego;
PBN. Polska Bibliografia Naukowa; Index Copernicus; CEJSH. The Central European Journal of Social Sciences;
CEEOL. Central and Eastern European Online Library; BazHum

Czasopismo „Bezpieczeństwo. Teoria i Praktyka" uzyskało dofinansowanie Ministerstwa Nauki i Szkolnictwa Wyższego
w ramach programu „Wsparcie dla czasopism naukowych" (2019–2020)

e-ISSN 2451-0718
ISSN 1899-6264

Wersją pierwotną czasopisma jest wydanie elektroniczne.

Wszystkie numery kwartalnika „Bezpieczeństwo. Teoria i Praktyka" są dostępne w wolnym dostępie (open access).
btip.ka.edu.pl

Redakcja nie zwraca materiałów niezamówionych. Decyzja o opublikowaniu tekstu uzależniona jest od opinii redakcji i recenzentów. Redakcja zastrzega sobie prawo modyfikowania tytułów i skracania tekstów przeznaczonych do druku. Artykuły powinny być przesyłane w dwóch egzemplarzach wraz z wersją elektroniczną.

Na zlecenie
Krakowskiej Akademii
im. Andrzeja Frycza Modrzewskiego
www.ka.edu.pl

Wydawca
Oficyna Wydawnicza AFM
Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego,
Kraków 2019

Sprzedaż i prenumeratę prowadzi
e-mail: ksiegarnia@kte.pl

BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA

Spis treści

Andrzej Chodyński: Podnoszenie poziomu bezpieczeństwa. Metody i narzędzia. Wprowadzenie 13

ARTYKUŁY I MATERIAŁY

Janusz Ziarko: Podejście systemowe w badaniach bezpieczeństwa organizacji 19

Andrzej Chodyński: Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja *smart* 39

Andrzej Marjański, Jarosław Ropęga: Ochotnicze Straże Pożarne. Zapewnienie efektu synergii w zarządzaniu kryzysowym 63

Jowita Świerczyńska: The Role of Customs Clearance in Ensuring the Security and Protection of Cross-Border Trade in the European Union 83

Sylwia Zawadzka: System wjazdu i wyjazdu (EES) i Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS). Rola i znaczenie nowoczesnych systemów w zakresie działań prewencyjnych i wzmacniania bezpieczeństwa UE 103

Elżbieta Majchrowska: Asian Development Bank and its Impact on Improving Security in the Asia-Pacific Region 119

Mirosław Laszczak: Zarządzanie bezpieczeństwem w erze cyfrowej 135

Piotr Komsta: Koncepcja modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych a bezpieczeństwo procesów biznesowych przy realizacji projektów IT 151

Z KART HISTORII

Janusz Wojtycza: Krakowska Chorągiew Męska ZHP. Powstanie i początki działalności (1920–1921). Kalendarium wydarzeń 165

VARIA

Andrzej Krzak: Rosyjskie rozwinięcia teorii „małej wojny”. Wymiar historyczny i współczesny 183

RECENZJE

Anna Bałamut: *Energetyka – bezpieczeństwo w wyzwaniach badawczych*, red. Piotr Kwiatkiewicz, Radosław Szczerbowski, tom 1 203

Wojciech Huszlak: Adam Skrzypek, *Dojrzałość i doskonalenie organizacji* 209

KOMUNIKATY, SPRAWOZDANIA

Mirosław Kwieciński: III Multidyscyplinarne Autorskie Seminarium Naukowe *Modus Securitas* „Determinanty skuteczności zarządzania bezpieczeństwem państwa i biznesu – koncepcje, modele, podejścia, praktyka, wizje, wyniki badań”, Dwór Rychwałd, 22–23.09.2019 r. 219

Jadwiga Mazur: XXX Międzynarodowa Konferencja Naukowa „Socjologia grup dyspozycyjnych. Pomiędzy teorią nauk społecznych a praktyką”, Wrocław, 9–10.05.2019 r. 223

Mirosław Kwieciński: IX Konferencja Naukowa „Bezpieczeństwo i zarządzanie kryzysowe”, Społeczna Akademia Nauk w Łodzi, Łódź, 18–19.09.2019 r. 227

INFORMACJE DLA AUTORÓW

231

Lista recenzentów za rok 2019 237

SECURITY • THEORY AND PRACTICE 2019 No. 4

Contents

Andrzej Chodyński: Improving the Level of Security: Methods and Tools. Introduction 13

ARTICLES AND MATERIALS

Janusz Ziarko: System Approach in the Research into Organisational Security 19

Andrzej Chodyński: Taking Advantage of the Achievements of Management Sciences to Enhance City Security: The Smart Concept 39

Andrzej Marjański, Jarosław Ropęga: Volunteer Fire Departments and Ensuring the Synergy Effect in Crisis Management 63

Jowita Świerczyńska: The Role of Customs Clearance in Ensuring the Security and Protection of Cross-Border Trade in the European Union 83

Sylwia Zawadzka: Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS): The Role and Importance of Modern Systems in the Area of Preventive and Strengthening of EU Security 103

Elżbieta Majchrowska: Asian Development Bank and its Impact on Improving Security in the Asia-Pacific Region 119

Mirosław Laszczak: Security Management in the Digital Era 135

Piotr Komsta: The Concept of Dynamic Modeling of Implementation Processes of Integrated Systems and the Safety of Business Processes in Connection with the Implementation of the IT Project 151

FROM THE HISTORY

Janusz Wojtycza: Krakow Region Boys' Division of the Polish Scouting and Guiding Association: Timeline of the Origins and Early Days (1920–1921) 165

VARIA

Andrzej Krzak: The Russian Development of the "Small Wars" Theory: Historical and Contemporary Dimension 183

REVIEWS

Anna Bałamut: *Energetyka – bezpieczeństwo w wyzwaniach badawczych*, red. Piotr Kwiatkiewicz, Radosław Szczerbowski, tom 1 203

Wojciech Huszlak: Adam Skrzypek, *Dojrzałość i doskonalenie organizacji* 209

BULLETINS, REPORTS

Mirosław Kwieciński: Report on the session of the 3rd Multidisciplinary Academic Symposium Modus Securitas: The Determinants of the effective management of the security of the state and business: key concepts, models, approaches, practice, visions, research findings (held at Dwór Rychwałd from 22 to 23 September 2019) 219

Jadwiga Mazur: Report on the 30th International Academic Conference The Sociology of the Uniformed Public Services: between the theory of social sciences and practice (held in Wrocław from 9 to 10 May 2019) 223

Mirosław Kwieciński: Report on the 9th Academic Conference Security and Crisis Management: managing security at the local level (held in Łódź from 18 to 19 September 2019) 227

INFORMATION FOR AUTHORS

231

List of academic reviewers in 2019 237

SICHERHEIT • THEORIE UND PRAXIS 2019 Nr. 4

Inhaltsverzeichnis

Andrzej Chodyński: Verbesserung der Sicherheit. Methoden und Instrumente. Einführung 13

BEITRÄGE UND MATERIALIEN

Janusz Ziarko: Systematischer Ansatz in der Forschung der Organisationssicherheit 19

Andrzej Chodyński: Nutzung des Leistungen der Managementwissenschaften für die Verbesserung der Sicherheit der Städte. Smart – Konzept 39

Andrzej Marjański, Jarosław Ropęga: Freiwillige Feuerwehren und Gewährleistung der Synergieeffekte beim Krisenmanagement 63

Jowita Świerczyńska: Bedeutung der Zollabfertigung im Prozess der Sicherheits- und Schutzgewährleistung im grenzüberschreitenden Güterverkehr in der Europäischen Union 83

Sylwia Zawadzka: Europäisches Einreise-/ Ausreisesystem (EES) und Europäisches Reiseinformations- und Autorisierungssystem (ETIAS) – Rolle und Bedeutung der modernen Systeme im Bereich der Präventionsmaßnahmen und Verstärkung der EU-Sicherheit 103

Elżbieta Majchrowska: Die Asiatische Entwicklungsbank und ihr Einfluss auf die Verbesserung des Sicherheitsniveaus in der Asien-Pazifik-Region 119

Mirosław Laszczak: Sicherheitsmanagement im digitalen Zeitalter 135

Piotr Komsta: Das Konzept zur dynamischen Modellierung der Umsetzungsprozesse der integrierten Systeme und die Sicherheit der Geschäftsprozesse bei der Ausführung von IT-Projekten 151

AUS DER GESCHICHTE

Janusz Wojtycza: Das männliche Fähnlein des Polnischen Pfadfinderverbands in Kraków. Entstehung und Anfang der Tätigkeit (1920–1921). Wichtigste Ereignisse 165

VARIA

Andrzej Krzak: Russische Entwicklung der Theorie des „kleinen Krieges". Historische und moderne Dimension 183

REZENSIONEN

Anna Bałamut: *Energetyka – bezpieczeństwo w wyzwaniach badawczych*, red. Piotr Kwiatkiewicz, Radosław Szczerbowski, tom 1 203

Wojciech Huszlak: Adam Skrzypek, *Dojrzałość i doskonalenie organizacji* 209

MITTEILUNGEN, BERICHTE

Mirosław Kwieciński: Bericht über die Sitzung des III. Multidisziplinären Wissenschaftlichen Autorenseminars Modus Securitas zum Thema Determinanten der Effektivität beim Management von Staats- und Geschäftssicherheit – Konzepte, Modelle, Ansätze, Praxis, Visionen, Forschungsergebnisse (Dwór Rychwałd, 22.–23. September 2019) 219

Jadwiga Mazur: Bericht über die XXX. Internationale Wissenschaftliche Konferenz Soziologie der Zivilschutzmitarbeiter. Zwischen der Theorie der Sozialwissenschaften und der Praxis (Wrocław, 9.–10. Mai 2019) 223

Mirosław Kwieciński: Bericht über die IX. Wissenschaftliche Konferenz Sicherheit und Krisenmanagement. Sicherheitsmanagement auf lokaler Ebene (Łódź, 18.–19. September 2019) 227

INFORMATIONEN FÜR AUTOREN

231

Liste der Rezensenten für das Jahr 2019 237

БЕЗОПАСНОСТЬ • ТЕОРИЯ И ПРАКТИКА
2019 № 4

Содержание

Andrzej Chodyński: Повышение уровня безопасности. Методы и инструменты. Введение 13

СТАТЬИ И МАТЕРИАЛЫ

Janusz Ziarko: Системный подход в исследованиях безопасности организации 19

Andrzej Chodyński: Использования достижений наук об управлении в сфере повышения безопасности городов. Концепция smart 39

Andrzej Marjański, Jarosław Ropęga: Добровольная пожарная охрана. Обеспечение синергии в антикризисном управлении 63

Jowita Świerczyńska: Значение таможенного обслуживания в процессе обеспечения безопасности и защиты в трансграничном движении товаров в государствах Европейского Союза 83

Sylwia Zawadzka: Система въезда и выезда (EES) и Европейская система авторизации и информации о путешествии (ETIAS). Роль и значение современных систем в области профилактических действий и обеспечения безопасности ЕС 103

Elżbieta Majchrowska: Азиатский банк развития и его влияние на повышение уровня безопасности в Азиатско-Тихоокеанском регионе 119

Mirosław Laszczak: Управление безопасностью в эре цифровых технологий 135

Piotr Komsta: Концепция динамического моделирования процессов имплементации интегрированных систем и проблема безопасности бизнес-процессов при реализации ИТ-проектов 151

СТРАНИЦЫ ИСТОРИИ

Janusz Wojtycza: Краковская мужская хоругвь Союза польских харцеров. Создание и начало деятельности (1920–1921). Календарь событий 165

ВАРИА

Andrzej Krzak: Российские разработки теории «малой войны». Исторический и современный аспекты 183

РЕЦЕНЗИИ

Anna Bałamut: *Energetyka – bezpieczeństwo w wyzwaniach badawczych*, red. Piotr Kwiatkiewicz, Radosław Szczerbowski, tom 1 203

Wojciech Huszlak: Adam Skrzypek, *Dojrzałość i doskonalenie organizacji* 209

СООБЩЕНИЯ, ОТЧЕТЫ

Mirosław Kwieciński: III Междисциплинарный авторский научный семинар Modus Securitas «Детерминанты эффективности управления безопасностью государства и бизнеса – концепции, модели, подходы, практика, восприятие, результаты исследований», Двур Рихвалд, 22–23.09.2019 г. 219

Jadwiga Mazur: XXX Международная научная конференция «Социология военизированных организаций. Между теорией социальных наук и практикой», Вроцлав, 9–10.05.2019 г. 223

Mirosław Kwieciński: IX научная конференция «Безопасность и кризисное управление», Общественная академия наук в Лодзи, Лодзь, 18–19.09.2019 г. 227

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

231

Список рецензентов за 2019 год 237

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-000

Andrzej Chodyński

prof. dr hab., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0003-4962-5143

Podnoszenie poziomu bezpieczeństwa. Metody i narzędzia. Wprowadzenie

Nauki o bezpieczeństwie oraz nauki o zarządzaniu i jakości jako dyscypliny naukowe wchodzą w skład dziedziny nauk społecznych[1]. Obiektem i przedmiotem badań w naukach społecznych jest rzeczywistość społeczna, na którą składają się: zbiorowości i zbiory społeczne, instytucje społeczne, a także procesy oraz zjawiska społeczne[2]. Występuje przy tym heterogeniczność obiektu badań, co wymaga stosowania różnorodnych narzędzi badawczych, metod i technik – często pochodzących z innych dyscyplin naukowych, spoza dziedziny nauk społecznych[3]. Jednym z celów badań dotyczących bezpieczeństwa może być podniesienie jego poziomu, także z wykorzystaniem dorobku nauk o zarządzaniu. Należy brać pod uwagę zróżnicowane rozumienie pojęcia „bezpieczeństwo"[4] i fakt, że termin ten jest obecnie dyskutowany[5].

Nauki o bezpieczeństwie charakteryzują się eklektyzmem metodologicznym – nie dopracowały się własnej metodologii, więc wykorzystują dorobek innych dyscyplin naukowych. Metodologia w naukach społecznych to zestaw dyrektyw badawczych, opartych na przyjętych założeniach teoretycznych, a także sposoby formułowania, uzasadniania i sprawdzania twierdzeń. Dotyczy to m.in. takich zabiegów poznawczych

1 Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych, Dz.U. z 2018 r., poz. 1818.

2 J. Sztumski, *Wstęp do metod i technik badań społecznych*, Katowice 2005.

3 A. Czupryński, *Naukowe aspekty bezpieczeństwa*, [w:] *Bezpieczeństwo. Teoria – badania – praktyka*, red. A. Czupryński, B. Wiśniewski, J. Zboina, Józefów 2015, s. 35–47.

4 A. Chodyński, *Nauki o bezpieczeństwie a nauki o zarządzaniu – paradygmaty i tożsamość*, „Bezpieczeństwo. Teoria i Praktyka" 2013, nr 2, s. 7–18.

5 M. Banasik, *Dilemmas of Security Perception*, „Scientific Journal of the Military University of Land Forces" 2018, vol. 50, nr 3 (189), s. 5–15.

jak stawianie i rozwiązywanie problemów, formułowanie zjawisk, ich opis i wyjaśnianie, prowadzenie badań, uzasadnianie twierdzeń oraz sposobów wnioskowania. W ramach zabiegów poznawczych w naukach o bezpieczeństwie następuje sformułowanie pytań badawczych, hipotez i twierdzeń o uwarunkowaniach procesu bezpieczeństwa, wypracowanie narzędzi badawczych, budowa modeli i teorii oraz tworzenie systemu organizacji badań naukowych, ich prowadzenia i kontroli. Narzędzia badawcze odnoszą się do rozpoznania zagrożeń i przeciwdziałania im, ale także (wraz z wypracowanymi metodami) – do systematycznego kumulowania wiedzy i rozwiązań praktycznych dotyczących bezpieczeństwa. Nauki o bezpieczeństwie jako dyscyplina naukowa w ramach nauk społecznych wykorzystują metody badań empirycznych. W przypadku trudności w sformułowaniu hipotez badawczych, w ich miejsce formułuje się pytania badawcze. Doświadczalną weryfikację hipotez badawczych cechuje postępowanie empiryczne, wykorzystujące najczęściej logikę indukcji, dopuszczalne jest wykorzystywanie logiki formalnej, rzadko – teorii dedukcji. Najbardziej reprezentatywne cechy przedmiotu badań ustala się za pomocą metod i technik badawczych. Rozumowanie indukcyjne zakłada cel w postaci uogólnień. Etapem wstępnym indukcji jest przedstawienie hipotezy. Najogólniejszymi metodami przetwarzania materiału badawczego w naukach społecznych są analiza i synteza, jako składniki szczegółowych metod i technik badawczych. Metoda analizy prowadzi do opracowania metodyki, dla uzyskania informacji o składzie badanej próby.

Przedmiotem badań nauk o bezpieczeństwie są systemy bezpieczeństwa – systemy są także przedmiotem badań nauk o zarządzaniu[6]. Julia Karcz zwraca uwagę, że podejście systemowe wiąże się z podejściem holistycznym do organizacji. Organizacja w tym przypadku jest traktowana jako system społeczno-techniczny (np. model Harolda Leavitta). Uwagę poświęca się analizie systemowej (i jej procedurom) – punkt wyjścia stanowi sytuacja problemowa; rozważania dotyczą dynamiki systemów – podstawą jest sieć relacji odnosząca się do zależności w systemie. Myślenie systemowe wiąże się z myśleniem sieciowym (strukturalnym). Archetyp systemowy stanowią powtarzalne wzorce zachowań systemu. Jako wady podejścia systemowego wymienia się marginalizację roli czynnika ludzkiego i brak uwzględnienia ekstremalnych stanów otoczenia (choć prawdopodobieństwo ich wystąpienia jest niewielkie). Niska jest użyteczność tego podejścia w warunkach znacznej niepewności (np. kryzysu).

Na bazie szkoły systemowej powstało podejście sytuacyjne. Jego głównym założeniem jest relatywizm i pragmatyzm. Jest to podejście ważne dla działań w otoczeniu turbulentnym (niestabilnym, wysoce zmiennym i niejednolitym). Interakcje z otoczeniem mają charakter zróżnicowany, wpływa na nie typ działalności i stosowana technologia. Zrozumienie sytuacji, w jakiej znajduje się organizacja, polega na zidentyfikowaniu cech relacji organizacji z otoczeniem zewnętrznym – ale także pomiędzy jej wewnętrznymi systemami. Metody zarządzania w podejściu sytuacyjnym są dobierane stosownie do zaistniałej sytuacji. Podejście sytuacyjne niweluje pewne słabości koncepcji systemowej[7]. Podejście systemowe może być odnoszone do wybranych

[6] B. Kuc, Z. Ścibiorek, *Zarys metodologii nauk o bezpieczeństwie*, Toruń 2018.

[7] J. Karcz, *Organizacja jako system*, [w:] *Zarządzanie, organizacje i organizowanie. Przegląd perspektyw teoretycznych*, red. K. Klincewicz, Warszawa 2016, s. 206–225.

problemów bezpieczeństwa, np. do bezpieczeństwa społecznego[8]. Podejście sytuacyjne dotyczy tylko organizacji jako klasy systemów. Nastawione jest na wykorzystanie koncepcji zawartych w głównych teoriach zarządzania w sytuacjach rzeczywistych. W tym podejściu zwraca się uwagę, że efektywność praktyk menadżerskich, funkcji, stylów i technik jest uzależniona od okoliczności, które podlegają zmianom. Rozpatrywane są zmienne sytuacyjne mające wpływ na wybór rozwiązania danego problemu. Takimi zmiennymi są m.in. wielkość organizacji, stopień rutyny w stosowaniu danej technologii, niepewność środowiska czy indywidualne różnice pomiędzy osobami, w tym – liderami[9]. Rozważania odnośnie do podejścia sytuacyjnego prowadzą do wniosku, że przed podjęciem decyzji co do wykorzystania konkretnej koncepcji lub metody zarządzania należy brać pod uwagę m.in. niepowtarzalne cechy danej sytuacji, współzależność elementów składających się na organizację oraz interakcje z otoczeniem. Podkreśla się złożoność sytuacji zarządczych. W kwestiach metodologicznych kluczowe są w tym przypadku metody ilościowe, podejście idiograficzne (opis i wyjaśnianie faktów oraz zdarzeń jednostkowych i niepowtarzalnych) oraz analiza studiów przypadków. Kierunek systemowy i sytuacyjny stanowi próbę integracji dorobku klasycznego w teorii organizacji i zarządzania[10]. Dyskusja na temat podejścia systemowego i sytuacyjnego ma duże znaczenie – także praktyczne – z punktu widzenia bezpieczeństwa organizacji.

Dyskutowane są różne aspekty metodologiczne nauk o zarządzaniu w nurtach teoretycznym i empirycznym. Agnieszka Sobol podkreśla, że teoria empiryczna stanowi system twierdzeń i metod: metody służą z jednej strony do uzyskiwania twierdzeń, z drugiej zaś – do ich weryfikacji. System twierdzeń tworzy teorię, zaś metoda naukowa stanowi instrument wykorzystywany do tworzenia tego systemu. Z kolei do rozwiązywania problemów teoretycznych w naukach o zarządzaniu wykorzystywane są następujące metody naukowe: indukcji (zupełnej lub niezupełnej), dedukcji oraz metody hipotetyczno-dedukcyjne. Metoda dedukcji służy w ramach nurtu teoretycznego nauk o zarządzaniu do rozwiązywania problemów naukowych związanych z brakiem wiedzy dotyczącej teorii. Metodę tę, choć nie jest to powszechne, można również wykorzystać do rozwiązywania problemów teoretycznych nurtu praktycznego nauk o zarządzaniu. Teoretyczne problemy naukowe nurtu empirycznego rozstrzyga się przy użyciu metod indukcyjnych (indukcja zupełna lub niezupełna). Problemy praktyczne odnoszą się w większości do działalności operacyjnej, do racjonalnych rozwiązań dotyczących celów, warunków lub działania[11].

W ostatnich latach pojawiły się opracowania związane z metodologią nauk o bezpieczeństwie, w tym dotyczące metrologii[12]. Tematyka podnoszenia poziomu

[8] J. Gierszewski, *Model bezpieczeństwa społecznego na tle teorii systemów*, „Colloquium Wydziału Nauk Humanistycznych i Społecznych AMW" 2013, nr 2 (10), s. 65–80.

[9] A. Tomaszuk, *Podejście systemowe i sytuacyjne*, [w:] *Koncepcje i metody zarządzania*, red. W. Matwiejczuk, Białystok 2009, s. 32–34.

[10] S. Lachiewicz, M. Matejun, *Ewolucja nauk o zarządzaniu*, [w:] *Podstawy zarządzania. Teoria i ćwiczenia*, red. A. Zakrzewska-Bielawska, Warszawa 2012, s. 109–116.

[11] A. Sobol, *Inteligentne miasta versus zrównoważone miasta*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 320, s. 75–86.

[12] *Metrologia nauk o bezpieczeństwie i obronności. Wybrane zagadnienia*, red. R. Białoskórski, P. Górny, Siedlce 2018.

bezpieczeństwa odnosi się do różnych wymiarów: międzynarodowego, krajowego[13], lokalnego i wymiaru różnego typu organizacji, w tym przedsiębiorstw. Dotyczy także określonych problemów, np. cyberbezpieczeństwa. Analizuje się przykładowo aspekty bezpieczeństwa cybernetycznego państw europejskich – w szczególności w kwestii zwiększania zdolności i gotowości do reagowania na zagrożenia cybernetyczne, ale także wzmacniania współpracy i koordynacji między państwami członkowskimi Unii Europejskiej. Ta współpraca i koordynacja powinna obejmować odpowiednie instytucje, agencje, władze oraz przemysł[14].

Dyskutowany jest wybór metodologii badania bezpieczeństwa. Odnosząc się do stosunków międzynarodowych, bezpieczeństwo podmiotów (nie tylko uczestniczących w stosunkach międzynarodowych) rozpatrywane jest w aspekcie paradygmatów: 1) realistycznego (odnoszącego się do państwa w wymiarze podmiotowym), akcentującego znaczenie czynnika militarnego; 2) liberalnego (idealistycznego), uwzględniającego m.in. współpracę narodów i państw, rozwijającego się w kierunku wzrostu znaczenia aktorów wewnątrzpaństwowych, aspektów niemilitarnych i niesiłowych metod kształtowania bezpieczeństwa; 3) konstruktywistycznego, negującego istnienie obiektywnej rzeczywistości społecznej, którą traktuje się jako formę świadomości. Bezpieczeństwo międzynarodowe można zatem traktować jako występujące w intersubiektywnej świadomości – stanowi ono konstrukt społeczny.

Metodologie badań bezpieczeństwa mogą mieć charakter pozytywistyczny (empiryczny, klasyczny – jak tradycjonalizm, realizm i neorealizm, liberalizm i behawioryzm oraz behawioralizm), a także postpozytywistyczny (teoria krytyczna, postmodernizm i konstruktywizm)[15].

Treści zawarte w tym numerze kwartalnika „Bezpieczeństwo. Teoria i Praktyka" odnoszą się do zasygnalizowanych powyżej kwestii. Dotyczą metod i narzędzi podnoszenia poziomu bezpieczeństwa: międzynarodowego (m.in. artykuły poruszające problematykę Unii Europejskiej i Rosji), krajowego oraz różnego typu organizacji – w tym miast i przedsiębiorstw. W szczególności prezentowana jest możliwość wykorzystania w tym celu metod i narzędzi zarządzania. Rozpatrywane są także problemy zarządzania bezpieczeństwem w ujęciu systemowym. W numerze zamieszczono również teksty o charakterze historycznym, recenzje oraz sprawozdania z wydarzeń poświęconych dyskusji o problemach teoretycznych i praktycznych związanych z bezpieczeństwem, w tym – z zarządzaniem bezpieczeństwem.

---

13 Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Siedlce 2016.

14 J. Cichosz, *Kierunki działań instytucji europejskich na rzecz podnoszenia poziomu bezpieczeństwa podmiotów państwowych i niepaństwowych w cyberprzestrzeni – wybrane przykłady*, „TEKA of Political Science and International Relations" 2018, vol. 13, nr 2, s. 49–63.

15 R. Zięba, *Bezpieczeństwo w ujęciu różnych paradygmatów naukowych*, [w:] *Bezpieczeństwo. Dyscyplina nauki wobec funkcjonowania państwa*, red. R. Skarzyński, E. Kużelewska, Białystok 2018, s. 13–26.

Artykuły i materiały
Articles and Materials
Beiträge und Materialien
Статьи и материалы

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-001

Janusz Ziarko

dr hab., prof. KA, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0002-9100-2807

Podejście systemowe w badaniach bezpieczeństwa organizacji

Wprowadzenie

Rozwój nauk o bezpieczeństwie warunkowany jest między innymi koniecznością wychodzenia poza tradycyjny paradygmat neopozytywistyczny, którego możliwości na gruncie nauk społecznych wyczerpują się. Wiąże się to z wieloraką złożonością zjawisk bezpieczeństwa i z coraz większą dynamiką zmian otaczającej człowieka rzeczywistości, którym tradycyjny paradygmat nie może sprostać.

Teza 1: W naukach o bezpieczeństwie obserwuje się zbyt duże przywiązanie większości przedstawicieli tych nauk do paradygmatu neopozytywistycznego. Teorie formułowane na gruncie nauk o bezpieczeństwie (podobnie jak w innych dyscyplinach nauk społecznych) w oparciu o paradygmat neopozytywistyczny są nieprecyzyjne, brak jest jednomyślności co do tego, czym jest bezpieczeństwo. Świadczy to o niedostatecznym zaawansowaniu bezpieczeństwa jako nauki – sprawia też, że niemożliwe staje się bezpośrednie porównanie elementów jednej teorii z elementami innej teorii[1].

Teza 2: Bezpieczeństwo, niezależnie od tego, jak je postrzegamy i definiujemy, ma cechy i właściwości systemu. Stąd nowym paradygmatem, z perspektywy którego analizować należałoby bezpieczeństwo, winien być paradygmat systemowy. Przejście do nowego paradygmatu jest trudne, ponieważ znacząca część przedstawicieli nauk społecznych nie widzi potrzeby takiej zmiany – paradygmatycznej

[1] J. Kozielecki, *Człowiek wielowymiarowy*, Warszawa 1996, s. 4; idem, *Koncepcje psychologiczne człowieka*, Warszawa 1996, s. 239, 258.

ekspansji. Zauważa się niechęć związaną z rozszerzaniem dotychczasowego czy poszukiwaniem nowego paradygmatu.

Złożoność i dynamika bezpieczeństwa leżą u podstaw przeświadczenia, że uchwycenie zjawisk i procesów bezpieczeństwa oraz ich zmian wymaga dynamicznego ich ujęcia, rozumianego jako zmienność w czasie i jednoczesna zdolność przystosowania się, a ujęciem takim powinno być podejście i analiza systemowa. Pomyślność każdego przedsięwzięcia ukierunkowanego na bezpieczeństwo warunkowana jest poznaniem z jednej strony potrzeb bezpieczeństwa podmiotu, z drugiej – zjawisk i procesów bezpieczeństwa i jego zagrożeń oraz skorelowanie ich z przedsięwzięciami i możliwościami realizacji. Niezbędne jest podejście indywidualne i zrozumienie specyfiki układu: zagrożenia – bezpieczeństwo, jego uwarunkowań kształtujących działania podmiotów. Myślenie i podejście systemowe/ analiza systemowa, dobrze zorganizowane i zrealizowane, ułatwiają pozyskanie adekwatnych informacji dotyczących układu: zagrożenia – bezpieczeństwo, zarówno tych bezpośrednio związanych z głównymi czynnikami wpływających na bezpieczeństwo podmiotu, jak i pośrednio warunkujących jego prawidłowe i bezpieczne działanie.

Celem artykułu jest przedstawienie teoretycznej koncepcji łączącej idee myślenia i podejścia systemowego w całość spełniającą przesłanki właściwej i solidnej metody badawczej i narzędzia poznania, które pozwoli uchwycić najważniejsze czynniki wpływające na kształt i charakter badanego aspektu bezpieczeństwa, na dokonywanie syntez rozważanych zagadnień, tak by stworzyć możliwości ich rozległego opisu wiedzą metodologiczną i teoretyczną przedstawiającą założenia badawcze jak i prawidłowości funkcjonowania badanego systemu.

W pracy przyjęto następujące hipotetyczne założenia: 1) myślenie i podejście systemowe jest wysoce użyteczną metodologią budowania wyjaśniających teorii bezpieczeństwa, a także skutecznym narzędziem tworzenia procedur interpretujących procesy i zjawiska bezpieczeństwa i jego zagrożeń w ujęciach retrospektywnych, aktualnych i prospektywnych; 2) podejście systemowe jest przydatne poznawczo w badaniu zjawisk i procesów bezpieczeństwa oraz jego zagrożeń charakteryzujących się szczególnym poziomem złożoności i umożliwia charakterystykę ich genezy, struktur, zakresu i skutków oddziaływania, uwarunkowań zewnętrznych i wewnętrznych, a także przedsięwzięć mających na celu zapewnienie pożądanego ich poziomu.

Istota systemu

Nauka coraz częściej i w coraz większym stopniu korzysta z terminów właściwych dla teorii systemów, takich jak złożoność, nieliniowość, chaos, gdyż zdaniem wielu badaczy teoria ta umożliwia dokładniejszy opis poznawanej rzeczywistości – uwzględniający naturę, funkcjonowanie i wzajemne powiązania występujące pomiędzy elementami tej rzeczywistości. Przesłanką teorii systemów jest hipoteza zakładająca niepodzielność nauki. Umożliwia to łączenie i wspólne rozważanie zjawisk, zdarzeń, procesów występujących w różnych obszarach rzeczywistości: przyrodniczej, społecznej czy gospodarczej. Pozwala koncentrować się na ich specyfice, istniejących współzależnościach, opisywać i wyjaśniać ich wzajemne oddziaływania, lokując je w kontekstach, w których zachodzą.

Zasadne jest więc pytanie: czy i dlaczego teoria systemów pozwala na dokładniejsze poznanie badanej rzeczywistości aniżeli badania prowadzone w paradygmacie analityczno-redukcjonistycznym czy holistycznym? Odpowiedź związana jest z podstawowym dylematem ludzkiego poznania, czyli relacją pomiędzy całością i jej częściami. Uwikłana jest więc w spór między holizmem optującym za supremacją całości nad częściami, a kartezjańskim redukcjonizmem, według którego części dominują nad całością.

Teoria systemów sygnalizuje możliwości przezwyciężenia tego poznawczego dylematu i radzenia sobie ze złożonością. System – kluczowe pojęcie tej teorii – łączy w sobie możliwości poznania i opisu złożonych zjawisk należących zarówno do świata przyrody, jak i do społeczeństwa, umożliwia odkrywanie funkcjonalnych i strukturalnych zasad charakteryzujących te zjawiska, określanie czynników je warunkujących i ich opisywanie[2]. Cechy, które znamionować winny każdą teorię bezpieczeństwa formułowaną w kategoriach teorii systemów, to pojęciowo-analityczne podstawy, osadzenie na danych uzyskiwanych z badań empirycznych, ale przede wszystkim to syntetyzujący, konsolidacyjny i integrujący charakter. Takie wyróżniające cechy i właściwości teorii bezpieczeństwa suponują, że głównym sposobem badania bezpieczeństwa jest traktowanie go jako systemu[3]. Czym więc jest system?

System jest zbiorem elementów celowo wyodrębnionych spośród innych (ze zbioru elementów pewnej rzeczywistości), stanowiących zorganizowaną całość. Elementy te, posiadające określone własności, wzajemnie powiązane i na siebie oddziałujące, pełnią uzgodnione funkcje, a zmiany zachodzące w jednym elemencie systemu mogą wpływać na niektóre lub wszystkie pozostałe elementy. Powiązanie elementów stanowi o istocie systemu, o jego niepowtarzalnych właściwościach, a wyeliminowanie z systemu chociażby jednego jego elementu mającego określone przeznaczenie, przekształca system w system jakościowo różny od pierwotnego[4].

System jako odrębna całość posiada granicę – systemy różnią się między sobą stopniem ich otwartości: od systemów zamkniętych o nieprzepuszczalnych granicach, do systemów otwartych komunikujących się z otoczeniem. System charakteryzują wejścia i wyjścia, procesy wewnętrznego przetwarzania oraz

---

[2] Systemowa wizja świata „[…] ujmuje rzeczywistość jako zhierarchizowany układ systemów lub może lepiej jako jeden wielki system z licznymi hierarchicznie uszeregowanymi podsystemami i to, zaznaczmy wyraźnie, podsystemami dynamicznymi, zmiennymi, ewoluującymi. Cała rzeczywistość jawi się więc jako olbrzymi układ obejmujący w sobie zespół mniejszych systemów będących w ustawicznym rozwoju, wzajemnie na siebie oddziałujących. A zatem filozofia systemowa jest ukierunkowana na uchwycenie czynnika zmienności, ewolucji w świecie. A zarazem czynnika pewnego ładu, porządku, harmonii. Rzeczywistość jawi się nam jako jeden wielki proces, jako ciągłe stawanie się", M. Lubański, *Informacja – system*, [w:] *Zagadnienia filozoficzne współczesnej nauki. Wstęp do filozofii przyrody*, red. M. Heller, M. Lubański, S.W. Ślaga, Warszawa 1997, s. 63.

[3] Zob. A.K. Koźmiński, *Analiza systemowa organizacji*, Warszawa 1976.

[4] Definicja własna, na podstawie: W. Gasparski, *Pojęcie systemu. Z zagadnień metodologii badań i projektowania systemowego*, [w:] *Projektowanie maszyn i systemów cyfrowych*, red. A. Michalski, Warszawa 1972, s. 29; S. Beer, *Cybernetyka a zarządzanie*, tłum. Ś. Sorokowski, Warszawa 1966, s. 13; M.J. Hatch, *Teoria organizacji*, tłum. P. Łuków, Warszawa 2002, s. 50; M. Sharma, *System Approach: An Inter-disciplinary Effort*, [w:] *System Approach: Its Application in Education*, red. M. Sharma, Bombay 1985, s. 17.

sprzężenia zwrotne, które określają jego dynamiczną naturę. System opisany jest też przez zbiór relacji pomiędzy jego elementami oraz ich relacji z wybranymi elementami otoczenia, dobrany tak, że całość zdolna jest do funkcjonowania w określony sposób dla realizacji celu (rozwiązania zadania), co stanowi zasadnicze kryterium wyodrębnienia systemu[5].

Powyższe definicje unaoczniają, że:

- system jest ogólnym terminem znajdującym zastosowanie w wielu dziedzinach, w tym w naukach o bezpieczeństwie;
- system nie jest zwykłym zbiorem elementów, lecz stanowi złożoną, uporządkowaną i całościową strukturę elementów wzajemnie powiązanych i współzależnych – ich celowe i specyficzne połączenie nadaje mu swoiste, niepowtarzalne właściwości;
- system to dynamiczna i zintegrowana całość, w której każdy element jest sprzężony z pozostałymi, a zmiana jednego pociąga za sobą zmiany w innych i w całym systemie – cyrkularna przyczynowość: relacje przyczynowości charakteryzują się wielokierunkowością związków zachodzących w obrębie systemu, który sprawnie funkcjonuje tylko przy prawidłowo ułożonym współudziale swoich elementów;
- system ma cele i funkcjonuje, by je osiągnąć. Dynamika systemu obejmuje transformację wejścia na wyjście, procesy, funkcje, czyli działania systemu, które są nastawione na osiągnięcie tych celów;
- system i wszystkie jego elementy mają swoje role, które muszą być określone w stosunku do siebie nawzajem oraz w odniesieniu do celów systemu;
- system otwarty podlega nieustannym przemianom na skutek oddziaływania otoczenia i przystosowywania się systemu do owych oddziaływań;
- system społeczny jest otwarty – posiada zdolności do samoregulacji i utrzymania dynamicznej równowagi pomimo zmian zewnętrznych. Dla sprawnego funkcjonowania musi umiejętnie kształtować swoje stosunki z otoczeniem, czyli z innymi systemami: nadrzędnymi, równorzędnymi i podrzędnymi;
- system wymianę z otoczeniem realizuje poprzez mechanizm sprzężenia zwrotnego, który wiąże się z występowaniem i interakcją dwóch rodzajów sprzężeń: 1) dodatnich, wykazujących tendencję do samowzmacniania, czyli wzrostu wartości liczbowych określonych zmiennych systemu; oraz 2) ujemnych, objawiających się spadkiem wartości określonych zmiennych, co wiąże się z działaniem równoważącym i stanowi przeciwwagę dla sprzężeń dodatnich;
- system posiada granicę oddzielającą elementy systemu od elementów jego otoczenia, a jej wytyczenie jest uzależnione od badacza i celów jego badań. Granice systemu są granicami dynamicznymi, a dynamizacja granicy systemu bezpieczeństwa określa zasięg oddziaływania czynników wpływających pozytywnie bądź negatywnie na bezpieczeństwo podmiotów systemu;
- system i każdy jego element mają ograniczenia – niektóre z systemów zewnętrznych lub ich komponenty mogą ułatwiać bądź hamować procesy danego systemu, a także elementy tego systemu mogą nie obsługiwać innych elementów we wszystkich aspektach – stąd ważne są informacje o ograniczeniach, aby można było opracować proces ich przezwyciężenia;
- system może i powinien się zmieniać/rozwijać – zmiana/rozwój polegać może np. na zmianie sekwencji, zmianie komponentu i ich wzajemnych zależności. Projektując zmianę, rozpatrywać musimy system, jak i wszystkie jego elementy i ich funkcje w kontekście ich wpływu na całość systemu, elementy powiązane i systemy sąsiednie;
- system i każdy jego element jako obiekt badania wymagają, by w procesie badania nawiązywać do własności systemu jako całości, do jego celów, procesów i treści, do jego struktury, funkcji i ewolucji.

[5] Definicja własna, na podstawie: T. Tomaszewski, *Człowiek i otoczenie*, [w:] *Psychologia*, red. T. Tomaszewski Warszawa 1976, s. 15; J. Habr, J. Vepřek, *Systemowa analiza i synteza. Nowoczesne podejście do zarządzania i podejmowania decyzji*, tłum. A. Kusto, Warszawa 1976, s. 32; K. Perechuda, *Organizacja wirtualna*, Wrocław 1997, s. 24.

Z powyższego wynika, że każdy obiekt rozważany jako system posiada swoją indywidualną, niepowtarzalną wewnętrzną organizację, układ ról i wzajemnych stosunków/interakcji między elementami tego systemu i wybranymi elementami otoczenia. System jako zorganizowana całość, która staje się przedmiotem badań, charakteryzuje się swoistymi właściwościami i cechami oraz właściwościami i cechami swoich elementów, które odróżniają go od otoczenia. Niezwykle istotna jest rola powiązań systemowych i międzysystemowych, czyli relacji pomiędzy własnościami (atrybutami) sytemu i własnościami poszczególnych jego elementów, a także wybranymi elementami otoczenia. To powiązania systemowe stanowią o celowo zorientowanej całości, to one kierunkują działania na osiąganie określonych celów systemu, wpływają na dynamikę procesów zachodzących w systemie i w jego otoczeniu, regulują relacje w systemie i pomiędzy systemem a otoczeniem. Rozważać je należy każdorazowo w kontekście celów – zarówno systemu jako całości, jak i celów poszczególnych jego elementów.

Teoria systemów, której podstawę stanowi idea całościowego rozpatrywania systemu, zaleca, żeby poszczególne części systemu badać i opisywać poprzez poznanie ich miejsca i znaczenia w i dla całości systemu. Jest to podejście całkowicie przeciwstawne redukcjonistycznej, mechanistycznej koncepcji funkcjonowania i poznawania świata. Dla redukcjonizmu charakterystyczny jest podział obiektu bądź problemu badań na części składowe (często przypadkowo wyodrębniane), zrywający różnorakie powiązania pomiędzy nimi występujące, po to, by przez kolejne uproszczenia badać własności jego oddzielnych, niepowiązanych części i w ten sposób wnioskować o zachowaniu się całości. Widać, że złożoność, która trudno poddaje się rozkładowi na czynniki pierwsze, stanowi zagrożenie dla tej metody naukowej.

Teoria systemów – hołdująca podejściu i myśleniu całościowemu – pozwala na badanie i wyjaśnienia ogólnego zachowania różnych systemów empirycznych, a w szczególności umożliwia:

- analizowanie systemu nie tylko jako sumy części i zależności pomiędzy nimi, ale także opisanie funkcji, zadań, procesów związanych z realizacją celów systemu;
- określenie granic wewnętrznych, które oddzielają od siebie podsystemy, a także granic zewnętrznych, które wyodrębniają system od otoczenia (innych systemów);
- opisanie hierarchicznego uporządkowania elementów systemu ze wskazaniem miejsca elementu/subsystemu w większej całości, a także jego relacji z innymi sybsystemami własnego systemu i sybsystemami innych systemów;

- badanie tego, co dzieje się w systemie, gdyż wywiera to ogromny wpływ na zachowanie każdego z jego członków, a wpływ ten jest tak duży, że nie da się zrozumieć zachowań danej jednostki bez znajomości systemu i jej sytuacji w systemie;
- ocenianie siły połączeń między elementami systemu, gdyż to one decydują o trwałości i stabilności systemu. Gdy te powiązania słabną, system łatwiej będzie ulegał dezorganizacji, będzie narażony na rozpad;
- wiązanie ogólnych własności systemu, jego funkcji, zadań, procesów z różnymi obiektami, zjawiskami czy wymaganiami otoczenia;
- uwzględnienie w wynikach działania systemu uwarunkowań wewnętrznych i zewnętrznych określających ramy i możliwości jego funkcjonowania;
- zrozumienie zachowań systemowych – co wzbogaca naszą wiedzę o realizowanych funkcjach, zadaniach, procesach i pozwala planować ich rozwój.

Bezpieczeństwo jako system

Teza: zachowania ludzi związane z jednostkowym czy grupowym bezpieczeństwem bardzo często znacząco się różnią, niekiedy wykluczają się, tak jakby zjawiska, zdarzenia czy procesy związane z bezpieczeństwem były przez nas postrzegane i interpretowane w zupełnie inny sposób. Powodem tej różnorodności jest pluralizm perspektyw poznawczych uwzględniający różnorodność, zróżnicowanie, a nawet konkurencyjność zjawisk społecznych[6], w tym związanych z bezpieczeństwem.

Pomiędzy zjawiskiem, zdarzeniem czy procesem, na które patrzymy, a obrazem, który widzimy, występują – ujmowane społecznie i kulturowo – nasze wartości, normy, wiedza i doświadczenie, które mają wpływ na to, że pluralistycznie postrzegamy i rozumiemy bezpieczeństwo. Analizując bezpieczeństwo, możemy posługiwać się pojęciem systemu, gdyż takie elementy bezpieczeństwa jak wartości, normy, wiedza i doświadczenie – wykorzystywane w jednostkowych i grupowych działaniach w obszarze bezpieczeństwa – są współzależne i skoordynowane oraz stanowią nierozerwalny i respektowalny komponent praktyki społecznej[7]. W takim rozumieniu bezpieczeństwo jednostki, grupy czy obiektu jest zjawiskiem złożonym z elementów tworzących całość, między którymi występują integrujące je związki i zależności, niekiedy bardzo skomplikowane. Tak więc elementy bezpieczeństwa są ze sobą powiązane i bezpieczeństwo należy traktować jako system, a nie jako grupę czy agregat składający się z niepowiązanych części.

Dla analiz bezpieczeństwa jednostki, grupy czy obiektu kluczowe staje się: 1) postrzeganie bezpieczeństwa oraz jego różnych podsystemów czy aspektów jako powiązanych ze sobą całości, czyli traktowanie bezpieczeństwa systemowo; 2) konieczność rozważania go w ścisłym związku ze społecznym i kulturowym otoczeniem, które należy traktować jako nadsystem w stosunku do systemu bezpieczeństwa. Traktowanie bezpieczeństwa jako systemu, który tworzony jest przez współzależne od siebie elementy, pozwala analitykom systemu znajdować w jego obrębie te elementy i ich powiązania i analizować pełnione przez nie funkcje w aspekcie doskonalenia praktyki

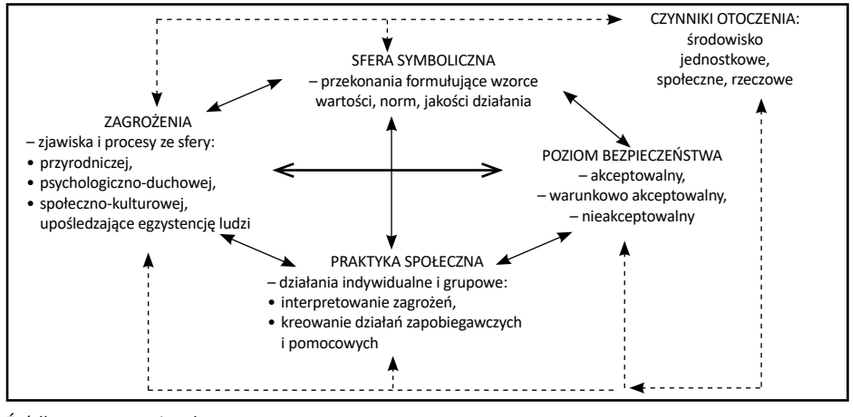
[6] J. Pluta, *Społeczno-kulturowe procesy definiowania postaw*, Wrocław 2002, s. 71.

[7] *Ibidem*, s. 70–73.

społecznej ukierunkowanej na bezpieczeństwo. Charakterystyczną cechą bezpieczeństwa ujmowanego jako system jest więc to, że żaden z analizowanych podsystemów ani żaden z jego elementów nie jest całkowicie neutralny w stosunku do pozostałych, do całości systemu, ani w stosunku do wyróżnionych elementów otoczenia. Jest to następstwem funkcjonalnej zależności wobec, z jednej strony, interesów i kompetencji określonych podmiotów bezpieczeństwa: jednostek, grup społecznych czy instytucji, występujących najczęściej jako elementy innych systemów społecznych, a z drugiej – obowiązujących wartości, norm społecznych i kulturowych oraz rozwiązań prawa zewnętrznego i wewnętrznego regulującego funkcjonowanie różnych systemów.

Bezpieczeństwo podmiotu rozpatrywane jako system, czyli odrębny i autonomiczny układ, nie jest prostą sumą elementów i czynników nań składających się, lecz jest całością, w której wszystkie elementy i czynniki są ściśle ze sobą powiązane i wzajemnie oddziaływają na siebie, stanowiąc pewną jakość, która jest odbierana/interpretowana przez podmiot jako poziom/poczucie bezpieczeństwa. Można i należy postrzegać je przez pryzmat jego elementów składowych, różnych ich ról i funkcji (np. obiegu informacji o zagrożeniach bezpieczeństwa czy procedur postępowania w sytuacji określonego zagrożenia) oraz wiążących je zależności – ze świadomością, że analiza bezpieczeństwa podmiotu w aspekcie wyróżnionego aspektu, roli czy funkcji (np. obiegu informacji) jest tylko jednym z możliwych jego ujęć. Stąd problem bezpieczeństwa podmiotu, traktowanego jako system, wymaga rozpatrywania w połączeniu z innymi elementami tego systemu i w kontekście specyficznych jego cech, i włączenia w ten proces podmiotu jako części składowej systemu (rysunek 1).

Rysunek 1. Ogólny obraz systemu bezpieczeństwa



Źródło: opracowanie własne.

Dotychczasowe próby usprawniania działań na rzecz bezpieczeństwa niewiele nowego wnoszą do sposobów myślenia i działania różnych podmiotów odpowiedzialnych za bezpieczeństwo swoje i innych. Potrzebna jest jasna wizja tego, jakie to bezpieczeństwo u siebie chcemy mieć, jak i jakimi środkami mamy je osiągać, a więc

wizja celów – nadająca kierunek rozwojowym przedsięwzięciom i określająca sposoby ich osiągania. Badanie bezpieczeństwa jako systemów społecznych łączy w sobie badanie obiektów należących do czterech powiązanych ze sobą obszarów: 1) zagrożeń i ich kontekstów, 2) skutków oddziaływania tych zagrożeń w różnych kontekstach, 3) zachowań/działań osób i ich zespołów/grup, które ochraniają i wspierają podmioty zagrożone, 4) jednostek i instytucji ochraniających i wspierających podmioty zagrożone w ich wzajemnych i środowiskowych relacjach, uwarunkowaniach i kontekstach. Dzięki temu różne zaangażowane w bezpieczeństwo podmioty będą wiedzieć, w jakim celu i w jaki sposób wykorzystać twórczy oraz organizacyjny potencjał, żeby osiągnąć zaplanowane efekty.

Myślenie i podejście systemowe do bezpieczeństwa

Myślenie systemowe

Czym powodowana jest stale rosnąca luka między stanem bezpieczeństwa a szybko zmieniającymi się (głównie rosnącymi) oczekiwaniami rozwijającego się społeczeństwa dotyczącymi bezpieczeństwa? Przyczyn tej luki upatrywać można przede wszystkim w dominującym u analityków bezpieczeństwa modelu myślowym, tj. sposobach, w jakie myślimy o bezpieczeństwie i o zagrożeniach tego bezpieczeństwa oraz analizujemy funkcjonowanie własne i instytucji za bezpieczeństwo odpowiedzialnych. Rozpowszechniony model myślowy zakorzeniony jest w tradycyjnym, pozytywistycznym podejściu do zdobywania wiedzy, cechującym się myśleniem analitycznym, redukcjonizmem i determinizmem. Skutkuje to[8]: 1) naszymi fragmentarycznymi studiami dotyczącymi bezpieczeństwa i często przypadkowym przyrostem wiedzy, którą wykorzystujemy w działaniach służących poprawie bezpieczeństwa; 2) niemożnością zintegrowania pomysłów dotyczących rozwiązań i działań doskonalących organizację pracy prewencyjnej, operacyjnej i pomocowej instytucji bezpieczeństwa w logiczną i spójną całość; 3) mentalnym i rzeczywistym pozostawaniem w obrębie dotychczasowych rozwiązań.

Teoria systemów propaguje formułę systemowego sposobu myślenia, operującą wielkościami: całości i części oraz relacji, które się między nimi tworzą – formułę myślenia całościowego ze względu na powiązania i zależności, istotną zarówno intelektualnie, jak i pragmatycznie. Znaczenie systemowego sposobu myślenia dla efektywności poznania i uzależnionego od niego działania jest stosunkowo mało znane, a w analizach uwarunkowań bezpieczeństwa taki myślowy nurt dociekań należy do rzadkości. Tak więc podejście i myślenie systemowe w praktyce badawczej nie jest zjawiskiem częstym, a zespoły naukowców takiej potrzeby w swojej badawczej działalności nie afirmują, hołdując neopozytywistycznym preferencjom metodologicznym. Przeważa mylne przeświadczenie, że podejście neopozytywistyczne wystarczająco dobrze opisuje i wyjaśnia zjawiska bezpieczeństwa. Nie zauważa się bądź pomija fakt, że to, co nie jest dostrzegane i rozpoznawane w teorii, następnie nie jest wykorzystywane w praktyce bezpieczeństwa.

[8] B.H. Banathy, *Projektowanie systemów edukacji. Podróże w przyszłość*, tłum. M. Bazewicz, Wrocław 1994, s. 17–21.

Na czym więc polega myślenie systemowe i jak można je wykorzystać w poznawaniu problemów bezpieczeństwa? Myślenie systemowe jest sztuką widzenia całości, a w niej – oddzielnych części i ich wzajemnych relacji, to także dostrzeganie charakteru i dynamiki zmian w czasie, a nie tylko liniowego łańcucha przyczyn i skutków czy statycznych migawkowych obrazów[9]. Jest to myślenie problemowe i holistyczne, wymagające rozwiniętej intelektualnej i mentalnej kultury organizacyjnej. Sprzyja rozumowaniu kategoriami identyfikacji skali i wagi problemów zagrożeń bezpieczeństwa, sposobów i kolejności ich rozwiązywania, a także uwzględnia interesariuszy, którzy z danego rozwiązania będą korzystać. Myślenie takie ułatwia odkrywanie wzorów powiązań i zależności pośród pozornie niepowiązanych zdarzeń, procesów, rzeczy, istot, umożliwia pogłębioną refleksję nad sposobem zorganizowania działań dla bezpieczeństwa, nad czynnikami, które to zorganizowanie warunkują, a które z reguły należą do różnych dyscyplin naukowych.

Istotą myślenia systemowego jest cyrkularne rozumienie przyczynowości – polega ono na odrzuceniu rozumowania przyczynowo-skutkowego (linearnego) na rzecz cyrkularnego rozumienia relacji i związków. W takim ujęciu elementy systemu działają na siebie w sposób cyrkularny, oddziałują na siebie nawzajem na zasadzie sprzężeń zwrotnych, które mogą być ujemne lub dodatnie. Sprzężenia ujemne korygują system i przywracają poprzednią równowagę, natomiast dodatnie mogą wzmacniać odchylenia prowadzące do jego rozpadu. Systemy sprzężeń zwrotnych ujemnych i dodatnich tworzą serię uwarunkowanych zdarzeń będących ze sobą w stałej interakcji[10]. Rozumienie cyrkularne zakłada obowiązywanie zasad ekwifinalności i ekwipotencjalności, według których jeden skutek może być wywoływany różnymi przyczynami, a ta sama przyczyna – prowadzić do różnych skutków. To sprawia, że nie można określić tak zwanej „pierwotnej przyczyny", gdyż przyczyna może być jednocześnie skutkiem, a skutek – przyczyną. Cyrkularne rozumienie przyczynowości uwidacznia zależności pokazujące, że np. zachowania agresora wpływają na myślenie atakowanego i na sposób jego zachowania, ale także myślenie i zachowanie atakowanego powoduje określone reakcje i działania agresora. Stąd agresor podejmuje określone działania między innymi dlatego, że atakowany zachowuje się w określony sposób (emanuje strachem, uległością, brakiem chęci do obrony – bądź jest do obrony przygotowany i reaguje adekwatnie do sytuacji), wówczas agresor, widząc zachowanie atakowanego, uwzględnia w swoich działaniach jego możliwości i zaangażowanie (rozpoznaje jego lęk i uległość, co wzmaga jego agresję – bądź odstępuje od ataku, nie widząc szans na sukces).

Dla podmiotów angażujących się w pracę dla bezpieczeństwa i jej usprawnianie ważna jest umiejętność spojrzenia na całość tej pracy, na występujące powiązania i zależności między zachodzącymi w niej procesami organizatorskimi i operacyjnymi, a to wymaga przyjęcia zarówno przez jednostki, jak i instytucje paradygmatu systemowego myślenia jako obowiązującego, zakładającego kwestionowanie jako jedynego tradycyjnego, liniowego, przyczynowo-skutkowego porządku normującego

[9] P.M. Senge, *Piąta dyscyplina. Teoria i praktyka organizacji uczących się*, tłum. M. Lipa, Warszawa 1998, s. 19–24.

[10] B. Józefik, *Rozwój myślenia systemowego a terapia rodzin*, [w:] *Ewolucja myślenia systemowego w terapii rodzin. Od metafory cybernetycznej do dialogu i narracji*, red. L. Górniak, B. Józefik, Kraków 2003, s. 12–18.

działania dla bezpieczeństwa. Myślenie systemowe, uwzględniające złożoność, nieliniowość, chaos, względny nieporządek charakteryzujący rzeczywistość i organizację działań dla bezpieczeństwa, pozwala na dostrzeżenie/odkrycie i zdefiniowanie funkcjonalnych obszarów, w których ukryte są prawdziwe przyczyny trudności, z którymi się borykamy i w których zmiana przyniesie realną korzyć. Tym samym umożliwia dostrzeganie problemu (zjawiska, procesu), który ulokowany jest w różnych warstwach czy poziomach tworzących hierarchię systemu, zróżnicowanych pod względem perspektywy i skali, które nie dotyczą jedynie przestrzeni, ale także czasu, informacji, zagrożeń, poczucia bezpieczeństwa[11].

Tradycyjne myślenie analityczno-redukcjonistyczne, wywodzące się z podejścia kartezjańskiego, polega na tym, że aby zbadać zjawisko lub rozwiązać problem, należy go podzielić na proste elementy, które są od siebie oddzielone, a to sprawia, że zajmujemy się problemami i potencjalnymi zmianami jedynie na poziomie objawów[12]. Dlatego w myśleniu systemowym niezbędny jest dialog łączący i godzący dwie antagonistyczne zasady: porządku i nieporządku, by dotrzeć do źródła problemu ważnego dla efektywności funkcjonowania podmiotów i instytucji bezpieczeństwa. Ta zasada jest niezbędna dla zrozumienia poznawanej rzeczywistości oraz dla znalezienia narzędzi rozwoju, które doprowadzą do pożądanej zmiany, i sposobów ich zastosowania adekwatnie do potrzeb bezpieczeństwa[13].

Myślenie systemowe nie zastępuje kartezjańskiej zasady rozdzielności badanych zjawisk zasadą całościowości, nie pokrywa się też z myśleniem holistycznym ani nie sprzeciwia się myśleniu analityczno-redukcjonistycznemu. Przeciwnie, jest to myślenie lokujące poznawany obiekt na kontinuum redukcjonizmu i holizmu i jest w stanie łączyć i godzić oba te podejścia. Pozwala na łączenie różnych planów badawczych, analizowanie elementów składowych zjawiska: społecznych, technicznych, przyrodniczych, syntetyzować wyniki badań, by wyjaśnić całe zjawisko. Rzeczywistość staje się wtedy systemem, a dokładniej – zestawem systemów, systemem systemów. Jedną z cech każdego z tych systemów jest to, że całość jest czymś więcej niż sumą części. Inną jest to, że każdy system samoorganizuje się: znajduje się w ciągłym ruchu i zmianie.

Podejście systemowe

Czym jest podejście systemowe i jak możemy je zastosować w usprawnianiu działań dla bezpieczeństwa – ukierunkowanych na eliminację określonych zagrożeń i przebiegających na różnych szczeblach organizacyjnych? W podejściu systemowym postrzegamy bezpieczeństwo jako system, który współdziała z mozaiką innych bytów/rzeczy w swoim węższym i szerszym otoczeniu, a jednocześnie sam składa się z identyfikowalnych elementów nawzajem na siebie oddziałujących. Każda część systemu

[11] J.M. Morawski, *Dominanty ujęć systemowych*, [w:] *Wybrane problemy metodologii badań na potrzeby sportu*, red. J.M. Morawski, Warszawa 2002, s. 115; A.K. Koźmiński, *Ujęcie systemowe*, [w:] *Współczesne teorie organizacji*, red. A.K. Koźmiński, Warszawa 1983, s. 109.

[12] Zob. B. Zych, *Myślenie systemowe – podstawowe zasady w pracy coacha*, [w:] *Myślenie systemowe w coachingu*, red. K. Ramirez-Cyzio, Warszawa 2013, s. 132–140.

[13] Zob. A. Syrek-Kosowska, *„A jeśli nic nie jest pewne?". Perspektywa złożoności – nowe wyzwania coachingu*, [w:] *Myślenie systemowe w coachingu…*, s. 81–89.

może być samodzielnym systemem i sama może być postrzegana zarówno jako obiekt widziany z zewnątrz, jak i jako zestaw oddziałujących części, a badany system może być częścią wchodzącą w interakcje z jednym lub większą liczbą szerszych systemów. Takie podejście pozwala z jednej strony na całościowe, systemowe spojrzenie na badaną rzeczywistość bezpieczeństwa i występujący w niej problem, łącznie z jej powiązaniami z otoczeniem, z drugiej strony pozwala tę rzeczywistość bezpieczeństwa traktować jako system z wejściami i wyjściami, w którym zachodzą określone procesy, a rozwój takiego systemu bądź jego elementu/ów nie jest samoistny i obiektywnie zdeterminowany, gdyż jest zależny od oddziaływań innych elementów systemu i impulsów płynących z otoczenia. Stąd przekształcenia systemu dokonują się zarówno pod wpływem zmieniających się uwarunkowań zewnętrznych, jak i zmienności zachowania jego elementów[14]. Poszukiwania rozwiązań problemów zagrożeń pojawiających się w różnych środowiskach i układach wymaga określenia właściwych obszarów rozważań, a w nich – kluczowych elementów determinujących określony problem, gdyż dopiero w ramach prawidłowo zidentyfikowanego obszaru i trafnie wybranych elementów kluczowych zasadne jest przeprowadzenie analizy relacji i sprzężeń zachodzących wewnątrz samych obiektów, jak też określenie wielostronnych i wielokierunkowych powiązań z obiektami zewnętrznymi. Takie podejście zapewnia z jednej strony uproszczenie złożoności problemu, z drugiej – uzyskanie takich informacji, które pozwolą sformułować trafne odpowiedzi na pytania i podjąć decyzje adekwatne do zagrożenia.

Tak rozumiane podejście jest z jednej strony metodą, swoistym punktem wyjścia skoncentrowanym na dowiedzeniu się, jaki jest poziom bezpieczeństwa i dlaczego jest taki, jaki jest, podstawą do projektowania, organizowania i zarządzania bezpieczeństwem, czyli określenia, jakie to bezpieczeństwo powinno być i co należy uczynić, aby było takie, jakie być powinno[15]. Z drugiej strony jest zbiorem technik, narzędzi i procedur, narzędziową aparaturą wywodzącą się z teorii systemów – będących w stanie sprawnie odpowiadać na nową rzeczywistość generującą zagrożenia, stosownie do sytuacji problemowej. Podejście to tworzy ustrukturyzowana sieć działań, która łączy wątki treściowe należące do rożnych dziedzin nauki, co sprawia, że badanie systemowe z natury rzeczy jest interdyscyplinarne[16]. Wykorzystanie koncepcyjnej i narzędziowej aparatury teorii systemów, rozumianych jako badanie relacji pomiędzy wyróżnionymi i zdefiniowanymi obiektami, pozwala na nadanie większej spójności poszukiwaniom interdyscyplinarnym, gdyż to podejście systemowe umożliwia łączenie poszczególnych koncepcji wywodzących się z rożnych dyscyplin naukowych wokół badanych problemów[17]. Interdyscyplinarny charakter podejścia systemowego znajduje wyraz także w tym, że dzięki jego teoretycznemu ugruntowaniu w cybernetycznych teoriach systemów, wykorzystaniu socjologicznej teorii władzy i wpływu oraz uogólnieniom zaczerpniętym z psychologii społecznej – pozwala

[14] B. Jankowski, *Modelowanie rozwoju krajowego systemu energetycznego z uwzględnieniem wymagań stabilizacji i redukcji emisji dwutlenku węgla w Polsce*, Warszawa 1997, s. 9–12.

[15] Zob. A.K. Koźmiński, *Analiza systemowa…*; G.A. Rummler, A.P. Brache, *Podnoszenie efektywności organizacji. Jak zarządzać „białymi plamami" w strukturze organizacyjnej?*, tłum. T. Ludwicki, Warszawa 2000, s. 36–37.

[16] A. Koźmiński, *Analiza systemowa…*, s. 12.

[17] *Ibidem*, s. 22, 36.

badaczowi na wielowątkowe opisanie problemu prowadzące do jego wyjaśnienia, zrozumienia i rozwiązania.

Wykorzystanie podejścia systemowego w bezpieczeństwie

Fazy, etapy i czynności podejścia systemowego

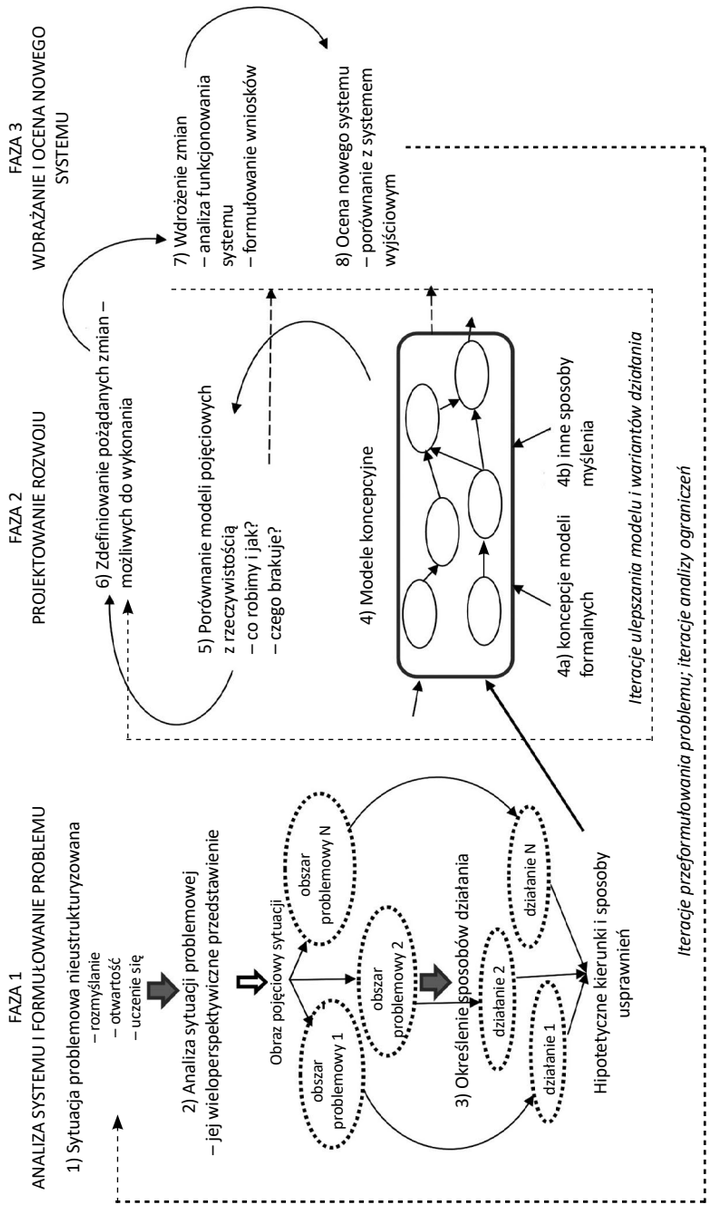
Podejście systemowe przejawia się w sposobie poznawczego patrzenia na naturę rzeczywistości bezpieczeństwa, który to sposób silnie związany jest z myśleniem systemowym i obejmuje fazy, etapy i czynności[18] (rysunek 2).

Faza pierwsza: analiza systemu
Na analizę systemu składają się trzy etapy: 1) stała analiza sytuacji, 2) formułowanie problemu/ów, 3) przedstawienie hipotetycznych sposobów ich rozwiązania.

W tej fazie analizuje się obecny stan systemu w celu uzyskania odpowiedzi na następujące pytania: Jakie są założenia i cele bezpieczeństwa systemu, realizowanych w systemie procesów oraz zaangażowanych w ich realizację zasobów? Jaka jest struktura systemu, jakie są jego elementy i relacje pomiędzy nimi? Jaka jest organizacja tych elementów, postrzeganych indywidualnie lub jako całość? Z jakich zasileń korzysta system, jakie są efekty ich przetwarzania oraz ograniczenia utrudniające ich przetwarzanie? Jak i w jakie wchodzą interakcje w systemie i środowisku? Jakie są granice systemu? Jakie są cele realizowanych procesów i ich przebiegi? W efekcie tej fazy badacz systemu może stwierdzić, jakie są rozbieżności między tym, co jest, a tym, co jest wymagane.

Etapy fazy pierwszej:
1. Stała analiza sytuacji – sytuacja nieustrukturyzowana
Cel tego etapu to systematyczne myślenie o sytuacji, analizowanie różnych jej aspektów, rozpoznawanie jej złożoności i bogactwa, a tym samym poszerzenie granic jej refleksyjnego doświadczania. Istotne są tu umiejętności aktywnej obserwacji, bezpośredniego doświadczania i wydobywania informacji z sytuacji, w której człowiek się znajduje, a także uczenia się traktowanego jako sposób pozyskiwania wiedzy pozwalającej na identyfikowanie zmian generujących sytuacyjne zagrożenia. Bardzo ważne jest też, aby być jak najbardziej otwartym na dopływające informacje i gromadzić je z uwzględnieniem różnych sytuacyjnych perspektyw oraz potrzeb bezpieczeństwa różnych stron. Obserwator powinien również posiadać umiejętności przenoszenia perspektyw pomiędzy potrzebami bezpieczeństwa różnych uczestników sytuacji, a tym samym – wspomagać ich proces uczenia się. Takie aktywne podejście do nadzorowania swoich sytuacji pozwala odpowiednio wcześnie zauważyć różnorakie symptomy informujące o rozwoju czy zmianach sytuacyjnych czynników mogących generować zagrożenia, których oddziaływanie jest dla systemu niebezpieczne.

[18] Opracowano na podstawie: S. Krim, *Applying Systems Approach to Educational-Organizational Change: Improvement of an Interdisciplinary Program: Master Program in Sustainable Development*, Uppasla University, 2009, s. 7–12.



Rysunek 2. Fazy, etapy i czynności podejścia systemowego

Źródło: opracowanie własne na podstawie: S. Karim, *Applying Systems Approach to Educational-Organizational Change: Improvement of an Interdisciplinary Program: Master Program in Sustainable Development*, Uppasla University, 2009, s. 8.

2. Zobrazowanie sytuacji problemowej
Celem jest opisanie i przedstawienie w różnych kombinacjach wyników analizy sytuacji problemowej, obrazujących te wszystkie czynniki, które motywują obserwatora/analityka do głębszego zainteresowania się nimi, by wypracować wytyczne i wskazówki do działania.

Podstawą poznawczą etapu drugiego są wyniki etapu pierwszego, prawidłowo prowadzonej analizy sytuacji oraz pojęciowe i definicyjne opracowanie sytuacji problemowej. To umożliwia badaczowi szybsze i dokładniejsze przedstawienie sytuacji problemowej, jej różnych aspektów, np. zlokalizowanie zachowań, procesów funkcjonalnych i procesów dysfunkcjonalnych, dewiacyjnych dla systemu. Wówczas łączy on w logiczną całość wszystkie informacje i różne perspektywy, tworząc bogaty obraz analizowanej sytuacji, który pokazuje jej elementy, ich znaczenia, związki i relacje pomiędzy nimi, szanse, zagrożenia, jej mocne i słabe strony. Taki rozbudowany obraz sytuacji stanowi bogate źródło informacji o niej, pozwalające dostrzegać jej złożoność, nadawać znaczenia jej elementom i wiążącym je relacjom. Dzięki temu badacz może ujawnić i sformułować ważne dla sytuacji tematy i zagadnienia, które stanowią problem (i są jego elementami), a które należy poddać analizom w dalszej pracy.

3. Opracowanie odpowiednich systemów działania
W tym etapie ważna jest umiejętność zdystansowania się od realnego świata, by zacząć myśleć abstrakcyjnie. Należy wówczas dla wybranych tematów-problemów wybierać z pojęciowo opisanej sytuacji te jej elementy i relacje między nimi (elementy kluczowe), które najlepiej obrazują problem i umożliwią wskazanie adekwatnych do określonych problemów kierunków działań i wyrażanie tych myśli-propozycji (motywów działania) w kategoriach systemowych. Wyrażenie tych motywów stanowi podstawę do modelowania koncepcyjnego, a w rzeczywistości jest zwartą wersją naszego zrozumienia sytuacji. Dla każdego z problemów – z myślą o rozwiązaniu sytuacji problemowej – badacz formułuje hipotezy o wynikach działania, które mogą uzdrowić sytuację poprzez przekształcenie obecnego systemu. Te hipotetyczne stwierdzenia stają się źródłem projektowania przez badacza bardziej szczegółowych systemów działania i modelowego ich przedstawienia. Omawiając te hipotezy z podmiotami sytuacji (interesariuszami), badacz dowiaduje się, co jest dla nich pożądane jako ulepszenie systemu i na czym powinien się koncentrować główny proces transformacji.

Faza druga: projektowanie rozwoju systemu
Teza: aktualna jest refleksja nad pytaniami dotyczącymi statusu modeli bezpieczeństwa: czym one są, do czego służą i jak je wykorzystywać w badaniach i praktyce?

Modelując, działamy intencjonalnie: wybieramy jedne elementy rzeczywistości bezpieczeństwa, a pomijamy inne, czyli z wielości możliwych rzeczy, zdarzeń czy cech opisujących daną rzeczywistość bezpieczeństwa świadomie wybieramy tylko te, które pozwalają posegregować i uporządkować w określony sposób zjawiska determinujące to bezpieczeństwo, dając skoordynowany jego obraz. Pojawiają się tutaj pytania: 1) co modelować – czyli czym jest rozważana sytuacja i podmiot bezpieczeństwa (obiekt zagrożony) w tej sytuacji, a czym jest jego otoczenie/kontekst?; 2) które elementy wybierać – czyli z jakich kluczowych elementów składa się sytuacja, jak

elementy te są powiązane i jak oddziałują na siebie i podmiot bezpieczeństwa?; 3) czy i jakie elementy otoczenia uwzględniać – jak sytuacja i podmiot bezpieczeństwa w tej sytuacji oddziałuje z otoczeniem? Odpowiedź na powyższe pytania wymaga działań poznawczych dających na nie wzajemnie spójne odpowiedzi.

Etapy fazy drugiej:
4. Opracowanie koncepcyjnych modeli bezpieczeństwa dla poprawy sytuacji
Model bezpieczeństwa jednostki, grupy czy organizacji postrzegać należy jako sposób opisu zagrażających bezpieczeństwu zjawisk i działań ukierunkowanych na ich eliminowanie. Wówczas posłużyć nam może jako narzędzie pośredniego poznania uwarunkowań bezpieczeństwa, dzięki z jednej strony uproszczeniu jego potencjalnej złożoności, a z drugiej – dzięki temu, że model taki jest analogiczny pod istotnymi względami wobec rzeczywistych uwarunkowań bezpieczeństwa i ich zmian, a przy tym jest poznawczo bardziej dostępny. Po ukształtowaniu hipotetycznych wizji rozważanej sytuacji zagrażającej oraz procesów transformacji (efekt fazy pierwszej) niezbędnych do ulepszania sytuacji (minimalizacji zagrożeń), badacz systemu zaczyna budować koncepcyjne modele działań, które będą realizowane w celu urzeczywistnienia każdego z procesów transformacji. Punktem wyjścia jest zdefiniowanie zakresu modelu przedstawiającego zagrożenie i działania ukierunkowane na jego eliminowanie. Wiąże się to ze zrozumieniem tego, co chce się osiągnąć, i wymaga stworzenia palety jednoznacznych wyborów kierunków działania. Kojarząc te działania z oczekiwanymi efektami, można uchwycić logikę przyczynowo-skutkową, którą ma przedstawiać model. W tym celu wykorzystuje się badania symulacyjne. Wymagają one stosowania skutecznych metod budowy modelu, jego weryfikacji i walidacji. Modele są podstawą do symulacji, czyli wirtualnego badania i przekształcania rzeczywistości. W poznawaniu systemów złożonych (złożoność szczegółowa i złożoność dynamiczna), symulacja przez swą zdolność manipulacji czasoprzestrzenią jest jedynym narzędziem pozwalającym ująć i zrozumieć przyczynowo-skutkowe powiązania odległe w czasie i w przestrzeni, z wieloma sprzężeniami zwrotnymi.

Wybory i działania są od siebie wzajemnie uzależnione i powiązane pętlami przyczynowo-skutkowymi, a to pomaga zilustrować wpływ każdego działania w kontekście jego przyczyniania się do rozwiązania problemu zagrożeń. Wówczas model taki pomaga objaśniać czynniki i wzajemne relacje między nimi, które mają lub mogą mieć wpływ na poziom bezpieczeństwa podmiotu i zmiany tego poziomu. W modelu bezpieczeństwa bezpieczeństwo jest zmienną endogeniczną (wyjaśnianą przez model), podlega ono wpływowi innych zmiennych/czynników zarówno endogenicznych, jak i egzogenicznych. Modele zaprojektowane na tym etapie nie są planowane do wdrożenia, ale stanowią podstawę do porównania z rzeczywistą sytuacją i mają zachęcać do dalszych dyskusji nad sposobami działania wśród zainteresowanych stron.

5. Porównanie modeli pojęciowych z rzeczywistością
Dysponując konceptualnymi modelami transformacyjnego działania ukierunkowanego na poprawianie zagrażającej sytuacji, badacz musi skonfrontować modele koncepcyjne z rzeczywistą sytuacją, aby odróżnić rzeczywistość od abstrakcyjnego myślenia. W tym celu można zadać pewne pytania, na przykład: 1) które z działań są

obecnie realizowane, jaki jest ich przebieg i skutki?; 2) jakich działań brakuje i dlaczego? 3) kto monitoruje aktywności podmiotów w sytuacji? od jakiego czasu? 4) w jakim celu wykorzystuje zgromadzone informacje?

6. Identyfikacja pożądanych i możliwych do wykonania zmian
Na tym etapie należy starannie przeanalizować naturę, przyczyny, środki, przeszkody i konsekwencje zmiany. W ten sposób badacz może określić, które z zaproponowanych działań opracowanych za pomocą modelu są najbardziej pożądane, bo mogą zagwarantować rozwiązanie problemu, a jednocześnie są wykonalne pod względem dostępności zasobów i występujących ograniczeń środowiskowych.

Faza trzecia: wdrażanie i ocena nowego systemu
Wdrożenie i ocena funkcjonowania systemu bezpieczeństwa organizacji stanowi podstawę do jego dalszego rozwijania i doskonalenia.

7. Wdrożenie zmian eliminujących zagrożenie
Po porównaniu wariantów działania i ocenie pozytywnych i negatywnych skutków każdego z wariantów, dysponujemy planem składającym się z konkretnych zapisów, które określają sposoby możliwych do wykonania działań. Jest to stosowny czas na ich wdrożenie. W planie należy też uwzględnić metody oraz wskaźniki postępów. Niemniej jednak nie jest to koniec procesu; każda zmiana w systemie tworzy inny system, który musi być monitorowany i utrzymywany. Czasem poziom poprawy jest niewystarczający lub nowa sytuacja może wywołać nowe poczucie niezadowolenia i konfliktu. Dlatego kolejny cykl działania musi być powtarzany. Poprawienie sytuacji (w przeciwieństwie do rozwiązania problemu) jest procesem stopniowym i powtarzalnym.

8. Ocena nowego systemu – porównanie z systemem wyjściowym
Stwierdzono, że przechodzenie przez cykle podejścia systemowego zwiększa wiedzę badacza i interesariuszy o zagrażającej sytuacji, a także o roli różnych czynników z sytuacją związanych. W rzeczywistości skuteczność podejścia systemowego jest powiązana z procesem uczenia się, który odbywa się podczas iteracji. W tym etapie ocenić należy, czy związek pomiędzy sytuacją a uczeniem się jest na tyle efektywny, że pozwala na skuteczne działania w danej sytuacji.

Podsumowanie

Myślenie i podejście systemowe w odniesieniu do problemów bezpieczeństwa organizacji pozwala badaczowi/analitykowi:

- zidentyfikować sytuację zagrażającą i przedstawić ją w kategoriach systemu – który jest tu traktowany jako jednorodny, celowy i otwarty, składający się z wzajemnie powiązanych części tworzących pewną całość wyróżniającą się w otoczeniu – czyli określić jego granice, wyodrębnić i scharakteryzować części/elementy oraz relacje wiążące części systemu i sam system z otoczeniem, tworząc reprezentację swojego postrzegania systemu, rozumienia swego i innych miejsca w tym systemie;

- zrozumieć wagę i wpływ elementów sytuacji zagrażającej na bezpieczne funkcjonowanie systemu, którego działania powinny być ukierunkowane na przetrwanie i rozwój. To pozwala określić warunki wewnętrznej siły i zwartości systemu oraz potrzebnych umiejętności wyszukiwania oraz wykorzystania zasobów niezbędnych do integralności i rozwoju systemu, do utrzymania i umacniania swojej pozycji w otoczeniu – czyli opisać i ocenić stan istniejącego systemu, jego części składowe i relacje między nimi i ich właściwościami, zakres i poziom realizowanych procesów i wykonywanych zadań oraz podmiotową rolę człowieka w ich wykonaniu;
- określić/sformułować problem lub problemy występujące w systemie – skompletować wiedzę o systemie i jego otoczeniu w różny sposób związaną z jego funkcjonowaniem i przetworzyć ją do postaci wskazującej na potrzebę rozwoju, doskonalenia systemu – co pozwoli zmienić stan początkowy/istniejący, który jest niezadowalający, na stan zadowalający;
- wskazać możliwe sposoby rozwiązania problemu – poprzez kreowanie wizerunku pożądanego stanu systemu i systemowe projektowanie uwzględniające zarówno obecny stan systemu, jak i jego przyszłe cele, charakterystyczne cechy, wymagane funkcje, które system ma pełnić – czyli przedstawić projekt struktury i funkcjonowania nowego systemu, zmniejszający złożoność, redukujący niepotrzebne role, poprawiający właściwości i usprawniający działania.

Bibliografia

Banathy B.H., *Projektowanie systemów edukacji. Podróże w przyszłość*, tłum. M. Bazewicz, Wrocław 1994.

Beer S., *Cybernetyka a zarządzanie*, tłum. Ś. Sorokowski, Warszawa 1966.

Gasparski W., *Pojęcie systemu. Z zagadnień metodologii badań i projektowania systemowego*, [w:] *Projektowanie maszyn i systemów cyfrowych*, red. A. Michalski, Warszawa 1972.

Habr J., Vepřek J., *Systemowa analiza i synteza. Nowoczesne podejście do zarządzania i podejmowania decyzji*, tłum. A. Kusto, Warszawa 1976.

Hatch M.J., *Teoria organizacji*, tłum. P. Łuków, Warszawa 2002.

Jankowski B., *Modelowanie rozwoju krajowego systemu energetycznego z uwzględnieniem wymagań stabilizacji i redukcji emisji dwutlenku węgla w Polsce*, Warszawa 1997.

Józefik B., *Rozwój myślenia systemowego a terapia rodzin*, [w:] *Ewolucja myślenia systemowego w terapii rodzin. Od metafory cybernetycznej do dialogu i narracji*, red. L. Górniak, B. Józefik, Kraków 2003.

Karim S., *Applying Systems Approach to Educational-Organizational Change: Improvement of an Interdisciplinary Program: Master Program in Sustainable Development*, Uppasla University, 2009.

Kozielecki J., *Człowiek wielowymiarowy*, Warszawa 1996.

Kozielecki J., *Koncepcje psychologiczne człowieka*, Warszawa 1996.

Koźmiński A.K., *Analiza systemowa organizacji*, Warszawa 1976.

Koźmiński A.K., *Ujęcie systemowe*, [w:] *Współczesne teorie organizacji*, red. A.K. Koźmiński, Warszawa 1983.

Lubański M., *Informacja – system*, [w:] *Zagadnienia filozoficzne współczesnej nauki. Wstęp do filozofii przyrody*, red. M. Heller, M. Lubański, S.W. Ślaga, Warszawa 1997.
Morawski J.M., *Dominanty ujęć systemowych*, [w:] *Wybrane problemy metodologii badań na potrzeby sportu*, red. J.M. Morawski, Warszawa 2002.
Perechuda K., *Organizacja wirtualna*, Wrocław 1997.
Pluta J., *Społeczno-kulturowe procesy definiowania postaw*, Wrocław 2002.
Rummler G.A., Brache A.P., *Podnoszenie efektywności organizacji. Jak zarządzać „białymi plamami" w strukturze organizacyjnej?*, tłum. T. Ludwicki, Warszawa 2000.
Senge P.M., *Piąta dyscyplina. Teoria i praktyka organizacji uczących się*, tłum. M. Lipa, Warszawa 1998.
Sharma M., *System Approach: An Inter-disciplinary Effort*, [w:] *System Approach: Its Application in Education*, red. M. Sharma, Bombay 1985.
Syrek-Kosowska A., *„A jeśli nic nie jest pewne?". Perspektywa złożoności – nowe wyzwania coachingu*, [w:] *Myślenie systemowe w coachingu*, red. K. Ramirez-Cyzio, Warszawa 2013.
Tomaszewski T., *Człowiek i otoczenie*, [w:] *Psychologia*, red. T. Tomaszewski, Warszawa 1976.
Zych B., *Myślenie systemowe – podstawowe zasady w pracy coacha*, [w:] *Myślenie systemowe w coachingu*, red. K. Ramirez-Cyzio, Warszawa 2013.

Podejście systemowe w badaniach bezpieczeństwa organizacji
Streszczenie

W pracy skoncentrowano się na możliwości wykorzystania założeń teorii systemów do badania zjawisk bezpieczeństwa. Przyjęto następujące założenia: 1) myślenie i podejście systemowe jest wysoce użyteczną poznawczo metodologią badania zjawisk i procesów bezpieczeństwa i jego zagrożeń charakteryzujących się szczególnym poziomem złożoności, a także budowania teorii wyjaśniających; 2) podejście systemowe jest skutecznym narzędziem tworzenia procedur interpretujących procesy i zjawiska bezpieczeństwa i jego zagrożeń, umożliwiającym charakterystykę ich genezy, struktur, zakresu i skutków oddziaływania, uwarunkowań zewnętrznych i wewnętrznych, a także przedsięwzięć mających na celu zapewnienie pożądanego ich poziomu.
Słowa kluczowe: system, bezpieczeństwo, podejście systemowe, myślenie systemowe, model systemu bezpieczeństwa

System Approach in the Research into Organisational Security
Abstract

The work focuses on the possibility of using the assumptions of system theories to study security phenomena. It was assumed that 1) system thinking and system approach is a cognitively useful methodology of considerable value for studying the processes and phenomena related to security and its threats, characterised by a particular level of complexity and building explanatory theories; 2) the system approach is an effective tool for creating procedures that interpret security processes and phenomena and its threats, enabling characterization of their genesis, structures, scope and impact, external and internal conditions, as well as projects aimed at ensuring their desired level.
Key words: system, security, system approach, system thinking, security system model

Systematischer Ansatz in der Forschung der Organisationssicherheit
Zusammefassung

In diesem Artikel hat man sich auf die Möglichkeiten der Nutzung der Voraussetzungen der Systemtheorie zur Forschung der Sicherheitsphänomene konzentriert. Man hat folgende Voraussetzungen angenommen: 1) Systemdenken und Systemansatz ist eine kognitiv sehr nützliche Methodologie für Forschung der Sicherheitsphänomene und Sicherheitsprozesse und ihrer Risiken, die sich durch ein besonderes Komplexitätsniveau kennzeichnen, als auch Aufbauen der Theorien zur Erklärung; 2) der Systemansatz ist ein wirksames Instrument zur Schaffung der Verfahren zur Auslegung der Sicherheitsprozesse und Sicherheitserscheinungen und ihrer Risiken, ermöglicht Beschreibung ihrer Genese, ihrer Strukturen, ihres Bereichs und Auswirkungen, der Außen- und Innenbedingungen, als auch der Maßnahmen, die Gewährleistung ihres entsprechenden Niveaus zum Ziel haben.
Schlüsselwörter: System, Sicherheit, Systemansatz, Systemdenken, Sicherheitssystemmodell

Системный подход в исследованиях безопасности организации
Резюме

В статье рассмотрены возможности использования принципов теории систем для исследования явлений безопасности. Приняты следующие концепции: 1) мышление и системный подход являются полезной, когнитивной методологией исследования явлений и процессов безопасности и угроз безопасности, отличающейся особым уровнем сложности, а также предоставляющей возможность построения объясняющих теорий; 2) системный подход является эффективным инструментом создания процедур, объясняющих процессы и явления безопасности и угроз безопасности, позволяющих дать характеристику их происхождения, структур, масштабов и последствий воздействия, внешних и внутренних условий, а также действий, направленных на обеспечение желаемого уровня безопасности.
Ключевые слова: система, безопасность, системный подход, системное мышление, модель системы безопасности

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-002

Andrzej Chodyński

prof. dr hab., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0003-4962-5143

Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja *smart*

Wprowadzenie

Korzystanie z dorobku nauk o zarządzaniu w działaniach praktycznych na rzecz organizacji niekomercyjnych często dotyczy koncepcji, metod i technik zarządzania. Nie może odbywać się to w sposób bezrefleksyjny, ze względu na różnice w zarządzaniu organizacją niekomercyjną (np. miastem) i organizacją komercyjną. Przede wszystkim miasto jest nastawione na realizacje celów społecznych (zaspokajanie potrzeb mieszkańców), a firma jest nastawiona na cele ekonomiczne – choć z coraz wyraźniej zaznaczająca się rolą aspektów społecznych. Według Tadeusza Markowskiego zarządzanie ogólne miastem obejmuje sformułowanie polityki miasta wraz z celami i zadaniami strategicznymi, wdrożenie tej polityki do realizacji oraz koordynację, kontrolę i ocenę podmiotów, realizatorów zadań miasta[1]. Zarządzanie miastem, nastawione na osiąganie celów rozwojowych, odnosi się do wywierania wpływu na hierarchię i systemy wartości, interesy, ale także dążenia i postawy oraz zachowania organizacyjne dotyczące podmiotu samorządu terytorialnego. Podmiotem tym jest społeczność miasta[2]. Michał Kudłacz i Paulina Mazur-Kurach zwracają uwagę, że nadrzędnym celem administracji samorządowej jest poprawa jakości życia mieszkańców,

[1] T. Markowski, *Zarządzanie rozwojem miast*, Warszawa 1999.

[2] J. Szołtysek, R. Otręba, *Zarządzanie miastem i jego wpływ na jakość życia mieszkańców miast województwa śląskiego – doniesienie badawcze*, „Problemy Rozwoju Miast. Kwartalnik Naukowy Instytutu Rozwoju Miast" 2015, R. XII, z. 2, s. 37–42.

z uwzględnieniem konkurencyjności terytorialnej (atrakcyjności lokalizacyjnej). W ramach modernizacji systemu zarządzania miastem proponuje się wykorzystanie koncepcji organizacji inteligentnej[3]. Wykorzystywane w organizacjach komercyjnych współczesne (i nowoczesne) koncepcje zarządzania, jak koncepcja kapitału intelektualnego organizacji, są rozpatrywane także dla miast. W tym przypadku uwzględniane są także kwestie bezpieczeństwa, np. w obszarze procesów odnoszą się one do przeciętnego czasu odpowiedzi policji i straży pożarnej, przeciętnego czasu oczekiwania na karetkę pogotowia, przeciętnego czasu dojazdu karetki do szpitala czy rocznej liczby przestępstw na jednego mieszkańca. Wymieniane są też tak istotne dla koncepcji *smart city* (miasta inteligentnego) wskaźniki związane z technologiami informacyjnymi[4]. Podnoszone są kwestie wykorzystania w zarządzaniu miastem koncepcji organizacji uczących się czy inteligentnych, stanowiących podstawę do tworzenia firm i miast o charakterze *smart.* W koncepcji tej można doszukać się także aspektów związanych z bezpieczeństwem[5]. Miasto można traktować jako organizację uczącą się[6].

Występuje pogląd, że podstawą zarządzania miastem powinny być trzy główne koncepcje, w oparciu o występujące realne (rzeczywiste) i rozwijające się wirtualne sieci interesariuszy: rozwój zintegrowany, zarządzanie strategiczne i zarządzanie zmianą (w tym procesy rewitalizacji i restrukturyzacji)[7]. Miasto można rozpatrywać w ujęciu systemowym ze względu na fakt, że spełnia ono warunki ujęcia całościowego przedmiotu badań, funkcjonalności i celowościowego (teleologicznego) charakteru zachowań. Funkcjonalność systemu wiąże się z siecią relacji miedzy jego elementami. Biorąc pod uwagę dwa charakterystyczne modele systemów: mechanistyczny (gdzie wzorcem jest maszyna) oraz organistyczny (gdzie wzorcem jest organizm), wydaje się, że miasto jest bliższe temu drugiemu. W ujęciu systemowym miasto można rozpatrywać jako terytorialny system społeczny (ujęcie społeczno-ekonomiczne), jako ekosystem (ujęcie ekologiczne) oraz system organiczny (ujęcie organistyczne). Miasto stanowi przedmiot multidyscyplinarnych badań naukowych[8]. Miasto ma cechy organizacji – zgodnie z definicją organizacji jako otwartego systemu społeczno-technicznego, o określonej strukturze i zorientowanego celowo. Działa w określonym otoczeniu, a celem tego działania jest realizacja interesu publicznego[9]. System miasta składa się z podsystemów: przestrzennego, gospodarczego i społecznego. Podstawę rozwoju gospodarczego stanowią funkcje miast – o charakterze

[3] M. Kudłacz, P. Mazur-Kurach, *Formy zarządzania publicznego w kontekście rozwoju miast w Polsce*, „Zarządzanie Publiczne" 2015, nr 4 (34), s. 50–65.

[4] L. Edvinsson, M.S. Malone, *Kapitał intelektualny*, tłum. M. Marcinkowska, Warszawa 2001, s. 139–140.

[5] T. Markowski, *op. cit*.

[6] B. Rożałowska, M. Macełko, *Miasto jako organizacja ucząca się. O znaczeniu idei inteligentnego miasta (obywatela) w społeczeństwie informacyjnym*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2015, z. 79, s. 271–283.

[7] K. Wrana, T. Kmieć, B. Kmieć, *Zarządzanie miastem w chmurze – cloud city*, [w:] *Partnerstwo i odpowiedzialność w funkcjonowaniu miasta*, red. T. Markowski, D. Stawasz, Warszawa 2014 , s. 91–104.

[8] J.J. Parysek, *Miasto w ujęciu systemowym*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2015, R. LXXVII, z. 1, s. 27–53.

[9] D. Stawasz, D. Sikora-Fernandez, *Koncepcja* smart city *na tle procesów i uwarunkowań rozwoju współczesnych miast*, Łódź 2016, s. 26–27.

działalności przemysłowej, usługowej, handlowej, transportowej, finansowej kulturalnej i administracyjnej. Strukturę społeczną miasta stanowi układ relacji pomiędzy poszczególnymi elementami społecznej zbiorowości miejskiej, który odnosi się do takich kwestii jak rozwój gospodarczy, zasoby siły roboczej, specjalizacja miasta, dostępność do edukacji (także wyższej), tożsamość lokalna wraz poczuciem przynależności oraz zdolność adaptacji do przestrzeni miasta[10]. Problematyka bezpieczeństwa w przedsiębiorstwach pojawia się w ramach przyjętych wartości organizacyjnych[11], zaś w odniesieniu do zarządzania miastem aspekt ten jest wyraźnie artykułowany w rozwiązaniach zarządzania publicznego[12].

Hipoteza: Poziom bezpieczeństwa miast może być podniesiony poprzez wykorzystanie metod i narzędzi zarządzania opartych na koncepcji organizacji inteligentnej.

Celem opracowania jest określenie praktycznych możliwości wykorzystania narzędzi zarządzania stosowanych w organizacjach komercyjnych na rzecz zarządzania miastem inteligentnym. Przedmiot badań stanowi miasto jako organizacja o określonym poziomie bezpieczeństwa.

Koncepcja *smart city* (miasta inteligentnego) a bezpieczeństwo

Organizacja inteligentna (*smart organization*) w kontekście pozyskiwanej wiedzy i zmian w otoczeniu zewnętrznym płynnie modyfikuje swoje zachowania, z wykorzystaniem rozwiniętych systemów informatycznych[13]. Stanowi organizację elastyczną, wyłapującą słabe sygnały z otoczenia. Dysponuje wysokim kapitałem intelektualnym. Adaptuje się do otoczenia lepiej niż organizacja ucząca się – wyprzedza zmiany w otoczeniu, a nawet je kształtuje[14]. Organizacja inteligentna kojarzona jest z inteligentnym zarządzaniem (*smart management*)[15]. *Smart organization* to organizacja gotowa do zmian, elastyczna, zdolna do adaptacji do zmiennego środowiska przez ciągły i dynamiczny proces uczenia się, treningu (*training*) i ciągłego rozwoju pracowników. Współcześnie *smart organization* wykorzystuje zasoby, by stać się lepszą, szybszą,

[10] *Ibidem*, s. 14–16.

[11] A. Chodyński, *Wpływ wspólnych wartości na zjawisko izomorfizmu organizacyjnego*, [w:] *Zarządzanie nowoczesną organizacją*, red. O. Grabiec, Sosnowiec 2018, s. 9–29.

[12] W strukturze zarządzania bezpieczeństwem publicznym występują podmioty uczestniczące w procesie zarządzania bezpieczeństwem publicznym, w tym samorząd terytorialny, zob. A. Kożuch *et al.*, *Obszary zarządzania publicznego*, Kraków 2016, s. 122–136 (Monografie i Studia Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego).

[13] P. Kordel *et al.*, *Inteligentne organizacje – zarządzanie wiedzą i kompetencjami pracowników*, Warszawa 2010.

[14] S. Łobejko, *Trendy rozwojowe inteligentnych organizacji w globalnej gospodarce*, PARP, Warszawa 2009, https://www.parp.gov.pl/storage/publications/pdf/2009_trendy_rozwojowe_lobejko.pdf [dostęp: 15.01.2018].

[15] D. Matheson. J. Matheson, *The Smart Organization: Creating Value Through Strategic R&D*, Boston, 1998. s. 261, [za:] J. Woźniak, *The Negative Implications of Offshoring and Strategic Economic Security of Business Organizations*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie" 2015, nr 104, s. 235–253.

inteligentniejszą (*smarter*), bardziej rygorystyczną (*rigorous*) w wielu kluczowych aktywnościach i wykorzystuje technologie, aby przewodzić w realizowanych aktywnościach i procesach. W istotnych dla organizacji typu *smart* elementach, tj. dotyczących strategii, struktury, procesów, pracowników i wynagradzania, proponuje się wprowadzanie zmian[16]. Pojęcie *smart* w odniesieniu do organizacji inteligentnej – w tym przedsiębiorstwa – oznacza działania: S – sprytne (dotyczy kombinacyjności w działaniu), M – mądre (wprowadzające nowe koncepcje, metody i techniki zarządzania w sposób twórczy), A – apolityczne (lub *agile*, w oparciu o trwałe wartości), R – rozwojowe (dające przedsiębiorstwu możliwość rozwoju), T – technologicznie zaawansowane (realizujące współczesne technologie nie tylko w wymiarze inżynierskim, ale także społecznym i organizacyjnym)[17]. Akronim SMART jest też rozwijany jako: S – *simple* (prosty), M – *measurable* (mierzalny), A – *achievable* (osiągalny), R – *relevant* (trafny), T – *timetable* (osiągalny w czasie)[18].

Koncepcja *smart city* zmierza w kierunku rozwoju zrównoważonego. Miasto to złożony system społeczno-gospodarczy o charakterze otwartym. Miasto inteligentne to miasto zaawansowane technologicznie. Istotną rolę odgrywają w nim zaawansowane technologie informacyjne i komunikacyjne (ICT), związane z koncepcją gospodarki opartej na wiedzy. Przegląd różnych poglądów wskazuje że:

- *Smart city* jako terytorium cechuje wysoka zdolność uczenia się, innowacyjność, kreatywność, występowanie instytucji prowadzących prace badawczo rozwojowe (B+R), szkolnictwa wyższego, infrastruktury cyfrowej oraz technologii komunikacyjnych. Odznacza się wysoką sprawnością zarządzania.
- Miasto inteligentne optymalizuje dostępne i nowe zasoby i możliwe inwestycje, zaś wsparcie przy użyciu zaawansowanych technologii informacyjnych i komunikacyjnych dotyczy głównie energetyki, infrastruktury technicznej, gospodarki odpadami, transportu oraz bezpieczeństwa.
- W Unii Europejskiej w ramach koncepcji *smart city* kładzie się nacisk na czystą energię, jej oszczędne zużycie i ograniczenie emisji dwutlenku węgla. W USA nacisk kładziony jest na kapitał ludzki i społeczny, infrastrukturę komunikacyjną (transport i technologie komunikacyjne), a w aspekcie rozwoju zrównoważonego – na lepszą jakość życia i wykorzystanie rządzenia partycypacyjnego. Australia eksponuje przemysły kreatywne i media cyfrowe. Koncepcja miasta inteligentnego uwzględnia inteligentny system transportu, kapitał społeczny, jakość życia, system zarządzania w mieście, gospodarkę i dbałość o środowisko naturalne[19].

[16] S. Lazarević, J. Lukić, *Building Smart Organization Through Learning, and Development of Employees*, [w:] *Creative Education for Employment Growth*, International Conference: Employment, Education and Entrepreneurship, 14–16 October 2015, Belgrade, Serbia, s. 256–268.

[17] G. Gierszewska, *Czy inteligentne przedsiębiorstwa to już teraźniejszość czy mglista przyszłość?*, [w:] *Co dalej z zarządzaniem?*, red. G. Gierszewska, Warszawa 2018, s. 34–61.

[18] J. Martyniuk-Pęczek, T. Parteka, O. Martyniuk, *Idea* smart city *w kontekście rozwoju przedsiębiorczości na przedmieściach*, „Biuletyn KPZK" (Komitet Przestrzennego Zagospodarowania Kraju, PAN) 2015, nr 257–258, s. 119–143.

[19] D. Sikora-Fernandez, *Koncepcja „smart city" w założeniach polityki rozwoju miasta – polska perspektywa*, „Acta Universitatis Lodziensis, Folia Oeconomica" 2013, nr 290, s. 83–94.

Dorota Stawasz i Dorota Sikora-Fernandez w odniesieniu do miast prezentują następujące pojęcia:

- miasta inteligentne – budowane w oparciu o dorobek gospodarki opartej na wiedzy, innowacjach i społeczeństwie cyfrowym;
- miasta zrównoważone – oparte na efektywnym wykorzystaniu zasobów, przy zachowaniu konkurencyjności i przyjazności dla środowiska naturalnego, związane z koncepcją *sustainability* w zarządzaniu.

Definicje *smart city* odnoszą się m.in. do następujących pojęć:

- miasto inteligentne, inwestujące w kapitał ludzki i społeczny oraz infrastrukturę komunikacyjną, cechujące się zrównoważonym wzrostem gospodarczym i wysoką jakością życia, mądrym zarządzaniem zasobami naturalnymi i zarządzaniem partycypacyjnym;
- miasto integrujące funkcjonowanie infrastruktury krytycznej dla optymalizacji zasobów, maksymalizujące usługi dla obywateli[20];
- miasto kreujące dystrybucję bogactwa, inwestujące w infrastrukturę, redukujące biedę i wykluczenie społeczne;
- miasto oparte na współpracy sektora publicznego i prywatnego (*smart sustainable city*);
- miasto wykorzystujące współpracę wielu gmin, korzystające z technologii (w szczególności informacyjno-komunikacyjnych) na rzecz konkurencyjności i zrównoważonej przyszłości, opierające się na symbiotycznym połączeniu sieci ludzi, firm, infrastruktury, konsumpcji, energii, przestrzeni i technologii (*smart sustainable city*)[21].

Wskazuje się następujące wymiary *smart city*: 1) konkurencyjność (*smart economy*) – ocenianą poprzez produktywność i przedsiębiorczość miast oraz ich innowacyjność; 2) transport i ICT (*smart mobility*) – transport powinien rozwijać się w sposób innowacyjny, zrównoważony i bezpieczny, także poza granicami miasta; 3) środowisko, zasoby naturalne (*smart environment*) – dotyczące atrakcyjności stanu środowiska naturalnego, ochrony tego środowiska i zrównoważonego zarządzania zasobami naturalnymi; 4) ludzie jako kapitał (*smart people*) – opisywany przez kreatywność, uczenie się i kwalifikacje, otwartość, różnorodność i partycypację w życiu społecznym; 5) jakość życia (*smart living*) – odnoszącą się do zdrowia i bezpieczeństwa mieszkańców, edukacji, atrakcyjności turystycznej, spójności społecznej oraz atrakcyjności obiektów kulturalnych, 6) zarządzanie (*smart governance*) – w tym transparentność w zarządzaniu, uspołecznienie rozwoju, strategie zarządzania perspektywami rozwojowymi (wraz z realizacją strategii rozwoju), strategie polityczne, partycypacja społeczna (która może dotyczyć również kwestii bezpieczeństwa), wysoki poziom usług publicznych.

W ramach projektu *European Smart Cities* zaproponowano pomiar „inteligencji miejskiej". Do sześciu wymiarów przyporządkowano 33 czynniki wraz z miernikami[22].

[20] Kwestia infrastruktury krytycznej ma szczególne znaczenie z punktu widzenia bezpieczeństwa.

[21] European Parliament, *Mapping Smart Cities in the UE*, Brussels 2014.

[22] D. Stawasz, D. Sikora-Fernandez, *op. cit.*, s. 80–86. W literaturze przedmiotu *smart economy*, *smart people*, *smart governance*, *smart mobility*, *smart environment* i *smart living* są tłumaczone na język polski odpowiednio jako: gospodarka, kapitał ludzki i społeczny, współwspółrządzenie, transport i technologie informacyjno-komunikacyjne, środowisko naturalne oraz jakość życia, zob. *ibidem*.

Są nimi:

1) dla *smart economy*: duch innowacyjny, przedsiębiorczość, gospodarczy wizerunek i znaki handlowe, produktywność, elastyczność rynku pracy, współpraca międzynarodowa;
2) dla *smart mobility*: lokalna dostępność transportowa, krajowa i międzynarodowa dostępność transportowa, dostępność infrastruktury ICT oraz sustensywne, innowacyjne i bezpieczne systemy transportowe (w tym zielona mobilność);
3) dla *smart environment*: atrakcyjność warunków naturalnych, zanieczyszczenie środowiska, ochrona środowiska, zrównoważone podejście do zarządzania zasobami naturalnymi;
4) dla *smart people*: poziom kwalifikacji, zdolność podejmowania kształcenia przez całe życie, społeczny i etniczny pluralizm, elastyczność, kreatywność, orientacja kosmopolityczna, uczestnictwo w życiu publicznym;
5) dla *smart living*: obiekty kultury, warunki zdrowotne, bezpieczeństwo osobiste (m.in. poziom przestępczości, liczba zgonów w wyniku napaści, poziom zadowolenia z osobistego bezpieczeństwa), jakość zasobu mieszkaniowego, obiekty edukacyjne, atrakcyjność turystyczna, spójność społeczna (m.in. odsetek osób biednych) oraz percepcja osobistego ryzyka popadnięcia w biedę. Wskazuje się na rolę *crowdsourcingu* w miastach (określanego jako *citizensourcing*)[23].
6) dla *smart governance*: uczestnictwo w procesach podejmowania decyzji, usługi publiczne i społeczne, przejrzystość form rządzenia[24].

Warto zwrócić uwagę, że wśród wymiarów miasta inteligentnego według projektu *European Smart Cities*, przy opisie rozszerzonym przez dorobek literatury przedmiotu pojawiają się także: w zakresie *smart economy* – m.in. wydatki na B&R, zaś dla *smart people* – kreatywność mierzona zatrudnieniem w sektorach kreatywnych[25].

W rankingu miast w świecie według Forbes (*The Smartest Cities In The World For 2017*) na czele znajduje się Nowy Jork. Dla Londynu (drugie miejsce) podkreśla się m.in. rolę kapitału ludzkiego. Można to powiązać z oceną kapitału intelektualnego miasta (kapitał ludzki jako jeden z elementów składowych kapitału intelektualnego). Ranking Easy Park 2017 powstał według następujących kryteriów: 1) transport i mobilność; 2) *sustainability* (w tym korzystanie z czystych źródeł energii, występowanie inteligentnych, pasywnych budynków, zarządzanie odpadami, polityka ochrony środowiska); 3) zarządzanie miastem (w tym partycypacja obywatelska, procesy cyfryzacji w zarządzaniu); 4) innowacyjność miasta; 5) standard życia mieszkańców; 6) cyfryzacja miasta (głównie dostęp do internetu), 7) perspektywy rozwoju. Np. w strategii *smart city* dla Wiednia jako cele przyjęto obniżenie emisji gazów cieplarnianych w przeliczeniu na jednego mieszkańca i osiągnięcie określonego udziału energii ze źródeł odnawialnych do roku 2030[26]. Z kolei w ramach tworzenia (z wykorzystaniem konsultacji społecznych) strategii dla Gdańska

[23] A. Sobol, *Inteligentne miasta versus zrównoważone miasta*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 320, s. 75–86.

[24] Właściwszym terminem niż „rządzenie" byłoby „zarządzanie".

[25] D. Stawasz, D. Sikora-Fernandez, *op. cit.*, s. 80–86.

[26] Przyjęte wskaźniki mogą być wykorzystane w konstrukcji Strategicznej Karty Wyników dla zarządzania miastem.

przyjęto 5 obszarów strategicznych: mieszkańcy, kształcenie, współpraca, mobilność i otwartość. Za tym idą plany operacyjne[27].

Jako wymiary *smart city* wskazuje się: inteligentną gospodarkę (opartą na wiedzy, z udziałem rozwiązań innowacyjnych), mobilność (inteligentny system transportu i komunikacji, optymalizacja systemu ruchu drogowego), inteligentne środowisko (optymalizacja zużycia energii, wykorzystanie energii odnawialnej, zmniejszenie emisji dwutlenku węgla, edukacja ekologiczna), inteligentnych ludzi (społeczeństwo uczące się, inicjowanie zmian przez mieszkańców), jakość życia (poziom i warunki życia, dostęp do usług publicznych, poziom opieki zdrowotnej, dostęp do infrastruktury technicznej i społecznej), inteligentne rządzenie (współrządzenie i współpraca między użytkownikami miasta w ramach systemu zarządzania miastem, wykorzystanie w tym zakresie procedur i nowoczesnych technologii). Elementami miasta inteligentnego są: gospodarka oparta na wiedzy, technologie informacyjno-komunikacyjne (ICT), zrównoważony rozwój, kapitał społeczny, współrządzenie i jakość życia. W ramach inteligentnego systemu zapewnienia bezpieczeństwa publicznego znacząca rolę odgrywa video monitoring, wykorzystanie technologii informacyjnych w komunikacji z mieszkańcami oraz efektywne zarządzanie kryzysowe, w tym powiadamianie o sytuacjach kryzysowych (np. z wykorzystaniem SMS) czy automatyczne nadawanie komunikatów (np. przez telewizję). Podkreśla się rolę inteligentnej administracji, korzystającej z zaawansowanych technologii informacyjnych (telekomunikacyjnych) w kontaktach zewnętrznych i wewnętrznych (np. obsługa elektroniczna klientów)[28]. Miasto inteligentne wykazuje wysoki poziom odporności miejskiej (*city resilience*), co pozwala na szybszą i lepszą reakcję na sytuacje kryzysowe[29].

Miasto inteligentne a miasto zrównoważone – aspekt bezpieczeństwa

W literaturze pojęcie *smart city* jest różnie interpretowane: jako wiązanie zagadnień społecznych, ekologicznych i ekonomicznych lub jako współczesna wersja miasta zrównoważonego (*sustainable city*). Pojęcie inteligentnych miast zrównoważonych (*smart sustainable cities*, SSC) uwzględnia klasyczne podejście do zrównoważonego rozwoju, w myśl którego rozwój wspierają nowoczesne technologie, zaspokajające potrzeby mieszkańców bez zmniejszania szans rozwoju przyszłych pokoleń. Zrównoważony rozwój to rozwój harmonijny, którego celem jest poprawa jakości życia w nieskończonym horyzoncie czasowym, z uwzględnieniem uwarunkowań społecznych, środowiskowych i ekonomicznych. Koncepcja *smart city* to źródło inspiracji, kreatywności, przedsiębiorczości, aktywności oraz wymiany wiedzy; w obszarze kultury akcentuje znaczenie klasy kreatywnej. Dla optymalnego

[27] O. Sobolewska, *Co dalej z miastami? Drogowskaz dla miast → „SMART"*, [w:] *Co dalej z zarządzaniem?*, s. 195–214.

[28] D. Sikora-Fernandez, *Koncepcja „smart city" w założeniach polityki rozwoju miasta…*

[29] R. Ferrara, *The Smart City and the Green Economy in Europe: A Critical Approach*, „Energies" 2015, vol. 8, s. 4725, [za:] D. Stawasz, D. Sikora-Fernadez, *op. cit.*, s. 48–49.

funkcjonowania miast jako całości wykorzystuje zrównoważone i inteligentne działania, które obejmują współpracę różnych podmiotów, integrację w zakresie rozwiązań infrastrukturalnych i usług.

Inteligentne miasto (*intelligent city*) powinno łączyć kapitał społeczny z organizacją i infrastrukturą techniczną[30]. Dzięki wykorzystaniu rozwiązań innowacyjnych, tworzeniu wiedzy i uczeniu się – miasto takie cechuje się wysoką sprawnością zarządzania w warunkach niepewności. Opiera się na infrastrukturze cyfrowej, świadczy e-usługi, na jego terenie funkcjonują jednostki B&R i szkoły wyższe, zamieszkuje je klasa kreatywna. W porównaniu do *intelligent city* w wąskim rozumieniu, *smart city* realizuje działania bardziej o charakterze technicznym dla realizacji idei miasta inteligentnego. Coraz częściej jednak pojęcie to ulega rozszerzeniu o kwestie kapitału ludzkiego i kapitału społecznego. Szeroko rozumiane pojęcie *smart city* jest zbliżone do *intelligent city*. W praktyce miasta realizujące koncepcję *smart city* opierają się głównie na wdrażaniu technologii ICT i partycypacji obywatelskiej w zakresie zrównoważonego rozwoju lub ekorozwoju. W literaturze proponuje się 40 wskaźników pomiaru „inteligencji miasta" w grupach: edukacja i umiejętności, instytucje wiedzy i innowacji, infrastruktura cyfrowa i e-usługi oraz osiągnięcia w zakresie innowacyjności (w tym m.in. udział innowacyjnych przedsiębiorstw, udział przedsiębiorstw z własnymi działami B&R)[31].

Łukasz Kowalski prezentuje pogląd, że w koncepcjach miasta inteligentnego i miasta zrównoważonego mieszczą się: innowacyjność, informacja i współpraca. Pojęcie miasta inteligentnego kładzie nacisk na technologie teleinformacyjne i innowacje, które można wykorzystać dla rozwoju zrównoważonego. Pojęcie miasta zrównoważonego to pojęcie szersze niż pojęcie miasta inteligentnego, nie kładzie jednak nacisku na technologie teleinformatyczne i innowacje[32].

W definicjach miasta inteligentnego podkreśla się, że technologie wykorzystywane na rzecz innowacji i uczenia się, zdobywania wiedzy – służą też do rozwiązywania problemów społecznych, środowiskowych i ekonomicznych miast. W ideę zrównoważonego rozwoju wpisuje się redukcja kosztów infrastruktury, w tym oparta na racjonalizacji zużycia zasobów i ograniczeniu wpływu na środowisko naturalne (np. zarządzanie energią w domu z użyciem komputera, wspólne planowanie dojazdów jednym samochodem itp.)[33]. Lepsze zarządzanie miastem może się przejawiać w wielu kwestiach – również związanych bezpośrednio z bezpieczeństwem[34].

[30] A. Sobol, *op. cit*.

[31] A. Zakrzewska-Półtorak, *Inteligentne miasto katalizatorem rozwoju regionu?*, [w:] *Gospodarka przestrzenna XXI wieku*, red. A. Zakrzewska-Półtorak, P. Hajduga, M. Rogowska, Wrocław 2016, s. 282–291 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 443).

[32] Jest to pogląd dyskusyjny, gdyż w ramach rozwoju zrównoważonego kładzie się nacisk na innowacyjność ekologiczną.

[33] Ł. Kowalski, *Inteligentne miasta – przegląd rozwiązań*, [w:] *Miasto w badaniach geografów*, t. II, red. M. Soja, A. Zborowski, Kraków 2015, s. 105–121.

[34] Przykłady: *smart grid* (inteligentne sieci elektroenergetyczne, np. dla optymalizacji przepływów energii w sieci), inteligentne systemy transportowe (np. właściwa reakcja na korki uliczne czy dostępność miejsc parkingowych), eHealth (zdalne monitorowanie zdrowia osób), *blue sky learning* (nauczanie przez internet), portale umożliwiające reakcje na skargi mieszkańców dotyczące infrastruktury, koniecznych napraw itp. (to przykład *crowdsourcingu*), wykorzystanie kart zbliżeniowych do opłat za komunikację miejska (opłaty mogą być wyższe np. w godzinach szczytu, władze mogą reagować na

W literaturze przedmiotu pojawia się też pojęcie inteligentnego wzrostu. *Smart growth* uzupełnia ideę zrównoważonego rozwoju (*sustainable development*) głównie o kwestie oszczędności (środowiska i energii). *Smart growth* dotyczy miasta oszczędnego, zwiększenie szans rozwojowych następuje poprzez ograniczenie zagrożeń, np. budowę inteligentnych sieci energetycznych zapobiegających wyłączeniom energii elektrycznej. *Smart growth* opiera się na szybkich reakcjach na zmiany i wyzwania, wykorzystujących zdolności i wartości endogeniczne miasta lub regionu. Ma on cechy długotrwałości, ale także adaptacyjności wobec zagrożeń lub kryzysów. *Smart growth*, tworzony na podstawie diagnoz miast amerykańskich, stanowi operacjonalizację *sustainable development*, lecz jest bardziej pragmatyczny[35]. W ramach pojęcia miasta zrównoważonego istotne są kwestie zagrożenia bezpieczeństwa ekologicznego miast. Jako negatywne skutki urbanizacji wskazuje się zmiany poziomu zanieczyszczeń, zmiany struktury i użytkowania gleb, zmiany rzeźby terenu, obniżenie poziomu wód gruntowych, zmiany flory i fauny, powstanie klimatu miejskiego, zagęszczenie, ubytek terenów zielonych, negatywne oddziaływanie na tereny sąsiednie[36].

Na jakość życia mieszkańców miasta wpływa poczucie bezpieczeństwa. Wymiar instytucjonalny poczucia bezpieczeństwa odnosi się do ogółu warunków i instytucji społecznych chroniących przed zjawiskami groźnymi dla ładu prawnego, życia ludzi i ich zdrowia, a także powodującymi duże straty materialne[37]. W raporcie Polskiej Fundacji im. Roberta Schumana oraz Fundacji Konrada Adenauera w Polsce za miasto bezpieczne i otwarte uznano takie, w którym mieszkańcy mają pewność utrzymania poczucia bezpieczeństwa. Bezpieczeństwo nie tylko stabilizuje życie mieszkańców, ale także pozwala na rozwój. Wskaźniki opisujące bezpieczne i otwarte miasto mają charakter zarówno twardy (liczba i rodzaj przestępstw) jak i miękki (dotyczący postrzegania bezpieczeństwa przez mieszkańców). Proponowane wymiary odnoszą się do: bezpieczeństwa publicznego (ogólnego poziomu przestępczości), otwartości i przyjmowania pracowników z innych krajów, bezpieczeństwa indywidualnego (w tym przemocy domowej), komunikacyjnego oraz społeczno-ekonomicznego. Dyskutowane są kwestie prywatności, zachowań w sytuacjach kryzysowych, cyberbezpieczeństwa, inteligentnego monitorowania ulic i komunikacji miejskiej, ale także internetu rzeczy czy inteligentnych sieci, np. ciepłowniczych. W dziedzinie bezpieczeństwa komunikacyjnego – dobra

zmiany popytu na usługi transportowe), systemy analizujące dane związane z mobilnością (np. turystów) w oparciu o dane GPS, Geograficzne Systemy Informacji (dostarczające władzom samorządowym danych odnośnie do gospodarki przestrzennej, komunalnej, w sytuacjach kryzysowych na drogach i wobec przestępczości), wykorzystanie portali internetowych (np. Twittera) w czasie klęsk żywiołowych i zamieszek, zob. Ł. Kowalski, *op. cit.*

[35] J. Martyniuk-Pęczek, T. Parteka, O. Martyniuk, *op. cit*.

[36] B. Dobrzańska, G. Dobrzański, D. Kiełczewski, *Ochrona środowiska przyrodniczego*, red. nauk. G. Dobrzański, Warszawa 2009; E. Lonc, E. Kantowicz, *Ekologia i ochrona środowiska. Podręcznik dla studentów*, Wałbrzych 2005.

[37] Literaturę dotyczącą poczucia bezpieczeństwa człowieka w przestrzeni miejskiej omówiono w: E. Bogacka, A. Siniecka, *Poczucie bezpieczeństwa mieszkańców miasta. Przykład Poznania*, „Rozwój Regionalny i Polityka Regionalna" 2016, nr 33, s. 57–71.

infrastruktura to mniej wypadków drogowych[38]. Warto zwrócić uwagę na możliwości jeszcze ściślejszego powiązania bezpieczeństwa miast z koncepcją *smart city*. Działania w zakresie gospodarki energetycznej w ramach powstałej w 2010 roku Europejskiej Inicjatywy na Rzecz *Smart Cities* dotyczą budownictwa, transportu i sieci energetycznych. Czynnikiem sukcesu miasta w ramach *smart city* stają się technologie informacyjne i komunikacyjne (ICT), w szczególności odnoszące się do takich obszarów jak: gospodarka energetyczna, gospodarka transportowa, budownictwo mieszkaniowe, e-administracja (innowacyjna i kreatywna) realizująca usługi cyfrowe, a także bezpieczeństwo mieszkańców[39].

Rozwiązywanie problemów badawczych. Metody zarządzania a bezpieczeństwo miast

W niniejszym rozdziale skupiono się na zagadnieniach badawczych dotyczących bezpieczeństwa a także na problemach badawczych nurtu praktycznego i metod rozwiązywania problemów praktycznych z wykorzystaniem dorobku nauk o zarządzaniu.

W literaturze przedmiotu rozważane są problemy badawcze z zakresu bezpieczeństwa. Opisane są pojęcia metod badań i technik badawczych. Przedstawiono metody teoretyczne w naukowych badaniach problemów bezpieczeństwa (np. modelowanie, symulacje, analizy, analizy systemowe, scenariusze, algorytm, analizy RAND). Przytaczany jest ogólny model poznania naukowego przydatnego w badaniach problemów bezpieczeństwa. Zwraca się uwagę, że w empirycznych badaniach problemów bezpieczeństwa wykorzystuje się różne metody badawcze (m.in. ankieta, wywiad, obserwacja – zarówno uczestnicząca, jak i postronna, eksperyment, analiza dokumentów), w ramach których stosuje się określone techniki badawcze, a w ich ramach – narzędzia badawcze[40]. W kontekście występujących problemów badawczych rozpatruje się kwestie metod zarządzania. Bolesław Kuc i Zbigniew Ścibiorek zwracają uwagę, że każdy problem naukowy jest problemem badawczym, ale nie każdy problem badawczy jest problemem naukowym. Problem badawczy to zestaw pytań lub pytanie, na które odpowiedź ma dostarczyć badanie naukowe. W badaniach empirycznych po sformułowaniu problemu badawczego następuje sformułowanie hipotez badawczych i metod ich weryfikacji. Przy formułowaniu problemu badawczego trzeba uwzględnić, co chcemy badać, czego chcemy się dowiedzieć, jakie założenia przyjmujemy przy określeniu przedmiotu i celu badania W naukach o bezpieczeństwie występuje problematyka zarówno teorii bezpieczeństwa,

[38] *Bezpieczne i otwarte miasta*, Raport Polskiej Fundacji im. Roberta Schumana i Fundacji Konrada Adenauera w Polsce przygotowany przez Politykę Insight, Warszawa, maj 2017, s. 28, http://www.miasta.pl/uploads/attachment/file/1436/Europolis.-Bezpieczne-i-otwarte-miasta.pdf [dostęp: 15.01.2018].

[39] D. Sikora-Fernandez, Smart city *jako nowa koncepcja funkcjonowania i rozwoju miast w Polsce*, [w:] *Gospodarka przestrzenna. Dylematy i wyzwania współczesności*, red. J. Potocki, J. Ładysz, Wrocław 2014, s. 175–181 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 339).

[40] M. Cieślarczyk, *Metody i techniki badawcze stosowane w badaniach problemów bezpieczeństwa*, [w:] *Bezpieczeństwo. Teoria – badania – praktyka*, red. A. Czupryński, B. Wiśniewski, J. Zboina, Józefów 2015.

jak i praktyki bezpieczeństwa. Doskonaleniu praktyki służą badania empiryczne[41]. Agnieszka Sobol, dokonując przeglądu literatury, zwraca uwagę, że problemy badawcze nurtu praktycznego nauk o zarządzaniu mogą zawierać problemy naukowe (dotyczące rozważań teoretycznych) oraz problemy praktyczne (związane z badaniami empirycznymi). Problemy naukowe jako problemy teoretyczne występują oczywiście także w nurcie teoretycznym. W nurcie tym występują badania teoretyczne związane z brakiem wiedzy odnośnie do teorii. W nurcie empirycznym występują z kolei rozważania teoretyczne jako nadbudowa problemów praktycznych. Problem naukowy jest problemem teoretycznym; stanowi subiektywne odzwierciedlenie obiektywnych braków w określonej nauce. Pojawia się pojęcie czynności naukowej jako ustalania problemu. Dotyczy ona określenia i objaśnienia subiektywnego stanu niewiedzy. Problem naukowy w naukach o zarządzaniu, podobnie jak dla wszystkich dziedzin i dyscyplin naukowych, może być ujęty w ramach ontologii, epistemologii, metodologii i aksjologii. Problem praktyczny w ramach nauk o zarządzaniu dotyczy celu, warunków lub działania. Problemy praktyczne jako problemy badawcze w zakresie badań empirycznych w naukach o zarządzaniu dotyczyć mogą doboru i wykorzystania działań i warunków oraz wyznaczania i realizacji celów[42].

Marek Lisiński zwraca uwagę, że problemy badawcze dotyczą zarówno nurtu teoretycznego (zawierają problemy naukowe oraz metody naukowe nauk formalnych), jak i nurtu praktycznego (zawierają problemy praktyczne z metodami badawczymi nauk empirycznych oraz problemy naukowe, obejmujące metody naukowe nauk empirycznych, a także metody naukowe nauk formalnych). Identyfikowanie problemu badawczego odnosi się do refleksji związanej ze stanem niewiedzy podmiotu oraz do wymagającej rozwiązania sytuacji, a także do zdefiniowania zadania badawczego, które należy rozwiązać. Procesem mającym na celu wytworzenie wiedzy niezbędnej dla rozwiązania problemu badawczego jest postępowanie badawcze. Problemy w naukach o zarządzaniu mogą mieć charakter badawczy, naukowy i praktyczny. Problemy badawcze nurtu teoretycznego stanowią sytuacje problemowe, w których nie wykorzystuje się badań empirycznych, lecz dociekania logiczne. Pokonanie braku wiedzy odnośnie do teorii nauk o zarządzaniu może owocować ustaleniami naukowymi i poznawczymi. Problemy badawcze nurtu praktycznego, wynikające z niedostatków wiedzy z zakresu organizacji i zarządzania, stanowią problemy organizacji jako instytucji. Rozstrzygniecie problemów praktycznych ma swoje skutki z reguły w nieodległej perspektywie czasowej. Stanowią je sytuacje problemowe odnoszące się do określonych potrzeb.

Metody rozwiązywania problemów praktycznych w naukach o zarządzaniu to metody zarządzania[43]. Etapy procesu badawczego służące poznaniu i wyjaśnieniu zjawisk, zdarzeń i procesów wynikających z potrzeb nauki i praktyki, skutkujące wzrostem wiedzy naukowej (teorii), wzrostem wiedzy utylitarnej i zastosowaniu ich w praktyce obejmują: 1) postawienie problemu badawczego; 2) dobór zmiennych i wskaźników; 3) sformułowanie hipotez roboczych; 4) dobór terenu i próby

[41] B. Kuc, Z. Ścibiorek, *Zarys metodologii nauk o bezpieczeństwie*, Toruń 2018, s. 142–145.

[42] A. Sobol, *op. cit.*

[43] M. Lisiński, *Problemy badawcze i metody ich rozwiązywania w naukach o zarządzaniu*, „Ekonomika i Organizacja Przedsiębiorstwa" 2017, nr 8, s. 3–20.

badawczej; 5) dobór metod i technik badawczych; 6) realizację badań; 7) analizę uzyskanych materiałów, 8) uogólnienie dotyczące potwierdzenia hipotezy (czy wyniki ją potwierdzają). Po postawieniu problemu badawczego ustala się cele badawcze i dokonuje wyboru pojęć, przy pomocy których chce się opisać rzeczywistość, oraz określa ich definicje. Kategoriom teoretycznym nadaje się sens podlegający empirycznej kontroli, czyli dokonuje się operacjonalizacji pojęć. Pojęcie stanowi kategorię poznawczą pośrednicząca między rzeczywistym zjawiskiem a badaczem, za pomocą której pojmowana jest rzeczywistość. Kategoriami pojęciowymi są m.in. „zagrożenie" i „bezpieczeństwo". Operacjonalizacja tych pojęć jest przeprowadzana np. w oparciu o definicje zawarte w różnych słownikach. Dla badań realizowanych w praktyce dobiera się narzędzia badawcze, którymi mogą być:

- metody (techniki) badawcze: metody teoretyczne (analiza, synteza, abstrahowanie), porównanie, uogólnienie, metody wnioskowania (dedukcja, redukcja, indukcja, analogia);
- metody (techniki) empiryczne: obserwacja, eksperyment naukowy, ankieta, wywiad, analiza dokumentacji źródłowej (operacyjnej) instytucji lub zjawiska, metody modelowania, metody eksperckie (burza mózgów, wariant delficki)[44].

Przeglądu pojęć w zarządzaniu dokonał Tomasz Sobczak[45]. Uwzględnia on następujące poglądy:

- Proponuje się czterostopniową hierarchie pojęć w naukach o zarządzaniu: orientacja, koncepcja, metoda ogólna i technika oraz metoda szczegółowa lub narzędzie[46]; wskazuje się że pojęcia: filozofia, orientacja, podejście i koncepcja to synonimy[47].
- Wymienia się koncepcje zarządzania zorientowane: na jakość (TQM, *six sigma*), na klienta (w tym marketing partnerski), na współdziałanie (w tym organizację sieciową czy wirtualną), na wyszczuplenie organizacji (*lean management*, *outsourcing*), na wiedzę (w tym organizację uczącą się, a także zarządzanie innowacjami)[48].
- Jako koncepcje zarządzania wskazuje się *benchmarking*, *outsourcing*, *lean management*, *reengineering*, TQM. Koncepcje zarządzania dzielą się na: klasyczne (logistyka, TQM), współczesne (*benchmarking*, *outsourcing*, *lean management*, *reengineering*) oraz nowoczesne (zarządzanie wiedzą, zarządzanie talentami, zarządzanie relacjami oraz organizacja wirtualna)[49]. Inny proponowany podział koncepcji zarządzania rozwojem firmy: klasyczne (*time based management*, logistyka, TQM), współczesne (BPR, *lean management, outsourcing, benchmarking*) oraz nowoczesne (organizacja wirtualna, organizacja fraktalna, zarządzanie wiedzą)[50].
- *Benchmarking*, *outsourcing*, *lean management, reengineering* i TQM mogą być traktowane jako metody[51].
- Z punktu widzenia praktycznego do współczesnych metod zarządzania zaliczono: *benchmarking*, *controlling*, *lean management*, *outsourcing*, reinżynierię i TQM[52].
- TQM, *reengineering*, *benchmarking*, *lean management* traktowane są jako metody organizatorskie[53].
- *Benchmarking* i *reengineering* traktuje się jako koncepcje lub metody, *outsourcing* i *lean management* – jako metody, a TQM – jako technikę[54].
- Proponuje się pojęcie instrumentu jako ogólnej konstrukcji myślowej. Nie ma jednak ściśle określonej granicy między instrumentami a koncepcjami i metodami, a także instrumentami i technikami (sposobami). Hierarchiczny model instrumentów zarządzania obejmuje (od góry): model zarządzania organizacją (np. TQM), metakoncepcję zarządzania (np. zarządzanie wartością), koncepcje zarządzania, metody zarządzania i wreszcie techniki zarządzania[55]. Prezentowany jest pogląd, że współczesne instrumenty zarządzania tworzą zbiór powiązanych z sobą idei, zasad, metod, technik i narzędzi. Służą one do nadawaniu określonego wizerunku (kształtu) systemowi zarządzania w przedsiębiorstwie. W ramach podejścia organicznego wskazuje się[56] na takie instrumenty zarządzania organizacjami jak zarządzanie procesowe, *reengineering*, *benchmarking*, *lean management*, *kaizen*, SMED, SKW (Strategiczna Karta Wyników) czy system Toyoty[57].

Metody te mogą być wykorzystywane w organizacjach funkcjonujących w systemie bezpieczeństwa na terenie miast. Specyfika zarządzania bezpieczeństwem wiąże się z potrzebą poszukiwania koncepcji, metod czy narzędzi odpowiadających nieoczekiwalności zdarzeń i pojawiających się zagrożeń. Wskazuje się na możliwości

44 B. Kuc, Z. Ścibiorek, *op. cit*., s. 168–172, 226–230.

45 T. Sobczak, *O koncepcjach i metodach w naukach o zarządzaniu w Polsce – raz jeszcze*, „Przegląd Organizacji" 2017, nr 5, s. 3–9.

46 J. Lichtarski, *Praktyczny wymiar nauk o zarządzaniu*, Warszawa 2015.

47 H. Jagoda, J. Lichtarski, *O istocie i ewolucji współczesnych koncepcji i metod zarzadzania przedsiębiorstwem*, „Przegląd Organizacji" 2003, nr 1, s. 3–6.

48 *Koncepcje zarządzania. Podręcznik akademicki*, red. M. Czerska, A.A. Szpitter, Warszawa 2010, s. 137–366.

49 A. Bitkowska, E. Weiss, *Wybrane koncepcje zarządzania przedsiębiorstwem. Teoria i praktyka*, Warszawa 2015.

50 K. Bartusik, *Przegląd współczesnych koncepcji w zarządzaniu rozwojem firmy*, „Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie" 2004, nr 5, s. 7–20.

51 A. Bieńkowska, A. Zgrzywa-Ziemak, *Współwystępowanie koncepcji i metod zarządzania w świetle badań empirycznych*, [w:] *Nowe kierunki w zarządzaniu przedsiębiorstwem – wiodące orientacje*, red. J. Lichtarski *et al.*, Wrocław 2014, s. 17–26 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 340).

52 M. Hopej, J. Kral, *Współczesne metody zarządzania w teorii i praktyce*, Wrocław 2011.

53 M. Ćwiklicki, *Ewolucja metod organizatorskich*, Kraków 2011.

54 S. Sokołowska *et al.*, *Koncepcje organizacji i metody zarządzania. Możliwości i ograniczenia*, Warszawa 2016.

55 S. Nowosielski, *Koncepcje zarządzania organizacją. Problemy terminologiczne*, [w:] *Zarządzanie w teorii*, red. M. Przybyła, Wrocław 2010, s. 13–23 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 137, Nauki o Zarządzaniu, nr 4).

56 J. Czekaj, *Metody organizatorskie w doskonaleniu systemu zarządzania*, Warszawa 2013, s. 11–47.

57 Sobczak załączył zestawienie tabelaryczne zróżnicowania poglądów poszczególnych autorów. Wynika z niego, że wg J. Lichtarskiego *lean management*, *reengineering* i TQM to koncepcje, podobnie jak u S. Nowosielskiego. U tego ostatniego autora metody to *benchmarking i outsourcing*. Z kolei M. Hopej i M. Ćwiklicki traktują *benchmarking*, *outsourcing*, *lean management*, *reengineering* i TQM jako metody. Według A.A. Szpitter *benchmarking*, *outsourcing*, *lean management* (brak odniesienia do *reengineeringu*), TQM to koncepcje, T. Sobczak, *op. cit.*, s. 3–9, tabela s. 8.

wykorzystania w zarządzaniu miastem metod *lean management* czy *reengineering*[58]. W ramach przygotowań strategii rozwoju miast wykorzystuje się metodę SWOT, często stosowaną w firmach. Warto zwrócić uwagę na możliwość wykorzystania również popularnej w przedsiębiorstwach metody Strategicznej Karty Wyników (SKW)[59], uwzględniającej cele społeczne, w tym ekologiczne – jako jedno z kryteriów dla miast można wprowadzić aspekt bezpieczeństwa. Podobnie w przypadku metody oceny kapitału intelektualnego. Miasto może być rozpatrywane z punktu widzenia występujących powiązań o charakterze sieciowym – również tę koncepcję można wykorzystać w celu poprawy bezpieczeństwa[60]. Jako partycypacyjną metodę zarządzania miastem wymienia się Living Lab, angażującą interesariuszy miasta w działania na rzecz innowacji i projektów. Proces rozwoju idei z udziałem interesariuszy obejmuje etapy: tworzenia idei, jej testowania i walidacji. Koncepcja zakłada partnerstwo biznesu z klientami i instytucjami publicznymi oraz wykorzystanie zarządzania sprawami publicznymi poprzez projekty[61].

Wykorzystanie na rzecz miasta – także jego bezpieczeństwa – koncepcji interesariuszy, powszechnie przyjętej w zarządzaniu organizacjami komercyjnymi, wymagałaby dostosowania metod wykorzystywanych w firmach: macierzy oceny oddziaływań interesariuszy (metoda Vestera), macierzy siły wpływu i poziomu zainteresowania interesariuszy oraz analizy atrybutów interesariuszy[62]. Możliwości wykorzystania tych koncepcji i metod są szczególnie istotne w sytuacji działań zmierzających do przekształcenia miast w myśl koncepcji *smart* i *sustainability* (zrównoważenia).

Szczególną uwagę chcę zwrócić na wykorzystanie metod zarządzania w zarządzaniu kryzysowym, na zarządzanie incydentami i uczenie się przez działanie.

Planowanie cywilne, zarządzanie incydentami, scenariusze zdarzeń krytycznych

Polityka miejska obejmuje kwestie bezpieczeństwa lokalnego jako część składową bezpieczeństwa publicznego, czyli ogółu warunków i urządzeń społecznych, których zadaniem jest chronienie obywatela przed zjawiskami groźnymi dla zdrowia i życia, które przynoszą straty gospodarcze i generują koszty społeczne. Władze lokalne w ramach swojej polityki powinny wykorzystywać odpowiednie instrumenty i metody zarządzania rozwojem miast dla przeciwdziałania zjawiskom negatywnym w sferze społeczno-gospodarczej (bieda, wykluczenie społeczne, przestępczość) i środowiskowej (klęski żywiołowe) – powinny stworzyć system bezpieczeństwa na

[58] M. Kudłacz, P. Mazur-Kurach, *op. cit*.

[59] A. Chodyński, A. Jabłoński, M. Jabłoński, *Strategiczna Karta Wyników (Balanced Scorecard) w implementacji założeń rozwoju organizacji*, Kraków 2007.

[60] A. Chodyński, *Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym*, „Bezpieczeństwo. Teoria i Praktyka" 2014, nr 1, s. 13–27.

[61] D. Stawasz, D. Sikora-Fernandez, *op. cit.*, s. 107.

[62] A. Chodyński, *Interesariusze w kształtowaniu bezpieczeństwa organizacji wobec kryzysu pozaekonomicznego*, „Bezpieczeństwo. Teoria i Praktyka" 2016, nr 4, s. 41–55.

szczeblu lokalnym[63]. Rewitalizacja (odnowa miasta) dotyczy obszarów kryzysowych (np. opuszczonych przez wojsko, poprzemysłowych, poportowych). Prowadzona jest z udziałem władz miasta i interesariuszy (np. mieszkańców, przedsiębiorstw, organizacji non profit, instytucji międzynarodowych, organizacji publicznych, wyższych uczelni, mediów, związków wyznaniowych, wspólnot mieszkaniowych czy deweloperów). Rewitalizacja to proces działań planowych, realizowany przez podmioty lokalne z wykorzystaniem takich zasobów jak kapitał społeczny, finansowy, gospodarczy czy przestrzenno-przyrodniczy. To odnowa obszaru zurbanizowanego, który uległ degradacji, co doprowadziło do stanu kryzysowego[64].

Zarządzanie kryzysowe realizowane jest na różnych szczeblach, także na poziomie gmin (miast)[65]. W publicznym zarządzaniu kryzysowym można wykorzystać takie koncepcje, metody i techniki czy podejścia jak: prognozowanie (*foresight*) regionalne, zarządzanie wiedzą, analiza interesariuszy, oceny kompetencji, a także zarządzanie ryzykiem operacyjnym, pobudzanie kreatywności[66] czy analiza SWOT[67]. Z zarządzaniem kryzysowym wiąże się planowanie cywilne. W procesie planowania cywilnego wykorzystuje się prognozowanie. Obejmuje ono m.in. tworzenie scenariusza z określeniem występujących interesariuszy typowych (głównie instytucji i organizacji biorących udział w pracach zespołu scenariusza zdarzeń niekorzystnych), jako etap poprzedzający opracowanie planu. Prognozowanie może być wspierane przez scenariusz zdarzeń niekorzystnych (SZN).

Dane o przeszłych niekorzystnych zdarzeniach powinny być gromadzone, a wyciągnięte z nich wnioski i ocena ryzyka – przyczyniać się do doskonalenia reagowania w przyszłości. Proponuje się wykorzystanie metody scenariuszowej, pozwalającej przygotować się na różne wersje rozwoju sytuacji kryzysowej (scenariusz optymistyczny, pesymistyczny i realny). W literaturze podkreślane jest występowanie interakcji elementarnych zagrożeń (efekt domina). Podano także wykaz dobrych praktyk (w metodykach zarządzania kryzysowego w różnych krajach i odniesiono się do podziału zagrożeń[68]. W budowaniu SZN wykorzystuje się m.in. metodę burzy mózgów, spotkania seminaryjne czy metody eksperckie. W zarządzaniu bezpieczeństwem infrastruktury krytycznej wykorzystuje się m.in. *benchmarking* najlepszych praktyk, w tym pochodzących z zagranicy. Rozpatrywanie SZN powinno uwzględniać m.in. poglądy dotyczące koncepcji i podejść do zarządzania oraz metod i technik organizatorskich (wymienia się podejście scenariuszowe i sytuacyjne, metody AIDA jako model procesu decyzyjnego i CBR (*case-based reasoning*), oparty na założeniu, że aktualny problem może być rozwiązany z wykorzystaniem rozwiązań

[63] D. Stawasz, D. Sikora-Fernandez, *op. cit.*, s. 22.

[64] *Ibidem*, s. 63–64.

[65] K. Grosicka, L. Grosicki, P. Grosicki, *Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa*, Pułtusk–Warszawa 2013, s. 82

[66] M. Kisilowski, *Co dalej z zarządzaniem publicznym?*, [w:] *Co dalej z zarządzaniem?*, s. 106–125.

[67] U. Kąkol *et al.*, *Stan planowania cywilnego w Polsce*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, red. M. Ćwiklicki, M. Jabłoński, S. Mazur, Kraków 2016, s. 75–84.

[68] M. Wiśniewski, M. Kisilowski, M. Marczewski, *Zasady budowy scenariuszy zdarzeń niekorzystnych w publicznym zarządzaniu kryzysowym*, [w:] *Współczesne koncepcje zarządzania publicznego...*, s. 97–110.

z przeszłości). W podejściu scenariuszowym ważne jest rozpatrywanie zdolności organizacji do uczenia się w sytuacji szoku zewnętrznego (np. klęska żywiołowa, atak terrorystyczny, absencja kluczowych pracowników) i odzyskiwania równowagi w kontekście zarządzania ryzykiem. W podejściu sytuacyjnym zalecane jest opracowanie modelowych rozwiązań zarządzania, z wykorzystaniem zgromadzonej wiedzy. Wskazuje się na znaczenie narzędzi informatycznych – baz i hurtowni danych, wspierania pracy grupowej czy symulacji procesów biznesowych[69].

W odniesieniu do zarządzania kryzysowego wskazuje się, że dotychczasowy zbiór metod i technik nie jest wystarczający i akcentuje się znaczenie zarządzania wiedzą oraz rolę zachowań antycypacyjnych. Podkreśla się możliwości wykorzystania narzędzi i analiz dotyczących *controllingu*, a także metod prognozowania. Formułowana jest propozycja twórczej adaptacji wybranych metod zarządzania dla realizacji racjonalnych badań i ocen w zakresie procesów rozpoznawania zagrożeń oraz planowania działań dotyczących następstw zdarzeń kryzysowych.

W kwestiach szczegółowych zwraca się uwagę, że:

- Aktualnie zarządzanie kryzysowe nie dysponuje odpowiednim zbiorem technik i metod rozwiązywania problemów na rzecz przewidywania stanów przyszłych. Dla prognozowania wykorzystać można eksperyment lub nabyte empiryczne doświadczenie.
- W prognozowaniu w ramach zarządzania kryzysowego proponuje się wykorzystywać scenariusze dla wyspecyfikowanych sytuacji kryzysowych i uwzględniać je w planowaniu kryzysowym w obszarach poszczególnych faz zarządzania kryzysowego: zapobiegania, planowania, reagowania i odbudowy.
- Wśród metod zarządzania i technicznego prognozowania przydatnych dla zarządzania kryzysowego wymienia się: 1) różne typy *controllingu* (wraz z grupami procedur dla zróżnicowanych zagrożeń, z wykorzystaniem narzędzi i analiz stosowanych w firmach); 2) *foresight* (jako zbór narzędzi do konstrukcji scenariuszy zdarzeń; narzędziami tymi są metody badawcze, analiza trendów oraz intuicja uczestników procesów prognozowania); 3) metody interdyscyplinarne.
- Dla zabezpieczenia procesów prognozowania i oceny ryzyka poszczególnych faz zarządzania kryzysowego istotny jest dobór metod zarządzania w aspekcie wykorzystania specjalistycznego instrumentarium obejmującego określone techniki i analizy. Dla poszczególnych faz zarządzania kryzysowego niezbędne jest przygotowanie systemu procedur antycypacji w oparciu o techniki *controllingu*, *foresight* oraz techniki interdyscyplinarne.
- W każdej z faz zarządzania kryzysowego zalecane jest określone podejście do oceny ryzyka. Czynniki ryzyka mogą mieć charakter zewnętrzny, wewnętrzny oraz mogą być związane z jakością zarządzania[70].

W ramach zarządzania kryzysowego istotna jest analiza dostępności zasobów. W teorii zarządzania strategicznego (w odniesieniu do organizacji) zasoby są rozważane m.in. w ujęciu ich wartości, rzadkości, trudności ich imitacji przez konkurentów – czyli z punktu widzenia stworzenia i utrzymania przewagi konkurencyjnej. W kontekście posiadanych zasobów rozważana jest możliwość ich wykorzystania

[69] *Ibidem*, s. 97–110.

[70] B. Stęplewski, *Podstawy niemilitarnego zarządzania kryzysowego*, Kraków 2017, s. 92, 94, 99–101.

wobec możliwych zagrożeń – np. metoda VRIO[71]. Doświadczenia tej metody mogą być przydatne w sytuacjach kryzysowych, a jej adaptacja dla potrzeb podniesienia bezpieczeństwa może być interesującym polem badawczym, w szczególności w powiązaniu z zachowaniami opisywanymi jako brikolaż. W literaturze przedmiotu zwraca się uwagę na istotną rolę uczenia się przez działanie (*action learning*), opartego na zaangażowaniu ludzi w uczenie się nawzajem ze swoich doświadczeń. Podkreśla się znaczenie studiowania sytuacji indywidualnych osób. Wyjaśnieniu podlegają cele, jakie organizacje chciałyby osiągnąć, oraz działania związane z usuwaniem przeszkód. W ramach nauki przez działanie (*action science*) podkreśla się znaczenie studiowania praktyki w otoczeniu organizacyjnym, która może stanowić źródło nowych rozumień i usprawnień[72].

W działaniach na rzecz poprawy poziomu bezpieczeństwa istotne jest zarządzanie incydentami. Dla oceny incydentów niezwiązanych z bezpieczeństwem informacji proponuję (wykorzystując doświadczenia z tego zakresu) stosowanie następujących kryteriów: fazy planowania i przygotowania, szybkości i sprawności wykrycia i raportowania, przeprowadzenia oceny i podejmowania decyzji, reakcji na incydenty, realizacji nauki z incydentu, obszaru incydentu, skali incydentu, konsekwencji finansowych, wizerunkowych, prawnych – dla klientów, a także dla kierownictwa i pracowników. Dużą rolę – zarówno w zarządzaniu kryzysowym, jak i dla zachowania ciągłości działania – odgrywa podejmowanie decyzji przed i w trakcie incydentu. Analiza ryzyka jest już wtedy niewystarczająca, należy podjąć działania na rzecz zarządzania incydentami[73].

Prezentowane propozycje dotyczące instrumentarium wykorzystywanego w zarządzaniu w sytuacjach kryzysowych mogą wiązać się z tym aspektem „inteligencji miasta", który dotyczy zagrożeń bezpieczeństwa. Pozwalają na antycypowanie możliwych przyszłych zdarzeń i przygotowanie się, na ile to możliwe, na ich wystąpienie.

Propozycje dalszych badań

Ciekawym kierunkiem badawczym jest możliwość rozpatrywania miast jako systemów o wysokiej odporności (*resilience*). W dyskusjach teoretycznych występują terminy *organization survival* (przetrwanie organizacji) i *organizational resilience* (sprężystość, odporność organizacji) – ten drugi dotyczy systemów: ekologicznych, społeczno-ekologicznych, społeczności (*communities*), łańcuchów dostaw i jednostek (*individuals*). Sprężystość systemu odnosi się do dynamicznych kompetencji (*dynamic capabilities*) i zasobów budujących systemowe zdolności adaptacyjne (*systems adaptive capacity*). Zdarzenia niszczące (np. katastrofy naturalne, akty terroryzmu) prowadzą do uczenia się organizacji. Poziomy odporności odnoszą się do

[71] J. Rokita, *Zarządzanie strategiczne. Tworzenie i utrzymywanie przewagi konkurencyjnej*, Warszawa 2005.

[72] S. Kemmis, R. McTaggart, *Uczestniczące badania interwencyjne. Działanie komunikacyjne i sfera publiczna*, [w:] *Metody badań jakościowych*, t. 1, red. N.K. Denzin, Y.S. Lincoln, red. wydania polskiego K. Podemski, Warszawa 2009, s. 775–831.

[73] B. Szomański, *Zarządzanie incydentami. Praktyka, zalecenia i wnioski dla kierownictwa*, [w:] *Co dalej z zarządzaniem?*, s. 229–251.

jednostek, systemów, struktur, infrastruktury, procedur i parametrów organizacji. W organizacji występują domeny o różnym stopniu odporności. Dynamika związana z odpornością wiąże się ze zdolnością systemu do rekonfiguracji w celu złagodzenia zagrożeń. Mechanizm związany z *organizational resilience* odnosi się do doskonalenia organizacyjnej świadomości o charakterze sytuacyjnym, ograniczenia wrażliwości na systemowe ryzyko zewnętrzne (środowiskowe, *environments*) oraz przywracania efektywności (*efficacy*) po zdarzeniu niszczącym[74]. W przypadku wystąpienia zagrożeń rutynowe zachowania i procedury są już niewystarczające. Badania powinny dotyczyć „inteligencji miast" i nowych koncepcji, metod i narzędzi dla zapewnienia sprężystości (*resilience*) miast. Rozwijane powinny być metody pozwalające na ocenę i wykorzystanie dostępnych zasobów (w tym kompetencji i umiejętności) w sytuacjach kryzysowych.

Perspektywicznym kierunkiem badań może być ekonomika miast, zajmująca się zależnościami między lokalizacją, wielkością produkcji i optymalną wielkością miasta. Obszary ekonomiki miasta to: 1) siły rynkowe wpływające na rozwój miast (w tym decyzje lokalizacyjne gospodarstw domowych i podmiotów gospodarczych); zwraca się uwagę na walory miast pozwalających rozwinąć optymalną skalę produkcji, prowadzącą do korzyści skali, korzyści lokalizacji (sąsiedztwa przedsiębiorstw o tej samej lub podobnej działalności, co wiąże się z wyspecjalizowanym rynkiem pracy i rynkiem zbytu) oraz korzyści urbanizacji (w przypadku prowadzenia przez przedsiębiorstwa odmiennej działalności korzystanie z elementów wspólnego otoczenia pozwala na obniżenie kosztów działalności); 2) sposób użytkowania terenów (decyzje lokalizacyjne, w tym koncentracja podmiotów gospodarczych); 3) transport miejski i metropolitarny; 4) budownictwo i polityka mieszkaniowa; 5) bezpieczeństwo publiczne – odnosi się m.in. do wpływu biedy, poziomu edukacji i wykluczenia społecznego na bezpieczeństwo w mieście. Bezpieczeństwo wiąże się m.in. z pewnością zatrudnienia, poziomem opieki zdrowotnej i poczuciem stabilności. Brak właściwej polityki władz prowadzi do marginalizacji określonych grup społecznych. Bezpieczeństwo można rozpatrywać albo jako brak zagrożeń (stan obiektywny), albo jak stan pozytywny (odczytywany subiektywnie), np. pewność czy spokój społeczny[75]. W ramach ekonomiki miast można również rozpatrywać konsekwencje nagłych wydarzeń związanych z zagrożeniami bezpieczeństwa, np. klęsk żywiołowych czy dużych awarii zakładów przemysłowych zlokalizowanych na terenie miast.

W sytuacjach nieprzewidywalnych szczególne znaczenie ma brikolaż. Określam go jako brikolaż kryzysowy. Brikolaż dotyczy kombinacji (połączenia, *combination*) zasobów „od ręki" z jednej strony w przypadku wystąpienia nowych problemów, ale również i szans (okazji, *opportunities*)[76]. Jest rozpatrywany w aspekcie przetrwania (*survival*) w sytuacjach niedogodnych (niepożądanych, *undesirable*), charakteryzujących się pojawieniem problemu w sposób nagły i niespodziewany

[74] K. Burnard, R. Bhamra, *Organisational Resilience: Development of Conceptual Framework for Organisational Responses*, "International Journal of Production Research" 2011, vol. 49, nr 18, s. 5581–5599.

[75] D. Stawasz, D. Sikora-Fernandez, *op. cit.*, s.16–18, 21.

[76] T. Baker, R.E. Nelson, *Creating Something from Nothing: Resource Construction through Entrepreneurial Bricolage*, "Administrative Science Quarterly" 2005, vol. 50, nr 3, s. 329–366.

(*unexpectedly*)[77]. Brikolaż stosuje się w podejmowaniu decyzji[78] w sytuacji niepewności lub ryzyka[79] co jest kluczowe w zarządzaniu bezpieczeństwem. W literaturze podkreśla się, że brikolaż ma związek z kreatywnością i improwizacją[80]. Tematyka brikoloażu może stanowić pole badawcze dotyczące zarządzania miastem w sytuacjach kryzysowych[81].

Dalsze badania wiązać się mogą z menadżerskim podejściem do zarządzania miastem (w ramach nowego zarządzania publicznego). Użytkownicy miasta są konsumentami usług publicznych – mają możliwość wyboru ich zakresu i sposobu wyboru. Władze miasta występują w roli menadżera miasta – funkcjonują w oparciu o przyjęte wartości i są odpowiedzialne za efekty swoich działań. Zarządzaniu sprawami publicznymi (również dotyczącymi bezpieczeństwa) wspólnie z mieszkańcami służy *crowdsourcing*, obejmujący: 1) konkursy społeczne z użyciem internetu, dla generowania nowych pomysłów lub testowania usług publicznych (*crowdcontest*); 2) wyszukiwanie osób o umiejętnościach specjalistycznych i ich udział w realizacji konkretnych zadań (*macrotasking*); 3) pozyskiwanie funduszy na rzecz konkretnych projektów (celów) (*crowdfunding*)[82].

Podsumowanie

W działaniach na rzecz podnoszenia poziomu bezpieczeństwa miast uwzględniać można szereg koncepcji i metod z zakresu zarządzania. Dotyczy to przede wszystkim koncepcji organizacji inteligentnej, uczącej się i zarządzającej wiedzą oraz koncepcji kapitału intelektualnego. Akcentowana jest przydatność metod z zakresu planowania strategicznego, np. metody SWOT czy analizy scenariuszowej. Wśród metod zarządzania w perspektywie rozwojowej szczególne znaczenie ma Strategiczna Karta Wyników. Podnoszone tam kwestie dotyczące zapewnienia ciągłości działania nabierają specjalnego charakteru w dziedzinie bezpieczeństwa. W przypadku wystąpienia nieoczekiwanych zagrożeń wzrasta przydatność innych metod (podejść), np. brikolażu – związanego z generowaniem zachowań przedsiębiorczych i innowacyjnych.

[77] M. Madajová, S. Mpumwire, P. Pallabi Mishra, *Social Entrepreneurship: The Dual Role of Bricolage on Innovation*, 2017.05.30, Master`s thesis, Departament of Business Studies, Uppsala University, https://pdfs.semanticscholar.org/8914/702083e4f577f25c53b50ae67e8572adc088.pdf?_ga=2.218432026.2022962652.1576007701-327157607.1576007701 [dostęp: 15.01.2018].

[78] T. Baker, R.E. Nelson, *op. cit.*, s. 329–366.

[79] Sytuacje wymagające podjęcia decyzji charakteryzują się pewnością, niepewnością lub ryzykiem, zob. A. Holska, *Teorie podejmowania decyzji*, [w:] *Zarządzanie, organizacje i organizowanie. Przegląd perspektyw teoretycznych*, red. K. Klincewicz, Warszawa 2016, s. 239–252, http://timo.wz.uw.edu.pl/zoo [dostęp: 15.01.2018].

[80] J. Kickul, M.D. Griffiths, L.K. Gundry, *Innovating for Social Impact: Is Bricolage the Catalyst for Change?*, [w:] *Handbook of Research on Social Entrepreneurship*, Cheltenham 2010, s. 232–251.

[81] Szerzej zob. A. Chodyński, *Brikolaż przedsiębiorczy w zarządzaniu innowacjami w firmie inteligentnej i odpowiedzialnej społecznie*, referat wygłoszony 10.06.2019 r. na XIX Konferencji Naukowej *Państwo, Gospodarka, Społeczeństwo*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 10–11 czerwca 2019.

[82] D. Stawasz, D. Sikora-Fernandez, *op. cit.*, s. 95–96, 108.

Bibliografia

Baker T., Nelson R.E., *Creating Something from Nothing: Resource Construction through Entrepreneurial Bricolage*, "Administrative Science Quarterly" 2005, vol. 50, nr 3.

Bartusik K., *Przegląd współczesnych koncepcji w zarządzaniu rozwojem firmy*, „Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie" 2004, nr 5.

Bezpieczne i otwarte miasta, Raport Polskiej Fundacji im. Roberta Schumana i Fundacji Konrada Adenauera w Polsce przygotowany przez Politykę Insight, Warszawa, maj 2017.

Bieńkowska A., Zgrzywa-Ziemak A., *Współwystępowanie koncepcji i metod zarządzania w świetle badań empirycznych*, [w:] *Nowe kierunki w zarządzaniu przedsiębiorstwem – wiodące orientacje*, red. J. Lichtarski *et al.*, Wrocław 2014 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 340).

Bitkowska A., Weiss E., *Wybrane koncepcje zarządzania przedsiębiorstwem. Teoria i praktyka*, Warszawa 2015.

Bogacka E., Siniecka A., *Poczucie bezpieczeństwa mieszkańców miasta. Przykład Poznania*, „Rozwój Regionalny i Polityka Regionalna" 2016, nr 33.

Burnard K., Bhamra R., *Organisational Resilience: Development of Conceptual Framework for Organisational Responses*, "International Journal of Production Research" 2011, vol. 49, nr 18.

Chodyński A., *Brikolaż przedsiębiorczy w zarządzaniu innowacjami w firmie inteligentnej i odpowiedzialnej społecznie*, referat wygłoszony 10.06.2019 r. na XIX Konferencji Naukowej *Państwo, Gospodarka, Społeczeństwo*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 10–11 czerwca 2019.

Chodyński A., *Interesariusze w kształtowaniu bezpieczeństwa organizacji wobec kryzysu pozaekonomicznego*, „Bezpieczeństwo. Teoria i Praktyka" 2016, nr 4.

Chodyński A., *Sieciowość w zarządzaniu bezpieczeństwem na poziomie regionalnym i lokalnym*, „Bezpieczeństwo. Teoria i Praktyka" 2014, nr 1.

Chodyński A., *Wpływ wspólnych wartości na zjawisko izomorfizmu organizacyjnego*, [w:] *Zarządzanie nowoczesną organizacją*, red. O. Grabiec, Sosnowiec 2018.

Chodyński A., Jabłoński A., Jabłoński M., *Strategiczna Karta Wyników (Balanced Scorecard) w implementacji założeń rozwoju organizacji*, Kraków 2007.

Cieślarczyk M., *Metody i techniki badawcze stosowane w badaniach problemów bezpieczeństwa*, [w:] *Bezpieczeństwo. Teoria – badania – praktyka*, red. A. Czupryński, B. Wiśniewski, J. Zboina, Józefów 2015.

Czekaj J., *Metody organizatorskie w doskonaleniu systemu zarządzania*, Warszawa 2013.

Ćwiklicki M., *Ewolucja metod organizatorskich*, Kraków 2011.

Dobrzańska B., Dobrzański G., Kiełczewski D., *Ochrona środowiska przyrodniczego*, red. nauk. G. Dobrzański, Warszawa 2009.

Edvinsson L., Malone M.S., *Kapitał intelektualny*, tłum. M. Marcinkowska, Warszawa 2001.

Gierszewska G., *Czy inteligentne przedsiębiorstwa to już teraźniejszość czy mglista przyszłość?*, [w:] *Co dalej z zarządzaniem?*, red. G. Gierszewska, Warszawa 2018.

Grosicka K., Grosicki L., Grosicki P., *Organizacja i kierowanie instytucjami bezpieczeństwa wewnętrznego państwa*, Pułtusk–Warszawa 2013.

Holska A., *Teorie podejmowania decyzji*, [w:] *Zarządzanie, organizacje i organizowanie. Przegląd perspektyw teoretycznych*, red. K. Klincewicz, Warszawa 2016, http://timo.wz.uw.edu.pl/zoo [dostęp: 15.01.2018].

Hopej M., Kral J., *Współczesne metody zarządzania w teorii i praktyce*, Wrocław 2011.

Jagoda H., Lichtarski J., *O istocie i ewolucji współczesnych koncepcji i metod zarządzania przedsiębiorstwem*, „Przegląd Organizacji" 2003, nr 1.

Kąkol U. *et al.*, *Stan planowania cywilnego w Polsce*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, red. M. Ćwiklicki, M. Jabłoński, S. Mazur, Kraków 2016.

Kemmis S., McTaggart R., *Uczestniczące badania interwencyjne. Działanie komunikacyjne i sfera publiczna*, [w:] *Metody badań jakościowych*, t. 1, red. N.K. Denzin, Y.S. Lincoln, red. wydania polskiego K. Podemski, Warszawa 2009.

Kickul J., Griffiths M.D., Gundry L.K., *Innovating for Social Impact: Is Bricolage the Catalyst for Change?*, [w:] *Handbook of Research on Social Entrepreneurship*, Cheltenham 2010.

Kisilowski M., *Co dalej z zarządzaniem publicznym?*, [w:] *Co dalej z zarządzaniem?*, red. G. Gierszewska, Warszawa 2018.

Kordel P. *et al.*, *Inteligentne organizacje – zarządzanie wiedzą i kompetencjami pracowników*, Warszawa 2010.

Koncepcje zarządzania. Podręcznik akademicki, red. M. Czerska, A.A. Szpitter, Warszawa 2010.

Kowalski Ł., *Inteligentne miasta – przegląd rozwiązań*, [w:] *Miasto w badaniach geografów*, t. II, red. M. Soja, A. Zborowski, Kraków 2015.

Kożuch A. *et al.*, *Obszary zarządzania publicznego*, Kraków 2016 (Monografie i Studia Instytutu Spraw Publicznych Uniwersytetu Jagiellońskiego).

Kuc B., Ścibiorek Z., *Zarys metodologii nauk o bezpieczeństwie*, Toruń 2018.

Kudłacz M., Mazur-Kurach P., *Formy zarządzania publicznego w kontekście rozwoju miast w Polsce*, „Zarządzanie Publiczne" 2015, nr 4 (34).

Lazarević S., Lukić J., *Building Smart Organization Through Learning, and Development of Employees*, [w:] *Creative Education for Employment Growth*, International Conference: Employment, Education and Entrepreneurship, 14–16 October 2015, Belgrade, Serbia.

Lichtarski J., *Praktyczny wymiar nauk o zarządzaniu*, Warszawa 2015.

Lisiński M., *Problemy badawcze i metody ich rozwiązywania w naukach o zarządzaniu*, „Ekonomika i Organizacja Przedsiębiorstwa" 2017, nr 8.

Lonc E., Kantowicz E., *Ekologia i ochrona środowiska. Podręcznik dla studentów*, Wałbrzych 2005.

Łobejko S., *Trendy rozwojowe inteligentnych organizacji w globalnej gospodarce*, PARP, Warszawa 2009, https://www.parp.gov.pl/storage/publications/pdf/2009_trendy_rozwojowe_lobejko.pdf [dostęp: 15.01.2018].

Madajová M., Mpumwire S., Pallabi Mishra P., *Social Entrepreneurship: The Dual Role of Bricolage on Innovation*, 2017.05.30. Master`s thesis. Departament of Business Studies, Uppsala University, https://pdfs.semanticscholar.org/8914/702083e4f577f25c53b50ae67e8572adc088.pdf?_ga=2.218432026.2022962652.1576007701-327157607.1576007701 [dostęp: 15.01.2018].

Markowski T., *Zarządzanie rozwojem miast*, Warszawa 1999.

Martyniuk-Pęczek J., Parteka T., Martyniuk O., *Idea* smart city *w kontekście rozwoju przedsiębiorczości na przedmieściach*, „Biuletyn KPZP" (Komitet Przestrzennego Zagospodarowania Kraju, PAN) 2015, nr 257–258.

Nowosielski S., *Koncepcje zarządzania organizacją. Problemy terminologiczne*, [w:] *Zarządzanie w teorii*, red. M. Przybyła, Wrocław 2010, s. 13–23 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 137, Nauki o Zarządzaniu, nr 4).

Parysek J.J., *Miasto w ujęciu systemowym*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2015, R. LXXVII, z. 1.
Rokita J., *Zarządzanie strategiczne. Tworzenie i utrzymywanie przewagi konkurencyjnej*, Warszawa 2005.
Rożałowska B., Macełko M., *Miasto jako organizacja ucząca się. O znaczeniu idei inteligentnego miasta (obywatela) w społeczeństwie informacyjnym*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2015, z. 79.
Sikora-Fernandez D., *Koncepcja „smart city" w założeniach polityki rozwoju miasta – polska perspektywa*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2013, nr 290.
Sikora-Fernandez D., Smart city *jako nowa koncepcja funkcjonowania i rozwoju miast w Polsce*, [w:] *Gospodarka przestrzenna. Dylematy i wyzwania współczesności*, red. J. Potocki, J. Ładysz, Wrocław 2014 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 339).
Sobczak T., *O koncepcjach i metodach w naukach o zarządzaniu w Polsce – raz jeszcze,* „Przegląd Organizacji" 2017, nr 5.
Sobol A., *Inteligentne miasta versus zrównoważone miasta*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 320.
Sobolewska O*., Co dalej z miastami? Drogowskaz dla miast → „SMART"*, [w:] *Co dalej z zarządzaniem?*, red. G. Gierszewska, Warszawa 2018.
Sokołowska S. *et al.*, *Koncepcje organizacji i metody zarządzania. Możliwości i ograniczenia*, Warszawa 2016.
Stawasz D., Sikora-Fernandez D., *Koncepcja* smart city *na tle procesów i uwarunkowań rozwoju współczesnych miast*, Łódź 2016.
Stęplewski B., *Podstawy niemilitarnego zarządzania kryzysowego*, Kraków 2017.
Szołtysek J., Otręba R., *Zarządzanie miastem i jego wpływ na jakość życia mieszkańców miast województwa śląskiego – doniesienie badawcze*, „Problemy Rozwoju Miast. Kwartalnik Naukowy Instytutu Rozwoju Miast" 2015, R. XII, z. 2.
Szomański B., *Zarządzanie incydentami. Praktyka, zalecenia i wnioski dla kierownictwa*, [w:] *Co dalej z zarządzaniem*?, red. G. Gierszewska, Warszawa 2018.
Wiśniewski M., Kisilowski M., Marczewski M., *Zasady budowy scenariuszy zdarzeń niekorzystnych w publicznym zarządzaniu kryzysowym*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, red. M. Ćwiklicki, M. Jabłoński, S. Mazur, Kraków 2016.
Woźniak J., *The Negative Implications of Offshoring and Strategic Economic Security of Business Organizations*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie" 2015, nr 104.
Wrana K., Kmieć T., Kmieć B., *Zarządzanie miastem w chmurze – cloud city*, [w:] *Partnerstwo i odpowiedzialność w funkcjonowaniu miasta*, red. T. Markowski, D. Stawasz, Warszawa 2014.
Zakrzewska-Półtorak A., *Inteligentne miasto katalizatorem rozwoju regionu?*, [w:] *Gospodarka przestrzenna XXI wieku*, red. A. Zakrzewska-Półtorak, P. Hajduga, M. Rogowska, Wrocław 2016 (Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, nr 443).

Wykorzystanie dorobku nauk o zarządzaniu na rzecz podnoszenia bezpieczeństwa miast. Koncepcja smart

Streszczenie

W artykule opisano pojęcie organizacji inteligentnej i odniesiono je do koncepcji miasta inteligentnego (*smart city*). Wskazano miejsce bezpieczeństwa w tej koncepcji. Dokonano przeglądu koncepcji, metod i technik zarządzania wykorzystywanych w organizacjach. Odniesiono się do możliwości rozwiązywania problemów badawczych i wykorzystania metod zarządzania na rzecz podniesienia poziomu bezpieczeństwa miast. Omówiono kwestie planowania cywilnego, zarządzania incydentami i scenariuszy zdarzeń krytycznych w działaniach na rzecz bezpieczeństwa miast. Odniesiono się do metod wykorzystywanych w zarządzaniu kryzysowym. Sformułowano i uzasadniono tezę, że poziom bezpieczeństwa miast może być podniesiony poprzez wykorzystanie koncepcji, metod i narzędzi zarządzania opartych na koncepcji organizacji inteligentnej. Wskazano kierunki dalszych badań na rzecz bezpieczeństwa miast, w tym problematykę menadżerskiego zarządzania miastem z wykorzystaniem dorobku dotyczącego sprężystości (*resilience*) organizacji oraz brikolażu (*bricolage*).
Słowa kluczowe: miasto inteligentne, metody zarządzania, zarządzanie bezpieczeństwem

Taking Advantage of the Achievements of Management Sciences to Enhance City Security: The Smart Concept

Abstract

This paper looks at the notion of a smart organisation by referring it to the concept of a smart city. It makes an attempt to properly locate the notion of security within the smart city concept by reviewing a selection of management concepts, methods and techniques applied in organisations. A reference has also been made to the possibility of solving research problems and use management methods in favour of city security. The author points to the numerous possibilities of taking advantage of the achievements of management sciences and discussed selected issues of civil planning, incident management and critical event scenarios for actions in favour of city security. Reference has also been made to the methods used in crisis management. The underlying thesis that the city security level may be increased by using management concepts, methods, based on the concept of a smart organisation has been substantiated along with an indication of directions for further research regarding city security and issues in smart city management based on the achievements in the field of organisation resilience and bricolage.
Key words: smart city, methods of management, security management

Nutzung des Leistungen der Managementwissenschaften für die Verbesserung der Sicherheit der Städte. Smart – Konzept

Zusammenfassung

Im Artikel wurde das Phänomen der intelligenten Organisation in Bezug auf das Konzept einer intelligenten Stadt (*smart city*) beschrieben. Es wurde der Platz der Sicherheit

in diesem Konzept festgelegt. Es wurden das Konzept und die in den Organisationen benutzten Managementmethoden und Managementtechniken analysiert. Es wurde auf die Möglichkeit der Untersuchung der Forschungsfragen und Nutzung der Managementmethoden für die Verbesserung der Sicherheit in den Städten Bezug genommen. Man wies auf die Möglichkeit der Nutzung der Leistung der Managementwissenschaften hin. Es wurden Probleme der zivilen Planung, des Incident-Managements und Szenarien der kritischen Ereignisse in den Maßnahmen für die Sicherheit der Städte behandelt. Es wurde Bezug auf die bei dem Krisenmanagement genutzten Methoden genommen. Es wurde die These formuliert und begründet, dass das Niveau der Städtesicherheit durch Nutzung der auf die intelligente Organisation gestützten Managementkonzepte, Methoden und Instrumente verbessert werden kann. Es wurden die Richtungen weiterer Forschung zugunsten der Sicherheit der Städte aufgeführt, darin das Problem des Managings einer Stadt mit Nutzung der Leistung zur Widerstandsfähigkeit (*resilience*) von Organsationen und Bricolage (*bricolage*).
Schlüsselwörter: intelligente Stadt, Managementmethoden, Sicherheitsmanagement

Использования достижений наук об управлении в сфере повышения безопасности городов. Концепция smart Резюме

В статье изложено понятие «умная организация» и рассмотрено концепцию «умного города» (smart city). Указано место безопасности в этой концепции. Приведены примеры понятий, методов и приемов управления, применяемых в организациях. Рассмотрены возможности решения исследовательских проблем с использованием методов управления, способствующих повышению уровня безопасности городов. Обсуждены вопросы гражданского планирования, управления инцидентами и сценарии критических событий, которые дают возможность обеспечить безопасность городам. Рассмотрены методы, используемые в антикризисном управлении. Сформулировано и обоснованно тезис о том, что уровень безопасности городов может быть повышен благодаря использованию концепций, методов и инструментов управления, базирующихся на концепции «умной организации». Указано направления дальнейших исследований по обеспечению безопасности городов, в том числе затрагивающих проблематику менеджмента городом с использованием знаний, касающихся устойчивости (resilience) организации и «бриколажа».
Ключевые слова: «умный город», методы управления, управление безопасностью

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-003

Andrzej Marjański

dr, Społeczna Akademia Nauk w Łodzi
ORCID: 0000-0001-6534-2632

Jarosław Ropęga

dr hab., prof. UŁ, Uniwersytet Łódzki
ORCID: 0000-0002-2435-4239

Ochotnicze Straże Pożarne. Zapewnienie efektu synergii w zarządzaniu kryzysowym

Wprowadzenie

Współczesne zagrożenia rozwijają się w sposób turbulentny i praktycznie nie ma ograniczeń w powstawaniu nowych[1] – zagrożenia charakteryzują się obecnie nie tylko nieprzewidywalnością i zmiennością, ale także wzajemnym przenikaniem i obejmowaniem prawie wszystkich dziedzin funkcjonowania społeczeństwa. W literaturze przedmiotu zidentyfikowano wiele rodzajów zagrożeń, ale zawsze efektem zagrożenia bezpieczeństwa jest wystąpienie kryzysu, który jest momentem przełomu, przesilenia. Kryzys stanowi także kulminacyjną fazę zagrożenia, w której następuje punkt zwrotny jakiegoś procesu: często dochodzi do utraty kontroli nad powstałą sytuacją kryzysową, a podmiot będący w sytuacji kryzysowej może ulec likwidacji, destrukcji lub powrócić do normalności[2]. Kryzys zawsze jest związany z brakiem bezpieczeństwa i prowadzi do zachwiania normalnych procesów funkcjonowania (realizacji

[1] F. Mroczko, *Problemy bezpieczeństwa i porządku publicznego*, „Zeszyty Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości" 2010, nr 14 (1), s. 33–41.

[2] M. Marszałek, G. Sobolewski, D. Majchrzak, *Zarządzanie kryzysowe w ujęciu narodowym i międzynarodowym*, Warszawa 2012, s. 31.

celów) oraz braku równowagi podmiotu. Kryzysom nie można w pełni zapobiegać, można jedynie się na nie przygotowywać i strać się ograniczać sytuacje wywołujące kryzys i minimalizować jego skutki[3].

Zapewnienie obywatelom bezpieczeństwa i warunków do ochrony przed zagrożeniami oraz reagowania w przypadku wystąpienia zagrożenia jest jednym z najstarszych, jeżeli nie najstarszym zadaniem władzy publicznej[4]. Państwo, które jest najwyższą formą reprezentacji społeczeństwa, przyjęło na siebie wiele obowiązków związanych z zapewnieniem bezpieczeństwa zarówno jednostkom, jak i grupom społecznym[5]. Nie oznacza to jednak, że w realizacji tych zadań biorą udział wyłącznie podmioty rządowe i samorządowe. Duże znaczenie zapewnieniu sprawności działania systemu zarządzania kryzysowego mają także organizacje pozarządowe, a w wśród nich Ochotnicze Straże Pożarne[6].

Postęp w różnych dziedzinach życia społecznego przynosi z jednej strony poprawę warunków życiowych, z drugiej jednak – możliwość występowania wielu niepożądanych zagrożeń: naturalnych, cywilizacyjnych, a nawet aktów terrorystycznych. W rozwoju zarządzania kryzysowego wykorzystuje się doświadczenia wielu pokoleń – dotyczące zagrożeń w wymiarze jednostkowym, lokalnym, narodowym i międzynarodowym. Od lat też prowadzone są badania procesów zarządzania w sytuacjach trudnych i ekstremalnych. Dzięki tomu możliwe było ukierunkowanie rozwoju zarządzania kryzysowego na zwiększanie poziomu bezpieczeństwa[7].

Problematyka zarządzania kryzysowego staje się coraz bardziej istotna ze względu na licznie pojawiające się nowe zagrożenia, często nieprzewidywalne. Państwo i jego organy są odpowiedzialne za funkcjonowanie systemu, który będzie w stanie skutecznie ograniczać występowanie zagrożeń oraz reagować w przypadku ich pojawienia się[8]. Zapewnienie bezpieczeństwa uznaje się za podstawę dobrego funkcjonowania państwa i jego społeczeństwa[9]. Wymaga to stworzenia systemu obejmującego szereg wyspecjalizowanych podmiotów – wykorzystujących bogatą, często interdyscyplinarną wiedzę i doświadczenie oraz zróżnicowane zasoby.

[3] M. Kopczewski, Z. Ciekanowski, A. Marjański, *Planowanie i organizacja działań w sytuacjach kryzysowych*, [w:] *Determinanty współczesnych zagrożeń bezpieczeństwa państwa*, red. J. Nowicka, S. Krysiński, K. Rejman, Jarosław 2018, s. 215.

[4] M. Kwieciński, *Niektóre niedoceniane rodzaje zagrożeń bezpieczeństwa publicznego w Polsce – wyzwania dla procesów zarządzania*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*, s. 21–28.

[5] J. Ziarko, *Sytuacje społeczne zagrażające bezpieczeństwu człowieka – uwarunkowania ich postrzegania i diagnozowania*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*, s. 43–57.

[6] M. Lisiecki, *Sprawność zarządzania organizacjami publicznymi funkcjonującymi na rzecz bezpieczeństwa obywateli*, „Studia Ekonomiczne" 2013, nr 168, s. 162–173.

[7] M. Kopczewski, S. Niedzwiecki, *Zintegrowany system ratowniczy elementem zarządzania kryzysowego*, „Przegląd Naukowo-Metodyczny" 2019, nr 1 (42), s. 265–276.

[8] G. Sobolewski, *Pożądane kierunki zmian i rozwoju systemu zarządzania kryzysowego RP*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, red. D. Wróblewski, Józefów 2015, s. 153.

[9] S. Choenni, E. Leertouwer, *Public Safety Mashups to Support Policy Makers*, [w:] *Electronic Government and the Information Systems Perspective*, red. K.N. Andersen, E. Francesconi, Å. Grönlund, T.M. van Engers, Berlin–Heidelberg 2010, s. 234.

W tym celu w Polsce stworzono system zarządzania kryzysowego, w którym funkcjonuje wiele różnorodnych podmiotów. Ich współdziałanie powinno zapewniać osiągnięcie efektów synergicznych, co jest szczególnie ważne w przypadku prowadzenia działań ratowniczych. System bazuje na rozwiązaniach prawnych, strukturach organizacyjnych i zasobach, uzupełniając je o zagadnienia związane z planowaniem i koordynacją. Jednym z kluczowych założeń tego systemu jest właśnie efekt synergii, który pozwala na osiąganie wysokiej efektywności, bez konieczności dublowania zadań i ponoszenia zbędnych kosztów[10]. Skuteczność działania systemu w sposób bezpośredni przekłada się na bezpieczeństwo ludzi, ochronę ich życia i zdrowia.

Hipoteza niniejszego opracowania brzmi: Organizacja systemu zarządzania kryzysowego musi być ukierunkowana na stałe osiąganie efektu synergii we współdziałaniu wielu podmiotów. Ochotnicze Straże Pożarne (OSP), stanowiące pozarządowy element systemu, w zasadniczym stopniu wpływają na osiąganie efektu synergii w działaniach ratowniczych. Jednak występuje coraz więcej czynników wpływających negatywnie na możliwości udziału OSP w zarządzaniu kryzysowym.

Celem artykułu jest dokonanie koniecznej z perspektywy teorii i praktyki zarządzania analizy roli Ochotniczych Straży Pożarnych w zarządzaniu kryzysowym w Polsce. Zwrócono uwagę na rolę Krajowego Systemu Ratowniczo-Gaśniczego oraz znaczenie udziału w nim OSP. Na podstawie wyników przeprowadzonych badań wskazano negatywne czynniki, które wpływają na ograniczenie aktywności OSP w działaniach Krajowego Systemu Ratowniczo-Gaśniczego (KSRG), a tym samym – mają istotny wpływ na ograniczenie efektu synergii w działaniach ratowniczo-gaśniczych i na zmniejszenie sprawności całego systemu.

Synergia jako zasada organizacji zadań zarządzania kryzysowego

Zarządzanie kryzysowe i jego organizacja stanowi zadanie organów administracji publicznej. Jest to złożony system, zbudowany z zasobów państwa, ale także społeczeństwa, ukierunkowany celowo na zapewnienie bezpieczeństwa ludzi, mienia i środowiska naturalnego. Stanowi ważny obszar zarządzania publicznego[11]. Jest realizowane przez władze publiczne przy współudziale wielu instytucji, organizacji i społeczeństwa[12]. Polega na zapobieganiu sytuacjom kryzysowym mogącym powstać w wyniku eskalacji zagrożeń, przygotowaniu do przejmowania nad nimi kontroli w oparciu o zaplanowane działania oraz reagowaniu w przypadku wystąpienia sytuacji kryzysowych, a następnie usuwaniu ich skutków oraz odtworzeniu zasobów i infrastruktury krytycznej[13]. Jego celem jest niedopuszczenie do powstawania sytuacji kryzysowych

[10] W. Skomra, *Zarządzanie kryzysowe. Praktyczny przewodnik*, Wrocław 2016, s. 29.

[11] K. Sienkiewicz-Małyjurek, *Zarządzanie bezpieczeństwem publicznym w samorządzie lokalnym – istota i inicjatywy*, „Organizacja i Zarządzanie" 2011, nr 1, s. 135–149.

[12] K. Sienkiewicz-Małyjurek, *Problemy organizacyjne zarządzania kryzysowego w samorządach*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2011, nr 59 (1864), s. 119–130.

[13] M. Gikiewicz, *Zarządzanie kryzysowe w strukturze administracji samorządowej*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych…*, s. 220.

poprzez podejmowanie działań prewencyjnych i przygotowanie systemu do działania w przypadku powstania zagrożenia – wtedy istotne znaczenie ma skuteczność reagowania, zapewniająca minimalizację negatywnego wpływu zagrożenia na podmiot, któremu niesiona jest pomoc. Ustawa o zarządzaniu kryzysowym[14] stanowi dokument systemowy określający organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania, a także zasady finansowania zadań realizowanych w tym zakresie[15]. Skuteczne zarządzanie kryzysowe ma wymiar sieciowy i musi być ukierunkowane na osiąganie efektu synergii we wzajemnych oddziaływaniach pomiędzy podmiotami uczestniczącymi w systemie.

Efekt synergii stanowi jedno z kluczowych pojęć w naukach o zarządzaniu. Biorąc pod uwagę wysoki stopień złożoności systemu zarządzania kryzysowego, należy poszukiwać jego funkcjonowaniu wielu przejawów efektu synergii[16]. W literaturze przedmiotu można wyróżnić trzy główne ujęcia synergii: procesowe (dynamiczne), wynikowe (statyczne) i uwzględniające typ mechanizmu zachodzącego w wyniki oddziaływania elementów[17]. Istotę synergii można określić jako podjęcie procesu współdziałania dwóch lub więcej czynników pozwalającego na uzyskanie efektu większego od łącznej interakcji efektu ich osobnego działania[18]. Natomiast określenie efekt synergiczny sugeruje, że zjawisko synergii należy wiązać z występowaniem określonych efektów[19].

Pojęcia te są jednak rzadko używane w zarządzaniu kryzysowym. Wykorzystywane są głównie w kręgach menedżerskich w odniesieniu do podmiotów komercyjnych oraz jednostek działających w ich ramach, gdzie osiągnięcie synergii stwarza możliwość zwiększenia efektywności działania i konkurencyjności podmiotu. Zapewnienie efektu synergii stanowi główną przesłankę tworzenia różnego rodzaju zespołów. Osiągnięcie przez zespół „wartości dodanej" wynika z połączenia pracy, wiedzy oraz umiejętności pojedynczych osób. Zespół jest w stanie osiągnąć pożądane efekty po spełnieniu szeregu wymagań, m.in.: odpowiedniego doboru członków zespołu, tak aby nie występowały dominujące indywidualności, właściwego kierowania zespołem, synchronizacji działania oraz odpowiedniego podziału ról i obowiązków.

Może występować również ujemny efekt synergii – co oznacza, że efekty uzyskiwane przez zespół są mniejsze niż suma efektów wygenerowanych przez pojedynczych członków zespołu. Powstanie takiego efektu może wynikać z nieskutecznego działania zespołów lub jednostek organizacyjnych niemających dopasowania strategicznego. Często słabe efekty są wynikiem braku zrozumienia pomiędzy członkami zespołu, którzy nie są w stanie podjąć wspólnej decyzji, gdyż są przekonani wyłącznie do swoich racji i nie uwzględniają opinii innych.

[14] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r., nr 89, poz. 590 z poźn. zm.

[15] A. Olszewski, B. Krzywicki, *Budowa systemu informatycznego wspierającego przygotowywanie planów zarządzania kryzysowego RISKO*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych…*, s. 83.

[16] M. Bielski, *Organizacje. Istota, struktury, procesy*, Łódź 1996, s. 77–78.

[17] J. Miklińska, *Efekty synergiczne w funkcjonowaniu centrum logistycznego*, „Logistyka" 2011, nr 3, s. 1905–1914.

[18] R.W. Griffin, *Podstawy zarządzania organizacjami*, tłum. M. Rusiński, Warszawa 2004, s. 55–56.

[19] J. Miklińska, *op. cit.*, s. 1905–1914.

W zarządzaniu kryzysowym niezbędne jest stałe poszukiwanie dodatnich efektów synergicznych oraz ograniczanie czynników, które mogą być powodem powstawania efektu ujemnego. Powinno to dotyczyć przede wszystkim zapobiegania powstawaniu sytuacji kryzysowych, a w przypadku ich wystąpienia – skuteczności ratowania życia i zdrowia poszkodowanych oraz zmniejszania powstałych strat. Istotne znaczenie mają także kwestie związane z zarządzaniem i ponoszonymi kosztami. Winno się dążyć do optymalizacji kosztów, unikania dublowania podejmowanych działań i ponoszonych wydatków oraz do jak najbardziej efektywnego wykorzystania dostępnych zasobów.

Efektów synergicznych można poszukiwać w wielu obszarach, zarówno organizacyjnych, jak i prawnych. Są to m.in.: efektywne rozwiązania organizacyjne i koordynacja poszczególnych elementów systemu; właściwe stanowienie prawa; terminowe i trafne podejmowanie decyzji; właściwe uprawnienia kompetencyjne osób funkcyjnych w systemie zarządzania kryzysowego; uwzględnienie w planach zarządzania kryzysowego sił i środków możliwych do szybkiego użycia w sytuacji kryzysowej; tworzenie i doskonalenie procedur działania; opracowywanie metod rozwiazywania hipotetycznych sytuacji kryzysowych; systematyczne szkolenie podmiotów uczestniczących w systemie i koordynowanie ich współdziałania; uwzględnienie specyfiki poszczególnych podmiotów uczestniczących w systemie.

System zarządzania kryzysowego, który tworzą organy administracji publicznej, określany jest mianem podsystemu kierowania[20]. Organy administracji publicznej powołują centra zarządzania kryzysowego oraz zespoły zarządzania kryzysowego na szczeblu gminnym, powiatowym, wojewódzkim i rządowym. Zarządzanie kryzysowe oparte jest na zasadzie prymatu terytorialnego, co oznacza, że główny ciężar decyzji i odpowiedzialności spoczywa na władzy funkcjonującej na danym poziomie podziału terytorialnego państwa, na którym wystąpiła sytuacja kryzysowa. Władze administracyjne zobowiązane są do posiadania zasobów niezbędnych do realizacji zadań zarządzania kryzysowego, tj.: struktur zarządzania kryzysowego w urzędach, służb ratowniczych, służb porządku publicznego, straży i inspekcji oraz innych podmiotów, z którymi zawarto porozumienia. W przypadku posiadania niewystarczających sił i środków lub gdy sytuacja kryzysowa obejmuje kilka jednostek administracyjnych, odpowiedzialność za jej rozwiązanie przejmuje organ nadrzędny[21].

Zarządzanie kryzysowe w Polsce jest zorganizowane na wszystkich szczeblach administracyjnych, którym zgodnie z Ustawą o zarządzaniu kryzysowym przypisano odpowiednie prawa i obowiązki[22]. Do kompetencji organów centralnych należy przede wszystkim tworzenie rozwiązań organizacyjnych oraz procedur działania systemu zarządzania kryzysowego. Natomiast na poziomie wojewódzkim za efektywne funkcjonowanie systemu zarządzania kryzysowego odpowiada wojewoda. W jego kompetencjach leży kierowanie działaniami związanymi zarówno z monitorowaniem, planowaniem, jak i reagowaniem na zagrożenia i usuwaniem ich skutków. Wojewoda jest zwierzchnikiem rządowej administracji zespolonej[23].

[20] M. Marszałek, G. Sobolewski, D. Majchrzak, *op. cit.*, s. 23–24.

[21] A. Olszewski, B. Krzywicki, *op. cit.*, s. 81.

[22] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym...

[23] Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie, Dz.U. z 2009 r., nr 31, poz. 206 z poźn. zm.

Powiat stanowi pośredni szczebel w zarządzaniu kryzysowym. Organem odpowiedzialnym na tym poziomie jest starosta. Zgodnie z zasadą prymatu układu terytorialnego powiat odgrywa szczególną rolę ze względu na występowanie administracji zespolonej oraz lokalizacji służb i straży. Stanowi podstawowy poziom wykonawczy, od którego zaczyna się reagowanie w przypadku wystąpienia sytuacji kryzysowej.

Najniższym szczeblem zarządzania kryzysowego jest gmina. Na tym poziomie prowadzone są działania zapobiegawcze, organem odpowiedzialnym jest wójt bądź prezydent miasta. W gminach funkcjonują Ochotnicze Straże Pożarne, stanowiące istotny komponent systemu zarządzania kryzysowego. Ważną rolą wójta jest współdziałanie i wspieranie tych podmiotów w realizacji ich zadań na rzecz zapewnienia bezpieczeństwa.

Na każdym poziomie administracji publicznej opracowywany jest plan zarządzania kryzysowego, który obejmuje m.in. analizę występujących zagrożeń, bilans potrzeb oraz posiadanych własnych sił i środków, a także procedury uzyskiwania pomocy zewnętrznej. Planowanie i przygotowanie się na wypadek wystąpienia potencjalnych zagrożeń oraz właściwa koordynacja działań podmiotów uczestniczących w systemie zarządzania kryzysowego ma istotne znaczenie dla zapewnienia jego efektywności i uzyskania efektu synergii bez konieczności znacznego zwiększania środków przeznaczanych na zapewnienie bezpieczeństwa[24]. Zadaniem systemu zarządzania kryzysowego jest dążenie do obniżenia ryzyka wystąpienia zagrożeń, a także stworzenie płaszczyzny do podejmowania działań mających na celu zapewnienie bezpieczeństwa ludności oraz ochrony infrastruktury krytycznej, środowiska naturalnego oraz zapewnienia ich niezakłóconego funkcjonowania[25].

W zarządzaniu kryzysowym oprócz organów administracji publicznej uczestniczy kilka wyspecjalizowanych systemów ratowniczych tworzących podsystem wykonawczy. Są to m.in.: Krajowy System Ratowniczo-Gaśniczy (KSRG) i Państwowe Ratownictwo Medyczne (PRM) oraz System Powiadamiania Ratunkowego (SPR). Powstanie tych systemów jest wynikiem ewolucji zachodzącej w organizacji ratownictwa i dążenia do integracji różnych podmiotów ratowniczych dla ich efektywnego współdziałania[26].

Problematyka organizacji funkcjonowania systemu zarządzania kryzysowego stanowi niezwykle trudne i złożone zagadnienie. O jego złożoności świadczy zarówno różnorodność definiowania, wielorakość zadań, jak i wieloaspektowe powiązania funkcjonalno-strukturalne. Efektywność tego systemu powinna przejawiać się w integracji i osiąganiu synergii dzięki połączeniu wysiłków poszczególnych organów, instytucji oraz służb ratowniczych uczestniczących w systemie[27].

Zarządzanie kryzysowe jest szczególnym przypadkiem zarządzania, ponieważ znaczna jego część (szczególnie w przypadku działań ratowniczych) jest realizowana

[24] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r., s. 15.

[25] K. Sienkiewicz-Małyjurek, B. Kożuch, *System zarządzania bezpieczeństwem publicznym w ujęciu teorii złożoności. Opracowanie modelowe*, „Bezpieczeństwo i Technika Pożarnicza" 2015, t. 37, nr 1, s. 33–43.

[26] J. Kalinko, S. Lipiński, Ł. Kuziora, *Mobilne stanowiska dowodzenia na potrzeby kierującego działaniem ratowniczym*, „Zeszyty Naukowe SGSP" 2017, nr 4 (64), s. 23–44.

[27] G. Sobolewski, *Pożądane kierunki zmian…*, s. 158.

pod presją (głównie czasu) właściwą dla sytuacji zaistnienia zagrożenia i ma na celu rozwiązywanie zaistniałych sytuacji kryzysowych oraz przywracanie stabilności funkcjonowania społeczności i organizacji[28]. Dlatego działania w tym zakresie powinny być podejmowane bez zbędnej zwłoki – tak szybko, jak to jest tylko możliwe. Ma to szczególne znaczenie w działaniach ratowniczych. Z tego powodu zarządzanie kryzysowe odbiega od klasycznego spojrzenia na proces zarządzania i jego funkcje. W związku z tym cele zarządzania kryzysowego nigdy nie mogą być do końca określone, a system musi realizować działania narzucone przez los.

System zarządzania kryzysowego bazuje na istniejących rozwiązaniach prawnych i organizacyjnych oraz zasobach, które uzupełnia o elementy planowania i koordynacji. Działanie systemu realizowane są przez różnorodne zespoły i wymaga interdyscyplinarnej wiedzy, zróżnicowanych umiejętności oraz doświadczenia. Ze względu na swoją specyfikę jest to dynamicznie rozwijający się obszar wiedzy. Konieczne jest stałe dostosowywanie sił i środków do zmieniającego się stanu bezpieczeństwa i utrzymanie zdolności do reagowania we współdziałaniu różnych służb i podmiotów ratowniczych. Dynamizm sytuacji kryzysowych tworzy konieczność wprowadzania ciągłych zmian w zakresie doskonalenia mechanizmów współpracy i procedur działania[29]. Można uznać, że kluczowym zadaniem systemu zarządzania kryzysowego jest wypracowywanie narzędzi umożliwiających efektywne wykorzystanie wszystkich sił i środków uczestniczących w systemie, na każdym poziomie reagowania. Wystąpienie dodatniej synergii jest szczególnie ważne podczas działań ratowniczych podejmowanych przez podmioty uczestniczące w Krajowym Systemie Ratowniczo-Gaśniczym.

Rola Krajowego Systemu Ratowniczo-Gaśniczego w podsystemie wykonawczym zarządzania kryzysowego

Podsystem wykonawczy jest tworzony przez służby, straże, inspekcje oraz szereg innych podmiotów, które dzięki posiadanym zasobom ludzkim oraz technologiom i odpowiedniemu wyposażeniu stanowią zasadniczą siłę w podejmowanych działaniach ratowniczych. Bez niej nawet najbardziej rozbudowany podsystem kierowania i organy odpowiedzialne za bezpieczeństwo nie byłby w stanie realizować swoich ustawowych zadań[30]. Założeniem podsystemu wykonawczego jest zapewnienie ciągłej gotowości do natychmiastowego podjęcia działań ratowniczych przez wyspecjalizowane podmioty ratownicze[31]. W tym obszarze najbardziej widoczna jest potrzeba dążenia do osiągania efektu synergii – dzięki właściwej organizacji współdziałania oraz przestrzeganiu zasad i procedur dotyczących rozwiązywania zaistniałych sytuacji kryzysowych.

[28] M. Kisilowski, *Aspekty prewencji i bezpieczeństwa w publicznym zarządzaniu kryzysowym i logistyce społecznej*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, red. M. Ćwiklicki, M. Jabłoński, S. Mazur, Kraków 2016, s. 85.

[29] K. Sienkiewicz-Małyjurek, *Problemy organizacyjne zarządzania kryzysowego…*, s. 119–130.

[30] G. Sobolewski, *Siły Zbrojne RP w zarządzaniu kryzysowym. Aspekt narodowy i międzynarodowy*, Warszawa 2013, s. 77.

[31] J. Popis, *Krajowy system ratowniczo-gaśniczy w systemie bezpieczeństwa wewnętrznego państwa*, [w:] *Ochrona przeciwpożarowa a bezpieczeństwo państwa*, red. J. Zboina, B. Wiśniewski, Józefów 2014, s. 89.

Kluczową strukturą wykonawczą realizująca zadania w zakresie zapewnienia ochrony życia i zdrowia obywateli oraz mienia i środowiska jest funkcjonujący od 1995 r. Krajowy System Ratowniczo-Gaśniczy, którego organizatorem jest Państwowa Straż Pożarna (PSP). Głównym założeniem tego systemu jest stworzenie jednolitego układu, który dzięki powiązaniu ze sobą różnych podmiotów ratowniczych będzie w stanie podejmować skuteczne działania ratownicze bez względu na rodzaj występującego zagrożenia. KSRG zorganizowany jest na trzech poziomach: powiatowym, wojewódzkim i krajowym. System jest na bieżąco rozwijany i dostosowywany do zmieniających się potrzeb, aktualnie unormowania pochodzą z roku 2017[32].

KSRG zorganizowany jest na trzech poziomach: powiatu, województwa i kraju. Na poziomie powiatu – jako poziomie podstawowym – wykonywane są działania ratownicze na obszarze gmin i powiatu. Poziom wojewódzki jest poziomem wspomagania i koordynacji działań ratowniczych na obszarze województwa. Natomiast poziom krajowy jest poziomem wspomagania i koordynacji działań ratowniczych w całym kraju. Na wszystkich poziomach systemu istotną rolę odgrywają stanowiska kierowania, gdzie następuje obsługa napływających zgłoszeń, dysponowanie do działań ratowniczych sił i środków systemu oraz wspomaganie i koordynacja tych działań i ich ewidencjonowanie[33].

Specyfika systemu powoduje, że funkcjonuje on w dwóch stanach: 1) czuwania i reagowania doraźnego, gdy działania podejmowane są przez własne siły i środki powiatu i tworzących go gmin; 2) wykonywania działań ratowniczych, które wymagają użycia sił i środków spoza powiatu. W tym przypadku uruchamiany jest poziom wspomagania i koordynacji ze szczebla wojewódzkiego lub krajowego.

Działanie systemu w głównej mierze opiera się na Państwowej Straży Pożarnej i Ochotniczych Strażach Pożarnych, a także na innych służbach, inspekcjach, strażach, instytucjach oraz podmiotach, które dobrowolnie w drodze umowy cywilnoprawnej zgodziły się współdziałać w działaniach ratowniczych[34]. Potencjał systemu wg stanu na koniec roku 2018 obrazuje tabela 1.

Ponadto w systemie funkcjonują 22 inne jednostki ochrony przeciwpożarowej: cztery Zakładowe Straże Pożarne, Służba Ratownicza Metra Warszawskiego, Lotniskowa Straż Pożarna Międzynarodowego Portu Lotniczego Balice oraz 16 Wojskowych Straży Pożarnych[35]. System wspomaga wiele innych podmiotów: Policja, Straż Graniczna, Państwowa Inspekcja Środowiska, Instytut Meteorologii i Gospodarki Wodnej, Państwowa Agencja Atomistyki, Stacje Ratownictwa Górniczego, Morska Służba Poszukiwania i Ratownictwa, Lotnicze Pogotowie Ratunkowe. W systemie bierze udział również wiele organizacji pozarządowych: Górskie Ochotnicze Pogotowie Ratunkowe, Tatrzańskie Pogotowie Ratunkowe, Aeroklub Polski oraz Związek Harcerstwa Polskiego, Polski Czerwony Krzyż i Polski Związek Alpinizmu[36].

[32] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 lipca 2017 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego, Dz.U. z 2017 r., poz. 1319.

[33] J. Popis, *op. cit.*, s. 90.

[34] J. Kalinko, S. Lipiński, Ł. Kuziora, *op. cit.*, s. 23–44.

[35] „Biuletyn Informacyjny Państwowej Straży Pożarnej" za rok 2018, s. 37–38.

[36] A. Chodyński, *Interesariusze w kształtowaniu bezpieczeństwa organizacji wobec kryzysu pozaekonomicznego*, „Bezpieczeństwo. Teoria i Praktyka" 2016, nr 4, s. 41–55.

Tabela 1. Potencjał Krajowego Systemu Ratowniczo-Gaśniczego w roku 2018

Województwo	Liczba Jednostek Ratowniczo-Gaśniczych PSP	Liczba posterunków	Liczba szkolnych Jednostek Ratowniczo-Gaśniczych	Liczba OSP włączonych do systemu
dolnośląskie	44	2	0	265
kujawsko-pomorskie	30	0	1	209
lubelskie	29	4	0	314
lubskie	19	0	0	140
łódzkie	34	0	0	335
małopolskie	32	2	1	397
mazowieckie	60	6	1	536
opolskie	17	0	0	162
podkarpackie	27	1	0	320
podlaskie	18	4	0	194
pomorskie	30	2	0	230
śląskie	46	3	1	379
świętokrzyskie	17	1	0	216
warmińsko-mazurskie	24	0	0	189
wielkopolskie	43	0	1	365
zachodniopomorskie	26	4	0	188
Razem	496	29	5	4439

Źródło: opracowanie własne na podstawie: „Biuletyn Informacyjny Państwowej Straży Pożarnej" za rok 2018, s. 37.

Problemem w funkcjonowaniu KSRG są ograniczone siły i środki. To uniwersalny problemem, z którym zmagają się organizacje bez względu na przedmiot ich działania. Także w przypadku systemu należy z jednej strony zapewnić zaangażowanie adekwatnych zasobów, a z drugiej – unikać marnotrawstwa i dążyć do optymalnego wykorzystania dostępnych zasobów. Z tego powodu należy patrzeć na KSRG jako przedmiot zarządzania. Zarządzanie systemem ma prowadzić do osiągania założonych celów w sposób sprawny (tj. pozbawiony marnotrawstwa) i skuteczny (przynoszący spodziewane efekty). Proces zarządzania jest realizowany przy istniejących ograniczeniach finansowych, ludzkich, czasowych, technicznych i informacyjnych oraz uwarunkowaniach zewnętrznych i wewnętrznych. Zarządzanie systemem ma prowadzić do maksymalizacji postawionych celów[37] i pozwalać na uzyskanie wysokiego efektu synergii.

[37] K. Szwarc, *Zapewnianie bezpieczeństwa jako przedmiot zarządzania*, „Studia Bezpieczeństwa Narodowego" 2016, R. XVI, nr 10, s. 131–146.

Ochotnicze Straże Pożarne jako pozarządowy element systemu zarządzania kryzysowego

Organizacje pozarządowe w odróżnieniu od organów publicznych są prywatne i powstają z inicjatywy swoich założycieli. Działają na rzecz realizacji wybranego interesu publicznego, w tym także w zakresie szeroko rozumianego bezpieczeństwa i ratownictwa. Ich celem nie jest osiągnięcie zysku – ani dla siebie, ani dla swoich członków[38]. Ich działanie w większości przypadków opiera się na społecznej pracy ich członków, zatem to od ich aktywności zależy efektywność działania organizacji. W Polsce istnieje ponad 110 tys. różnych organizacji pozarządowych[39].

Organizacje pozarządowe w wielu krajach Unii Europejskiej, w tym także w Polsce, odgrywają ważną rolę w systemie zarządzania kryzysowego. Funkcjonują w strukturach państwa jako niezależne i autonomiczne jednostki prawne. Jednocześnie podejmują się wykonania na rzecz państwa zadań, które bez ich pomocy nie mogłyby być skutecznie wykonywane. Z racji swojego potencjału sił i środków, stopnia wyszkolenia ratowników oraz dysponowania profesjonalnym sprzętem ratowniczym stanowią niezbędne wspomożenie działania innych służb. Państwo może wspierać organizacje pozarządowe w realizacji ich zadań środkami z budżetu[40].

Ochotnicze Straże Pożarne są w Polsce najstarszymi i najbardziej licznymi organizacjami społecznymi zaangażowanymi w działania ratownicze. Ich zasadniczym celem jest realizacja zadań z zakresu bezpieczeństwa ludności, ochrony przeciwpożarowej oraz walki z zagrożeniami naturalnymi i cywilizacyjnymi. Umundurowane i wyposażone w specjalistyczny sprzęt niezbędny do prowadzenia działań ratowniczych, OSP stanowią istotną część sektora pozarządowego uczestniczącego w systemie zarządzania kryzysowego w Polsce. Ich działalność jest prowadzona we współpracy z Państwową Strażą Pożarną oraz organami samorządu terytorialnego.

Szczególną rolę OSP odgrywają na obszarach słabo zurbanizowanych, na terenach wiejskich i w małych miastach, ponieważ tam siły i środki Państwowej Straży Pożarnej są ograniczone i nie zawsze jest ona w stanie samodzielnie prowadzić tam działania ratownicze. W Polsce działa ponad 16 tysięcy Ochotniczych Straży Pożarnych, w których jest zrzeszonych ponad 670 tysięcy członków, głownie mieszkańców wsi i małych miast[41]. W wielu OSP dzięki wysokiemu zaangażowaniu ich członków zgromadzono duże zasoby materialne w postaci nieruchomości, samochodów ratowniczych, sprzętu i wyposażenia. Funkcjonowanie OSP nie ogranicza się do działań ratowniczych – podejmują one także szereg inicjatyw w obszarze profilaktyki i prewencji oraz sportu i kultury. Spełniają zatem istotną funkcję w tworzeniu bezpieczeństwa na poziomie lokalnym[42].

[38] J. Schmidt, *Rozwój organizacji pozarządowych. Teoria i praktyka*, Warszawa 2012, s. 14.

[39] T. Tiszbierek, *Wykorzystanie organizacji pozarządowych w systemie zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych…*, s. 235.

[40] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego…, s. 30.

[41] Sprawozdanie z działalności Związku Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej w XIII kadencji w latach 2012–2017, www.zosprp.pl/files/zjazd/zjazd14/Sprawozdanie%20lata%202012-2017.pdf [dostęp: 19.10.2019].

[42] J. Ropęga, Z. Wilk-Woś, *Zarządzanie funkcjonowaniem i rozwojem OSP poprzez zastosowanie kultury organizacyjnej w celu wzmocnienia bezpieczeństwa mieszkańców gmin*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*, s. 127–142.

Jednym z ważniejszych warunków efektywnego funkcjonowania OSP i ich udziału w działaniach ratowniczych jest – obok właściwego wyposażenia w sprzęt – posiadanie infrastruktury i dostosowywanie jej do współczesnych wymagań. Bariery finansowe i organizacyjne uniemożliwiają OSP samodzielne zrealizowanie tego zadania – do tego potrzebne jest wsparcie zarówno gmin, jak i organów państwa odpowiedzialnych za funkcjonowanie systemu zarządzania kryzysowego[43].

Współcześnie OSP stanowią fenomen społeczny. Działający społecznie strażacy ochotnicy są w każdym momencie gotowi – z narażeniem swojego życia i zdrowia – nieść pomoc potrzebującym. W społecznościach, w których działają, wywierają wpływ na kształtowanie się więzi społecznych i tożsamości ukierunkowanej na ochronę wspólnych wartości i dóbr. Ich szczególny charakter jest widoczny w wysokim poziomie zaufania społecznego, szacowanym na 95%. Jest to najwyższy poziom zaufania społecznego wśród organizacji pozarządowych[44].

Wydaje się, że często pomijany jest czynnik kluczowy dla funkcjonowania Ochotniczych Straży Pożarnych – mianowicie zasoby ludzkie. Pozyskiwanie i rozwój nowych strażaków ochotników ma olbrzymie znaczenie dla zachowania ciągłości działania OSP. Poprzez współpracę ludzi w organizacji dokonuje się przekazywanie zasobów wiedzy, umiejętności oraz kreowanie postaw społecznych. Dzięki wykorzystaniu różnych kompetencji strażaków ochotników może zaistnieć efekt synergii[45]. Niestety coraz powszechniej obserwowanym zjawiskiem jest zmniejszające się zainteresowanie młodych ludzi wstępowaniem w szeregi OSP. Brak nowych pokoleń strażaków ochotników może doprowadzić do ograniczenia udziału OSP w działaniach ratowniczo-gaśniczych podejmowanych przez KSRG. Wydaje się, że ten problem z biegiem czasu będzie narastał i konieczne staje się podjęcie badań nad przyczynami tego zjawiska oraz wdrożenie działań zaradczych.

Ochotnicze Straże Pożarne w podejmowanych przez KSRG działaniach ratowniczych odgrywają szczególną rolę, ponieważ uczestniczą w zapobieganiu występowaniu sytuacji kryzysowych oraz działaniach ratowniczo-gaśniczych. Często OSP nie ustępują podstawowymi kwalifikacjami oraz wyposażeniem Państwowej Straży Pożarnej. Praktyka pokazuje, ze w wielu przypadkach bez udziału strażaków ochotników PSP nie byłaby w stanie prowadzić skutecznych działań ratowniczych. Udział OSP w działaniach ratowniczo-gaśniczych obrazuje tabela 2.

Dane te obrazują istotną rolę OSP w Krajowym Systemie Ratowniczo-Gaśniczym. Bez ich udziału prowadzenie działań ratowniczych byłoby bardzo utrudnione – lub wręcz niemożliwie.

[43] P. Ostachowski, S. Sanetra-Półgrabi, *Regionalne programy wsparcia modernizacji infrastruktury lokalnych jednostek ochrony przeciwpożarowej na przykładzie województwa małopolskiego w latach 2011–2015*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*, s. 101–113.

[44] L. Berliński, *Zarządzanie i dowodzenie Ochotniczą Strażą Pożarną. Wiedza, nowoczesność i tradycja*, Warszawa 2012, s. 11.

[45] J. Ropęga, Z. Wilk-Woś, *op. cit.*, s. 127–142.

Tabela 2. Porównanie udziału strażaków Państwowej Straży Pożarnej i strażaków Ochotniczych Straży Pożarnych w działaniach ratowniczo-gaśniczych w latach 2015–2018

Rok	**2015**	**2016**	**2017**	**2018**
Liczba zdarzeń	489 881	446 819	519 902	502 055
Liczba strażaków PSP	1767 tys.	1688,5 tys.	1848,5 tys.	1941 tys.
Liczba strażaków OSP	1695 tys.	1381 tys.	1733 tys.	1694 tys.

Źródło: opracowanie własne na podstawie: „Biuletyny Informacyjne Państwowej Straży Pożarnej" za lata 2015, 2016, 2017, 2018.

Wnioski z badań

Badania empiryczne zostały przeprowadzone przez autorów w latach 2018–2019. Wykorzystano metodę badań etnograficznych – obejmującą wywiady, obserwację i analizy tekstów. Podejście jakościowe dało możliwość dotarcia do konkretnych przypadków i zrozumienia specyfiki działania badanych OSP oraz relacji w nich zachodzących. Zastosowane metody jakościowe, w odróżnieniu od metod ilościowych, pozwoliły dzięki ograniczeniu uprzedzeń informacyjnych na pozyskanie wiarygodnych danych na tematy „wrażliwie", które były przedmiotem badania. Przeprowadzono 34 wywiady pogłębione, oparte na powtarzalnym scenariuszu badawczym, który stwarzał możliwość zadawania respondentom dodatkowych pytań uszczegółowiających. Dobór respondentów był celowy i obejmował 14 Ochotniczych Straży Pożarnych funkcjonujących na terenie powiatu brzezińskiego w województwie łódzkim, w tym sześć włączonych do Krajowego Systemu Ratowniczo-Gaśniczego. Celem badania było ustalenie wpływu Ochotniczych Straży Pożarnych na efekt synergii w zarządzaniu kryzysowym, a także identyfikacja kluczowych czynników, które w opinii strażaków ochotników wpływają na ograniczenie możliwości osiągania efektu synergii w działaniach OSP powiatu brzezińskiego w systemie zarządzania kryzysowego.

Powiat brzeziński położony jest we wschodniej części województwa łódzkiego i graniczy z powiatami ziemskimi: łowickim, łódzkim wschodnim, skierniewickim, tomaszowski i zgierskim. Jest położony blisko Łodzi, odległość od centrum wynosi ok. 15 km. Powiat tworzą miasto Brzeziny i gminy wiejskie: Brzeziny, Dmosin, Jeżów i Rogów. Powierzchnia powiatu wynosi 358,5 km^2. Na poziomie interwencyjnym pierwszym i najważniejszym elementem Krajowego Systemu Ratowniczo-Gaśniczego w powiecie jest Komenda Powiatowa Państwowej Straży Pożarnej w Brzezinach. Obsada osobowa Komendy Powiatowej obejmuje 43 funkcjonariuszy i dwóch pracowników cywilnych. W Jednostce Ratowniczo-Gaśniczej (JRG) służba strażaków odbywa się w systemie trzyzmianowym. Przy takiej obsadzie kadrowej do działań ratowniczych może wyjechać jednorazowo od czterech do sześciu strażaków PSP. Kolejnym problemem jest czas dojazdu do miejsca zdarzenia. Jedynie w ok. 1/3 powiatu brzezińskiego zastęp JRG jest w stanie dotrzeć w czasie do 8 minut.

Sytuacja ta pokazuje, że występują dysproporcje pomiędzy możliwościami służb państwowych a potrzebami i oczekiwaniami społecznymi w zakresie niesienia pomocy

w stanach zagrożeń. W większości przypadków jako pierwsi działania ratownicze podejmują strażacy ochotnicy z OSP położonych najbliżej miejsca zdarzenia. Ma to olbrzymie znaczenie dla ratowania życia i zdrowia osób poszkodowanych. W powiecie brzezińskim działa 26 OSP, z których osiem jest włączonych do KSRG. W roku 2018 na terenie powiatu miało miejsce 735 zdarzeń wymagających interwencji KSRG. Ochotnicze Straże Pożarne brały udział w 626 zdarzeniach, co stanowi 85% wszystkich zdarzeń[46]. Należy zwrócić uwagę, że przy szczupłości obsady Jednostki Ratowniczo-Gaśniczej to strażacy OSP stanowią główny zasób osobowy w prowadzonych działaniach ratowniczych. Oznacza to, że udział OSP w działaniach ratowniczych jest niezbędny do skutecznego funkcjonowania KSRG. W obszarze działalności ratowniczej z przeprowadzonych wywiadów i obserwacji można wnioskować, że kluczowe czynniki dla efektywności i sprawności działania OSP powiatu brzezińskiego w systemie zarządzania kryzysowego są spełnione, dzięki czemu osiąga się w tym zakresie wysoki efekt synergii.

Zwraca się jednak uwagę na takie kwestie jak niespójny system alarmowania. Zdarzało się, że w pierwszej kolejności alarmowana była JRG w Brzezinach, a dopiero po kilku minutach OSP, w której obszarze działania nastąpiło zdarzenie. W opinii badanych z jednej strony opóźniało to podjęcie działań ratowniczych, a z drugiej – budziło wątpliwości mieszkańców co do możliwości operacyjnych OSP. Zastrzeżenia w niektórych przypadkach budziło dysponowanie do działań ratowniczych OSP mających siedzibę poza gminą, na której terenie nastąpiło zdarzenie. Wskazywano, że jeżeli mieszkańcy widzą, że przy zdarzeniu nie ma miejscowych ochotników, to zaczynają powątpiewać w sens funkcjonowania OSP oraz przenoszą te wątpliwości na forum samorządu gminnego. Zwracano również uwagę na problemy w komunikacji interpersonalnej pomiędzy strażakami PSP a strażakami OSP. Postulowano doprecyzowanie zasad prowadzenia działań ratowniczych na terenach graniczących ze sobą powiatów, ponieważ w niektórych przypadkach pomocy można udzielić szybciej z terenu sąsiedniej gminy, znajdującej się już w innym powiecie. Pomimo poniesienia znacznych kosztów na nowoczesne terminale alarmowania OSP, ze Stanowiska Kierowania Komendanta Powiatowego wysyłana jest jedynie informacja o treści „Alarm pożarowy", bez podania miejsca i charakteru zagrożenia. Przy dzisiejszych możliwościach Systemu Wspomagania Dowodzenia celowe byłoby bardziej szczegółowe określenie rodzaju zdarzenia, co pozwoliłoby na racjonalne podejmowanie działań.

Niestety w obszarze działalności organizacyjnej występuje szereg negatywnych aspektów w relacjach pomiędzy samorządami gminnymi i Komendą Powiatową PSP, utrudniających strażakom wypełnianie ich misji w systemie zarządzania kryzysowego. W obszarze działalności ratowniczej wskazywano, że nie uwzględnia się specyfiki działalności społecznej i nie szanuje się czasu strażaków ochotników. Podawano np., że zebrania i odprawy w Komendzie Powiatowej PSP organizowane są z reguły w godzinach pracy, co powoduje, że aby wziąć udział w zebraniu, trzeba korzystać z urlopu. To wyraźnie zniechęca do aktywnej działalności w zarządach straży.

[46] *Informacja z działalności Komendy Powiatowej Państwowej Straży Pożarnej w Brzezinach za rok 2018*, Brzeziny 2019, s. 3, 4.

Zwracano uwagę, że system dotacji dla OSP działających w systemie ratowniczym powoduje ich destabilizację. Często trzeba przygotowywać plany zakupów z dnia na dzień i to na wyposażenie wskazane przez Państwową Straż Pożarną, a nie rzeczywiście potrzebne danej OSP. Wskazywano, że w ciągu krótkiego czasu po przekazaniu środków finansowych trzeba dokonać zakupów i złożyć rozliczenie. Wysokość dotacji z KSRG nie pozwala na pokrycie kosztów pozyskiwania i utrzymania sprzętu wymaganego przez standardy ratownictwa specjalnościowego. Bolączką jest również nieskorelowanie terminów uruchamiania środków przez samorządy gminne (które swoje budżety uchwalają na początku roku) ze środkami z KSRG, uruchamianymi w drugiej połowie roku. Uniemożliwia to uzyskanie efektu synergii związanego z połączeniem różnych źródeł finansowania.

W obszarze współpracy z samorządem gminnym, na rzecz którego OSP realizują zadania z zakresu zarządzania kryzysowego, wskazywano na niejasne kryteria finansowania i nieuzasadnioną niczym chęć ograniczenia kosztów utrzymania OSP i pomocy w dostosowaniu ich infrastruktury do współczesnych wymagań. Okazuje się, że władze niektórych gmin uważają, że to OSP odpowiadają za stan ochrony przeciwpożarowej i wspomaganie ich działalności przez samorządy jest tylko wyrazem ich dobrej woli. Strażacy ochotnicy muszą stale rozwiązywać problemy związane z niejasnymi regułami współpracy z administracją samorządową oraz nadmiernie rozbudowaną biurokracją administracji, co wydatnie zniechęca do angażowania się w działalność OSP.

Ochotnicze Straże Pożarne stają również przed szeregiem rosnących wyzwań wewnętrznych. W większości OSP coraz wyraźniej widoczny jest problem kadrowy. W szeregi strażaków ochotników nie wstępują nowi członkowie. Zaangażowanie w społeczną działalność straży jest związane nie tylko z prowadzeniem działań ratowniczych, ale także z koniecznością udziału w długotrwałych szkoleniach, ćwiczeniach i badaniach lekarskich Pomimo zgromadzonego profesjonalnego sprzętu pojawiają się problemy z zebraniem niezbędnej liczby strażaków do wyjazdu ratowniczego. Zamierają również realizowane dotąd różne formy aktywności dodatkowej OSP. Jest to zapewne efekt zmian struktury polskiej wsi oraz rozluźnienia więzi społecznych – ale także braku rozwiązań systemowych, takich jak np. wprowadzono w Wojskach Obrony Terytorialnej.

Podsumowanie

Rozwiązania strukturalno-organizacyjne systemu zarządzania kryzysowego w Polsce mają na celu obniżenie poziomu ryzyka związanego z możliwością występowania zagrożeń oraz stworzenie rozwiązań pozwalających na prowadzenie działań na rzecz zapewnienia bezpieczeństwa ludności, ochrony mienia oraz infrastruktury krytycznej i środowiska naturalnego. Działanie systemu zarządzania kryzysowego ma prowadzić do osiągania efektu synergii. Konieczne jest także stałe jego doskonalenie i rozwój. Od osiągnięcia wysokiego poziomu synergii zależy sprawność struktur systemu i możliwości sprostania wyzwaniom i zagrożeniom, a tym samym – efektywność niesienia pomocy ludziom w stanach zagrożenia życia

i zdrowia. Realizowana w praktyce ścisła współpraca wszystkich podmiotów ratowniczych ma bezpośredni wpływ skuteczność prowadzonych działań.

Trzeba umiejętnie wykorzystywać pojawiające się szanse na rozwój systemu i ograniczać zagrożenia. Jednym z kluczowych dodatnich efektów synergii musi być doskonalenie ciągłości podejmowania decyzji i koordynacji działań podmiotów uczestniczących w systemie. Zwiększanie pozytywnego efektu synergii powinno być kluczową zasadą w procesie doskonalenia Krajowego Systemu Ratowniczo-Gaśniczego. Efektywność i spójność systemu wyrażać się będzie synergią we współpracy poszczególnych podmiotów zarządzania kryzysowego – bez względu na to, czy są one zawodowe, czy społeczne.

Ochotnicze Straże Pożarne, a szczególnie ponad cztery tysiące OSP włączonych do Krajowego Systemu Ratowniczo-Gaśniczego, stanowią istotny element systemu zarządzania kryzysowego w Polsce. Ich aktywność w działaniach ratowniczych i niesieniu pomocy w sytuacjach zagrożeń w wielu przypadkach stanowi o efektywności działania systemu, w którym występuje współdziałanie z podmiotami zawodowymi. Jest to także przykład sytuacji, kiedy suwerenna organizacja społeczna oddaje się pod rozkazy profesjonalnej służby, jaką jest Państwowa Straż Pożarna.

Utrzymanie takiego stanu jest szczególnie ważne, ponieważ Krajowy System Ratowniczo-Gaśniczy, który jest organem wykonawczym systemu zarządzania kryzysowego, nie jest w stanie bez udziału dobrze wyposażonych, wyszkolonych i sprawnie działających Ochotniczych Straży Pożarnych osiągnąć efektu synergii w prowadzonych działaniach ratowniczych. Szczególnie jest to odczuwalne w terenach mało zurbanizowanych, w których nie ma zlokalizowanych Jednostek Ratowniczo-Gaśniczych PSP z odpowiednią liczbą strażaków ratowników.

W przypadku działalności społecznej coraz częściej występujące braki legislacyjne oraz rozbieżności unormowań prawnych i różne ich interpretacje powodują ograniczenia w bieżącym funkcjonowaniu oraz rozwoju OSP. Nowe rozwiązania oraz zmiany wprowadzane w sferze udziału OSP w systemie ratownictwa muszą uwzględniać specyfikę ich społecznej działalności oraz prowadzić do zachowania współdziałania wszystkich podmiotów ratowniczych, a tym samym zapewnienia wysokiego efektu synergii. Konieczne jest zrozumienie przez organa zarządzania kryzysowego, że OSP jako organizacje społeczne są z bardzo odporne w czasie prowadzonych działań ratowniczych, ale niezwykle wrażliwe na próby ingerencji w ich wewnętrzne funkcjonowanie i ograniczania ich suwerenności. Potrzebne jest kompleksowe podejście do dalszego zapewnienia udziału OSP w systemie zarządzania kryzysowego, Doskonalenie tego systemu musi mieć na celu eliminację lub ograniczenie czynników mających negatywny wpływ na możliwość osiągnięcia efektu synergii, a przy tym uwzględniać specyfikę funkcjonowania Ochotniczych Straży Pożarnych.

Bibliografia

Berliński L., *Zarządzanie i dowodzenie Ochotniczą Strażą Pożarną. Wiedza, nowoczesność i tradycja*, Warszawa 2012.

Bielski M., *Organizacje. Istota, struktury, procesy*, Łódź 1996.

„Biuletyn Informacyjny Państwowej Straży Pożarnej" za rok 2018.
Chodyński A., *Interesariusze w kształtowaniu bezpieczeństwa organizacji wobec kryzysu pozaekonomicznego*, „Bezpieczeństwo. Teoria i Praktyka" 2016, nr 4.
Choenni S., Leertouwer E., *Public Safety Mashups to Support Policy Makers*, [w:] *Electronic Government and the Information Systems Perspective*, red. K.N. Andersen, E. Francesconi, Å. Grönlund, T.M. van Engers, Berlin–Heidelberg 2010.
Gikiewicz M., *Zarządzanie kryzysowe w strukturze administracji samorządowej*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, red. D. Wróblewski, Józefów 2015.
Griffin R.W., *Podstawy zarządzania organizacjami*, tłum. M. Rusiński, Warszawa 2004.
Informacja z działalności Komendy Powiatowej Państwowej Straży Pożarnej w Brzezinach za rok 2018, Brzeziny 2019.
Kalinko J., Lipiński S., Kuziora Ł., *Mobilne stanowiska dowodzenia na potrzeby kierującego działaniem ratowniczym*, „Zeszyty Naukowe SGSP" 2017, nr 4 (64).
Kisilowski M., *Aspekty prewencji i bezpieczeństwa w publicznym zarządzaniu kryzysowym i logistyce społecznej*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego*, red. M. Ćwiklicki, M. Jabłoński, S. Mazur, Kraków 2016.
Kopczewski M., Ciekanowski Z., Marjański A., *Planowanie i organizacja działań w sytuacjach kryzysowych*, [w:] *Determinanty współczesnych zagrożeń bezpieczeństwa państwa*, red. J. Nowicka, S. Krysiński, K. Rejman, Jarosław 2018.
Kopczewski M., Niedzwiecki S., *Zintegrowany system ratowniczy elementem zarządzania kryzysowego*, „ Przegląd Naukowo-Metodyczny" 2019, nr 1 (42).
Kwieciński M., *Niektóre niedoceniane rodzaje zagrożeń bezpieczeństwa publicznego w Polsce – wyzwania dla procesów zarządzania*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*.
Lisiecki M., *Sprawność zarządzania organizacjami publicznymi funkcjonującymi na rzecz bezpieczeństwa obywateli*, „Studia Ekonomiczne" 2013, nr 168.
Marszałek M., Sobolewski G., Majchrzak D., *Zarządzanie kryzysowe w ujęciu narodowym i międzynarodowym*, Warszawa 2012.
Miklińska J., *Efekty synergiczne w funkcjonowaniu centrum logistycznego*, „Logistyka" 2011, nr 3, s. 1905–1914.
Mroczko F., *Problemy bezpieczeństwa i porządku publicznego*, „Zeszyty Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości" 2010, nr 14 (1).
Olszewski A., Krzywicki B., *Budowa systemu informatycznego wspierającego przygotowywanie planów zarządzania kryzysowego RISKO*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, red. D. Wróblewski, Józefów 2015.
Ostachowski P., Sanetra-Półgrabi S., *Regionalne programy wsparcia modernizacji infrastruktury lokalnych jednostek ochrony przeciwpożarowej na przykładzie województwa małopolskiego w latach 2011–2015,* „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*.
Popis J., *Krajowy system ratowniczo-gaśniczy w systemie bezpieczeństwa wewnętrznego państwa*, [w:] *Ochrona przeciwpożarowa a bezpieczeństwo państwa*, red. J. Zboina, B. Wiśniewski, Józefów 2014.

Ropęga J., Wilk-Woś Z., *Zarządzanie funkcjonowaniem i rozwojem OSP poprzez zastosowanie kultury organizacyjnej w celu wzmocnienia bezpieczeństwa mieszkańców gmin*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*.
Schmidt J., *Rozwój organizacji pozarządowych. Teoria i praktyka*, Warszawa 2012.
Sienkiewicz-Małyjurek K., Kożuch B., *System zarządzania bezpieczeństwem publicznym w ujęciu teorii złożoności. Opracowanie modelowe*, „Bezpieczeństwo i Technika Pożarnicza" 2015, t. 37, nr 1.
Sienkiewicz-Małyjurek K., *Problemy organizacyjne zarządzania kryzysowego w samorządach*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie" 2011, nr 59 (1864).
Sienkiewicz-Małyjurek K., *Zarządzanie bezpieczeństwem publicznym w samorządzie lokalnym – istota i inicjatywy*, „Organizacja i Zarządzanie" 2011, nr 1.
Skomra W., *Zarządzanie kryzysowe. Praktyczny przewodnik*, Wrocław 2016.
Sobolewski G., *Pożądane kierunki zmian i rozwoju systemu zarządzania kryzysowego RP*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, red. D. Wróblewski, Józefów 2015.
Sobolewski G., *Siły Zbrojne RP w zarządzaniu kryzysowym. Aspekt narodowy i międzynarodowy*, Warszawa 2013.
Sprawozdanie z działalności Związku Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej w XIII kadencji w latach 2012–2017, www.zosprp.pl/files/zjazd/zjazd14/Sprawozdanie%20lata%202012-2017.pdf [dostęp: 19.10.2019].
Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, przyjęta uchwałą Rady Ministrów z dnia 9 kwietnia 2013 r.
Szwarc K., *Zapewnianie bezpieczeństwa jako przedmiot zarządzania*, „Studia Bezpieczeństwa Narodowego" 2016, R. XVI, nr 10.
Tiszbierek T., *Wykorzystanie organizacji pozarządowych w systemie zarządzania kryzysowego*, [w:] *Zarządzanie kryzysowe. Wybrane wyniki badań naukowych i prac rozwojowych*, red. D. Wróblewski, Józefów 2015.
Ziarko J., *Sytuacje społeczne zagrażające bezpieczeństwu człowieka – uwarunkowania ich postrzegania i diagnozowania*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 8, cz. II: *Bezpieczeństwo i zagrożenie kryzysowe. Źródła i rodzaje zagrożeń bezpieczeństwa publicznego*.

Akty prawne

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r., nr 89, poz. 590 z poźn. zm.
Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie, Dz.U. z 2009 r., nr 31, poz. 206 z poźn. zm.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 lipca 2017 r. w sprawie szczegółowej organizacji krajowego systemu ratowniczo-gaśniczego, Dz.U. z 2017 r., poz. 1319.

Ochotnicze Straże Pożarne. Zapewnienie efektu synergii w zarządzaniu kryzysowym
Streszczenie

Celem artykułu jest wyjaśnienie – z perspektywy teorii i praktyki zarządzania –znaczenia zapewnienia efektu synergii w zarządzaniu kryzysowym. Wskazano na rolę organizacji pozarządowych, jakimi są Ochotnicze Straże Pożarne, w systemie zarządzania kryzysowego oraz ich wpływ na zapewnienie efektu synergii w działaniach ratowniczych podejmowanych przez Krajowy System Ratowniczo-Gaśniczy. W oparciu o wyniki przeprowadzonych badań podjęto próbę zidentyfikowania czynników mogących prowadzić do ograniczenia aktywności Ochotniczych Straży Pożarnych w działaniach ratowniczych, co może się przełożyć na zmniejszenie efektu synergii w funkcjonowaniu podsystemu wykonawczego, a tym samym – na ograniczenie możliwości niesienia pomocy w stanach nagłego zagrożenia życia, zdrowia, mienia i środowiska.
Słowa kluczowe: synergia, zarządzanie kryzysowe, organizacja systemu bezpieczeństwa Ochotnicze Straże Pożarne

Volunteer Fire Departments and Ensuring the Synergy Effect in Crisis Management
Abstract

The goal of the paper is to explicate the role of ensuring synergy in crisis management from the perspective of management theory and practice. It highlights the role of non-governmental organisations – such as Volunteer Fire Departments – within the crisis management system, and their impact on ensuring synergy effect in rescue operations undertaken by the National Firefighting and Rescue System. Based on the research findings obtained, an attempt was made to identify the negative factors that may limit the activity of the Volunteer Fire Department operations, which may translate into a reduction of the synergy effect in the functioning of the executive subsystem, and thus limit of the possibilities to provide assistance in emergency situation that threaten life, health, property and the natural environment.
Key words: synergy, crisis management, security system organization, Volunteer Fire Departments

Freiwillige Feuerwehren und Gewährleistung der Synergieeffekte beim Krisenmanagement
Zusammefassung

Der Artikel setzt sich zum Ziel die Bedeutung der Gewährleistung der Synergieeffekte beim Krisenmanagement aus der Perspektive der Managementtheorie und der Managementpraxis zu erläutern. Es wurde die Rolle der Nichtregierungsorganisationen, und zwar der Freiwilligen Feuerwehren im System des Krisenmanagements aufgeführt, und ihre Beteiligung bei der Gewährleistung der Synergie in den durch das Landessystem zur Rettung und Feuerlöschung ergriffenen Maßnahmen. Auf der Grundlage der durchgeführten Untersuchungen versuchte man die Faktoren zu identifizieren, welche der Beschränkung der Aktivität der Freiwilligen Feuerwehren beitragen können, was die Verschlechterung der Synergieeffekte im Funktionieren des Teildurchführungssystems

mitbringen kann, und damit sich auf die Begrenzung von Möglichkeit der Hilfeleistung in den Situationen der unmittelbaren Lebens-, Gesundheits-, Vermögens- und Umweltgefahr auswirken kann.
Schlüsselwörter: Synergie, Krisenmanagement, Organisation des Sicherheitssystems, Freiwilligen Feuerwehren

Добровольная пожарная охрана. Обеспечение синергии в антикризисном управлении
Резюме

В статье объяснено, с точки зрения теории и практики управления, значение обеспечения синергетического эффекта в антикризисном управлении. Указано на роль неправительственных организаций, какой является Добровольная пожарная охрана, в системе антикризисного управления и ее влияние на обеспечение эффекта синергии в спасательных операциях Национальной пожарно-спасательной системы. На основании результатов проведенных исследований была предпринята попытка выявления факторов, которые могут привести к ограничению деятельности подразделений Добровольной пожарной охраны во время проведения спасательных операций, что может сказаться на снижении эффекта синергии в функционировании исполнительной подсистемы, и тем самым привести к ограничению возможности оказания помощи в ситуациях угрожающей жизни и здоровью человека, его имуществу, окружающей среде.
Ключевые слова: синергия, антикризисное управление, организация системы безопасности, Добровольная пожарная охрана

BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-004

Jowita Świerczyńska
PhD, Andrzej Frycz Modrzewski Krakow University
ORCID: 0000-0002-6748-9635

The Role of Customs Clearance in Ensuring the Security and Protection of Cross-Border Trade in the European Union

Introduction

Ensuring the security and protection of cross-border trade by the customs authorities of the Member States of the European Union is one of the tasks carried out as part of its protective function. Admittedly, the enforcement of this function – given the existing economic and technological conditions that, on the one hand, are conducive to an increasingly larger economic freedom, and, on the other hand, provide a stimulus for numerous abuses in customs and taxation – plays a pivotal role, as it encompasses a vast array of tasks that are related to traders, the society, the state, and the natural environment. In cross-border trade, the actions that are taken focus primarily on ensuring a fully legitimate system of importing goods into the EU customs territory, and an equally lawful export of goods beyond it. In light of the above, throughout a given transaction, each importer and exporter has to attend to certain formalities set out by the applicable customs legislation, and, therefore, becomes a party to the entire process of customs handling and clearance that is administered by the customs authorities. The quality of this service has an unquestionable importance, as it may have a major impact on the overall safety and security of the trade in goods.

The goal of this paper is to look at the significance of customs clearance throughout the process aimed at safeguarding the security and protection of

cross-border trade in the European Union. The research hypothesis has been formulated as follows: the customs authorities, viewed as the bodies equipped with a comprehensive array of competences in the field of surveillance and control of all the goods transported across the customs borders, can, as part of the European Customs Union, implement modern and coherent solutions that are geared towards ensuring an effective protection of the trade in goods, facilitating customs clearance rather than creating further barriers. The research is based on a descriptive analysis preceded by an overview of the subject literature available, as well as a selection of EU laws and domestic secondary legislation. The overriding theme of the study is a subject of current interest which is of key importance. The research conducted thus far on the role of customs handling and clearance for the assurance of the security and protection of trade has not been sufficiently disseminated. The conclusions drawn, above all, pertain to the subject matter at hand and attempt to fill in the existing gap in the studies conducted so far.

Market security and protection as a key priority area of EU customs administrations

The European Union has a major share in the global trade in goods, estimated at approximately 16%. In 2018, the overall value of trading with non-EU countries stood at over 3.936 billion EUR: the value of import reached 1.980 billion EUR, and the value of export stood at 1.955 billion EUR.[1] It is clear to see that the scale of customs operations is enormous: on average, within the span of one year, approximately 313 million customs declarations are accepted, which equates to about 594 declarations per minute. In 2017 2,140 customs offices handled as many as 332 million customs declarations.[2] The economic growth of the European Union to a large extent hinges upon international trade, which means that the European Union is heavily exposed to a variety of threats that pose a risk to the security and protection of its trading activities.[3] One of the salient objectives set to be attained by all the Member States is the pursuit of the single internal market, which despite the lack of control at the internal borders, guarantees a certain level of safety and security for their citizens, and the natural environment.

The notion of security is clearly ambiguous. Etymologically, the word "security" is derived from the Latin phrase *sine cura* (*securitas*),[4] which means "without care" or without sufficient care, which, in turn, denotes a condition of being free from

[1] *Top Trading Partners 2018 – Trade Statistics*, http://ec.europa.eu/trade/policy/eu-position-in-world-trade/ (accessed: 21.07.2019).

[2] European Commission, *EU Customs Union – Unique in the World*, https://ec.europa.eu/taxation_customs/facts-figures/eu-customs-union-unique-world_en (accessed: 21.07.2019).

[3] European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on Customs Risk Management and Security of the Supply Chain, COM 0793 final, 2012, p. 1.

[4] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004, p. 27.

anxiety or fear; a situation that gives a sense of reassurance.[5] Nowadays, security is frequently associated not only with a condition that guarantees the certainty of existence and survival of a given entity, but it also implies the freedom of its growth. B. Płonka points to the fact that in a number of EU documents, the terms "security" and "protection" are used in various contexts. The notion of "security" appears with reference to the cross-border movement of weapons, explosives, the dual use goods (i.e. for civil and military purposes), biological materials, and chemical and radioactive substances. The term "protection", in turn, is used in connection to the safeguarding of the health and life of citizens and the natural environment, and it denotes the surveillance and control of goods that may spread diseases, hazardous and noxious substances, waste and contaminations, medicines, precursors of drugs, and even goods of everyday use.[6] Since the European Union does not have a single common customs administration, but rather a network of separate domestic authorities competent to handle this particular field of interest, the "customs" area is to a certain degree shaped by solutions adopted in the individual Member States. The EU customs laws and regulations do not create a uniform structure of customs administration, the internal subdivision of competences, or the place of customs bodies in the structure of public administration. The enforcement of these legal provisions has been transferred to each Member State to be handled individually. In line with the overriding principles and assumptions of the treaties that constitute the customs union, the common dimension of activity rests on the application of a unified customs legislation with regard to trading with non-EU countries. This foundation is above all put into practice by the EU Customs Code, and the Common Customs Tariff. Although the enforcement of the provisions that result from these legal acts lies in the hands of each Member State, and the scope of duties and responsibilities of the individual administrations differs, in consequence – with the idea of effective functioning of the European Customs Union in mind – the customs administrations of the Member States ought to act in a manner that ensures that they are a single entity. At the moment, despite the differences, the nature of customs is such that the interaction of the customs authorities is strong enough to make sure that the individual administrative bodies are able to operate as a single entity. The bodies in charge of customs are to a large extent responsible for overseeing the EU's international trading, implementing the external aspects of the internal market, the common trade policy, as well as the remaining common policies of the EU that are related to the trade in goods, not to mention the security of the entire supply chain.[7] Customs administrations have been launching measures geared, in particular, towards the protection of the EU's financial interests and those of its Member States, the protection of the EU

[5] Idem, 'Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych', in D.B. Bobrow, E. Haliżak, R. Zięba (ed.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Warszawa 1997, p. 33.

[6] B. Płonka, 'Zarządzanie bezpieczeństwem obszaru celnego Unii Europejskiej', *Zeszyt Naukowy Wyższej Szkoły Bezpieczeństwa Publicznego i Indywidualnego APEIRON w Krakowie*, vol. 3, 2009, p. 68, http://bazhum.muzhp.pl/media//files/Zeszyt_Naukowy/Zeszyt_Naukowy-r2009-t3/Zeszyt_Naukowy-r2009-t3-s62-72/Zeszyt_Naukowy-r2009-t3-s62-72.pdf (accessed: 24.07.2019).

[7] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L. 269 of 10.10.2013, art. 3.

against unfair and illegal trade at the same time supporting legal commercial activity, safeguarding the security and protection of the EU and its residents, as well as the protection of the natural environment (where applicable, this occurs in close cooperation with other bodies), and maintaining a proper balance between customs controls and facilitating a trade that is fully legitimate.[8]

It is important to highlight the fact that the implementation of the protective function performed by the customs administrations is a truly multidimensional operation, as it regards:

- traders: the customs authorities protect supply chains against the influx of goods as a result of unfair competition, including protection against the potential infringement of intellectual property rights, trademarks, or patent rights. Breaches of intellectual property rights have negative effects for traders, as they generate, among others, lower incomes caused by a decreased demand for legal goods, additional costs generated on account of proceedings and enquiries related to cases that pertain to the protection of intellectual property rights against infringement, and, last but not least, they can also damage the reputation of given trademarks – as the quality of counterfeit goods is frequently worse, which makes them useless. In 2017, numerous EU customs bodies seized over 31 million counterfeit products at EU borders, their overall value going well beyond 580 million EUR. The major country of origin of forged goods that enter the EU customs territory is China, which, along with Hong Kong, is the top-ranked country as regards the largest number of fake mobile phones and related accessories, toners, and CDs/DVDs. Forged clothes, in turn, came mostly from Turkey, and counterfeit and potentially harmful medication originated mainly from India. In 90% of all the reported cases, the goods were destroyed, or appropriate court proceedings were launched to deal with the issue;[9]
- societies: the role of customs authorities is to check whether the goods imported to the territory of the European Union meet the mandatory quality standards, and to check whether the items and/or appliances do not pose a threat to the life, safety and health of EU citizens. A safe product is a product that does not pose any threat to the consumers, or indeed poses a minimal threat related to its use and is regarded as permissible in regular everyday use, taking into account the high level of protection of the security and health of consumers.[10] In 2017, counterfeit and potentially hazardous items used every day – such as health care products, medication, toys, and electrical appliances – constituted 43% of all the seized goods. The largest category of counterfeited items were groceries (24%), followed by toys (11%), cigarettes (9%), and clothes (7%);[11]

[8] *Ibidem*.

[9] European Union, *Rapid Alert System for Dangerous Products – 2017 Annual Report*, Luxembourg 2018, p. 15, https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/reports/docs/Rapex_annual_Report_2017.pdf (accessed: 16.07.2019).

[10] Directive 2001/95/EC of the European Parliament and the Council of 3 December 2001 on general product safety, OJ L 011 of 15.01.2002, art. 2.

[11] *Ibidem*.

- the natural environment: the main task of the customs authorities is to provide the necessary protection against predatory trade in species that are on the verge of extinction, and against the import of hazardous and noxious substances and/or microorganisms. The protection of the natural environment handled by customs administrations plays a pivotal role, although it is frequently underrated, neglected and regarded as a minor responsibility of these bodies. The steps taken focus primarily on: 1) endangered animals and plants, and 2) the movement of waste. Currently, in the majority of cases, those most frequently seized are dead specimens, ready products (mostly handbags, and shoes), and souvenirs. As far as tourists are concerned, a vast majority of their attempts to smuggle across the border what they frequently refer to as "souvenirs" are the consequence of a lack of adequate knowledge and information about the laws related to the protection of animals and/or plants. Beyond the tourist-related trafficking of prohibited specimens, there is yet another side of the issue in question: illegal trade handled by organised criminal groups that treat this kind of activity as a source of massive profits.[12] Detection of the illegal transboundary transport of endangered species of animals and/or plants is indeed a major area of activity for customs authorities, as the European Union is a key import market for the international trade of species featured on the CITES list.[13] In 2017, approximately 106,000 import transactions were reported at a total estimated value of 1.506 million EUR. At the same time, there were over 336,000 export transactions – of which 54% were cases of re-exportation – with a total estimated value of 2.595 million EUR. The overall value of the import of plants stood at 240.8 million EUR, and in the case of export it reached 262 million EUR. In 2017, customs authorities revealed almost 5,000 cases of breaching the provisions of CITES;[14]
- domestic budgets and the EU budget: the customs authorities are the first and last "official contact point" for the goods that are subjected to customs duties and fiscal duties on account of import, and this explains their role as protectors of the state budget against the loss of income generated from the financial payments due. As 80% of the inflows from customs are transferred to the EU budget, and merely 20% of the sums collected are withheld by the Member States as collection costs,[15] ensuring fiscal security plays a major role not only

[12] J. Świerczyńska, 'Bezpieczeństwo i ochrona rynku jako priorytetowy obszar działania europejskiej służby celnej', in J. Rymarczyk, M. Domiter, W. Michalczyk (ed.), *Przemiany strukturalne i koniunkturalne na światowych rynkach*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu No 369, Wrocław 2014, pp. 229–230.

[13] The Convention on International Trade in Endangered Species of Wild Fauna and Flora (also known as the Washington Convention, or CITES) was signed by 21 states on 3 March 1973 in Washington. Poland ratified the document on 3 November 1989, and it has been effective since 12 March 1990. The document contains a list of species of a variety of plants and animals that have been classified as endangered or that could become endangered in the future. The list does not feature animals or plants endangered on account of natural or environmental causes, but rather those that are imperilled due to the human desire to possess them.

[14] European Commission, Directorate General Environment, *EU Wildlife Trade 2017: Analysis of the European Union's annual reports to CITES 2017*, Belgium 2019, pp. 3–26.

[15] Council Decision of 26 May 2014 on the system of own resources of the European Union, No 2014/335/EU, Euratom, L 168, art 2. In 1970, as a result of the Council's decision to establish the

at the level of the Member States. In 2017, the sum total of disclosed losses in customs revenues in Member States stood at 482 million EUR.[16] Abuses related, among others, to evasion or intended customs evasion, indirect taxes and other fees applied to imported goods are immeasurably dangerous from the point of view of the protection of fiscal interest. This explains the vital importance of the need to protect the budget against loss of revenues, and it requires the customs administration bodies of the Member States to shoulder a specific kind of responsibility.

The efficiency of the actions taken by the European Union as a large trading bloc depends on the effective flow of goods into the customs union and out of it, as well as on an unimpeded movement of goods within the single market. The freedom of movement of goods, which implies that each item that crosses the customs border of the European Customs Union and is acknowledged for trading may without any further hindrances circulate in this market, helps to generate irregularities, and in respect to the customs administration it triggers a larger number of requirements as regards security and protection. The fact that the customs bodies act as a guard in cross-border trade is a derivative of a number of factors. Likewise, assigning certain key tasks in this area to customs administration stems from the fact that these bodies have been equipped with full competencies with regard to the surveillance and control of all the goods that are transported across the customs borders, thus safeguarding and facilitating their movement. In practice, this means that because they are viewed as the service that is the most abundantly represented at the customs border, they take actions aimed at ensuring that within the EU's customs territory only such goods are brought in that are safe, and which therefore do not pose a threat to people's life and/or health, do not damage the natural environment, or put public safety at risk.

Within the cross-border trade in goods, the implementation of the protective function plays a major role for the following reasons:

- fiscal reasons: illegal trading in goods leads to losses for domestic budgets on account of unpaid taxes;
- social reasons: here, it is the health aspect that has a fundamental meaning, as launching hazardous goods into the market causes health hazards, and in many cases also for the health of prospective consumers;
- economic reasons: protecting entrepreneurs and manufacturers who act according to the law and observe all the necessary regulations against unfair competition.

Community's own financing resources, the payments due collected by the domestic customs administrations became the first own resources, the so-called Traditional Own Resources (TOR). At the beginning, the customs duties – seen as own resources of the EU's general budget – were adding funds to it at a rate of 90% of the registered payments due. From 2000 to 2013, these proportions stood at 25% and 75%, respectively (Council Decision, 2007/436/EC).

16 European Commission, *Customs sees what you don't… and protects you*, https://ec.europa.eu/taxation_customs/facts-figures/customs-sees-what-you-dont-protects-you_en (accessed: 23.07.2019).

The role of customs clearance in the protection of cross-border trade

Admittedly, the cross-border security of the European Union has to be understood as a process that is the outcome of all the actions geared towards ensuring the safe crossing of the EU's customs border. In trade, what plays a fundamental part is the movement of the freights that are part of the international supply chain across the customs border. The international supply chain is a set of several intertwined elements: entrepreneurs, streams of products, information, and the financial means that flow between them. One of the fundamental goals of the supply chain is to maintain a constant flow – i.e. one without demurrage or disruptions – of goods from the place of their origin to the end buyer.[17] Traders, at the individual stages of the exchange – from the manufacturing phase of a product to the moment in which it is delivered to the consumer based in a different customs area – inevitably become its participants. From the point of view of the customs proceedings, as set out by the recommendation of the European Commission, the group of participants includes, among others, the manufacturer, the exporter, the freight forwarder, the warehouse keeper or another storage facilities operator, the customs agent/representative, the carrier, and the importer.[18] Throughout the execution of a given transaction, the participants of the supply chains have to attend to certain formalities set out by the customs legislation, and, therefore, become a party to the process of the customs service provided by the customs administrations. Following E. Gwardzińska, the customs services include the administrative customs services that are provided by the customs administration, and the customs services that are related to the clearance of goods that can be realised directly by a trader – and, as such, are not customs agency services – or a customs representative, thus becoming a customs agency service.[19] According to the definition adopted by the Customs Service, a customs service is a set of actions taken as part of the tasks carried out by the customs administration aimed at providing a client a number of advantages or benefits in response to his or her needs.[20] Broadly speaking, the notion of customs service encompasses all customs-related formalities performed with regard to the transactions made by the participants of a supply chain in the international trade of goods, carried out before the customs authorities in line with the applicable laws.[21] The threats posed to cross-border security are deeply rooted in the international and global setting, as well as in a variety of external sources. This

17 A. Harrison, R. van Hoek, *Logistics Management and Strategy: Competing through the Supply Chain*, 3rd ed., Harlow 2008, pp. 6–15.

18 European Commission, *Authorised Economic Operators. Guidelines*, TAXUD/B2/047/2011-REV.6, Brussels 2016, pp. 17–20.

19 E. Gwardzińska, *Przedstawicielstwo celne w międzynarodowym obrocie towarowym*, Warszawa 2018, p. 141.

20 Ministerstwo Finansów, *Program e-Cło – e-Usługi*, speech delivered at the conference held on 29.07.2014, Departament Służby Celnej i Cła, Warszawa 2014.

21 J. Świerczyńska, 'Jakość obsługi celnej a konkurencyjność przedsiębiorstw uczestniczących w obrocie międzynarodowym', in P. Antonowicz, E. Malinowska, J. Siciński (ed.) *Sektorowe uwarunkowania funkcjonowania i rozwoju przedsiębiorstw*, Gdańsk 2019, p. 187.

can clearly cause disruptions in the functioning of the supply chain, and/or internal sources, which, in turn, is connected to the use of the supply chain to criminal activities, such as e.g. smuggling weapons of mass destruction, or using a means of transport as a weapon, which turns it into an actual threat for people's health and life, the infrastructure, the economy, or for the level at which a given society feels safe.[22] It is worth highlighting the fact that the biggest threat within a supply chain occurs during the transportation or reloading of goods. Threats typically occur whenever the security measures applied are insufficient and are least expected. As regards the participants of the international supply chains, the threats in cross-border trade are frequently the effect of customs risk.

The notion of risk was added to EU customs legislation in 2005.[23] Since then, working out a single approach of the Member States to managing customs risk has become a major issue of concern against the backdrop of safeguarding the security of the supply chains. Based on the applicable laws of the EU Customs Code, risk implies the likelihood and the impact of an event occurring, with regard to the entry, exit, transit, movement or end-use of goods moved between the customs territory of the European Union and countries or territories outside this territory. It also applies to the presence of non-Union goods within the customs territory of the European Union, which would prevent the correct application of Union or national measures, compromise the financial interests of the Union and its Member States, or pose a threat to the security and safety of the Union and its residents, to human, animal or plant health, to the environment, or to consumers.[24] The number of entities that take part in a supply chain, as well as the diverse nature of their activities, extends the areas of potential customs risk beyond any imaginable limits. As a rule, the threats and risk related to customs stem from customs crimes and petty offences, whose sources are indeed varied. In the transboundary movement of goods, the key sources of risk include:

- behaviour that violates the provisions of customs legislation or the application of measures related to the bans and restrictions, and trade policy measures,
- failure to comply with the applicable customs norms and standards,
- incomplete or improper control of the movement of goods,
- lack of control of the transport of goods,
- inaccurate, insufficient or absolute lack of knowledge about trading partners,
- the likelihood of the appearance of goods as part of unfair competition, goods that infringe the intellectual property rights, goods that fail to comply with EU standards and ones that pose a threat to life and/or health.

[22] World Bank, *Supply Chain Security Guide*, Washington 2009, p. 8.

[23] Regulation (EC) No 648/2005 of the European Parliament and of the Council of 13 April 2005 amending the Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, OJ L 117/13 of 04.05.2005. Pursuant to Article 4, risk implied the likelihood of an event with regard to the entry, exit, transit, movement and end-use of goods moved between the customs territory of the EU and non-EU countries, and the presence of non-Union goods, which would prevent the correct application of EU or national measures, compromise the financial interests of the Union and its Member States, or pose a threat to the security and safety of the Union and its residents, to human, animal or plant health, to the environment or to consumers.

[24] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L. 269 of 10.10.2013, *op. cit*., art. 5, point 7.

Doubtless, it is impossible to fully eradicate the customs risk and all the threats that may occur in the international supply chains. Yet it is worth taking all the possible actions to bring them down to a minimum. This is why the role of the level of customs clearance, which is an intrinsic stage of transactions in the international market, is so important. And, indeed, the quality of this service is a major factor that determines the effectiveness and efficiency of the actions taken within the area of protecting cross-border trade in goods. M. Bugdol points to the following factors that shape the overall quality of customs service: availability of the service, manner of communication, competences, politeness, credibility, responsibility, reliability, security, understanding, and specificity.[25] This proves that quality is indeed the response to a client's expectations. The factors that have an impact on the quality of customs services are the standards of service adopted, and the level at which they are provided. A high quality of customs service necessitates the customs administration taking a modern approach and dynamically adapting to the ever-changing environment. As regards the overall quality of customs service – especially in the cross-border movement of goods – an absolute priority for traders is the time and the cost of the service, the functionality of the services, easy access to information, and a uniform mode of providing the service at all the organisational units of the customs administrations of the Member States. Another major component is the security of the supply chain, as only such a chain can be a source of benefits and profits for traders. Therefore, it is of key importance to make sure that an effective protection of the cross-border trade safeguarded by the customs administrations is geared towards ensuring security in a positive way, i.e. by removing any existing barriers, and streamlining customs procedures. Indeed, the growth of global trade requires a systematic reduction of the level of interference that results from the inspections.[26] A major premise for such a reduction of barriers in customs handling by the European Union are the Framework of Standards to Secure and Facilitate Global Trade of the World Customs Organisation (WCO SAFE Framework).[27] Adopted in 2005, the document introduced modern security standards into a supply chain, enhancing the level of involvement of the customs authorities in the creation of the economic security of the individual states and made it possible to simplify the handling of legal trade. It is made up of four elements:[28]

- harmonisation of the guidelines with regard to advance information about the deliveries of goods;
- taking of a coherent approach with regard to risk management in order to identify risk for the supply chain;

[25] Cf. M. Bugdol, *Zarządzanie jakością w urzędach administracji publicznej. Teoria i praktyka*, Warszawa 2011.

[26] N. Wilson, *Examining the Trade Effect of Certain Customs and Administrative Procedures*, OECD Trade Policy Working Papers, No 42, Paris 2007, p. 18.

[27] World Customs Organization, *SAFE Framework of Standards to Secure and Facilitate Global Trade*, http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/safe_package.aspx (accessed: 15.06.2019).

[28] *Ibidem*.

- in justified cases, applying early risk evaluation, a more invasive approach to the inspection of containers and high-risk loads, based on scanning done with the use of non-invasive methods or physical inspection;
- the benefits that can be gained by enterprises that meet the minimum security standards in a supply chain and will apply the best practices.

The change of the approach to the security of loads in a supply chain that can be discerned after this period regards, among others, the need for the participants of a supply chain to provide more detailed information on the origin, intended use and type of load (including any information documenting the previous stages in the supply chain), and to shift the inspection of a good from the point of destination to the place of shipment, which is the consequence of introducing the duty of providing the customs authorities with detailed information on the freight before it has been loaded onto the means of transport.

The impact of selected instruments of customs clearance on the quality of actions taken in the process of ensuring the security and protection of trade

The catalogue of the customs services provided by the customs authorities of the Member States is broad and is updated on an ongoing basis. It encompasses, among others, the services that result from the implementation of the customs policy, which is the consequence of being part of the EU's customs union; the implementation of incomes generated from customs duties and other payments connected to the entry and exit of goods (collection of fees due, and settlements with the EU and the budget); covering goods with customs procedures and regulating the status of goods related to their entry and exit; identification, detection and combatting criminal offences and petty offences committed with regard to the goods whose sales are subjected to prohibitions and/or restrictions; preventing such incidents, and prosecuting their perpetrators. The obligation undertaken by the customs administrations to guarantee an unimpeded movement of goods necessitates a constant improvement of the relevant tools that facilitate the operations. Having said this, facilitating customs clearance must not have a negative impact on the level of security and protection of the European Union. Reaching a compromise between the number of solutions aimed at reducing the barriers that hinder customs clearance and the need to ensure effective protection – which, in turn, is the key element in the process of safeguarding the security of cross-border trade – is indeed an arduous task, but an attainable one, as proved by experience.

Admittedly, throughout customs clearance, what plays a pivotal role for traders is, above all, the manner in which the customs authorities carry out their controls. Customs controls in cross-border trade are the epitome of the protective function performed by the customs administrations. This tool serves to verify the proper observance of the customs laws and other provisions related to the import and export of goods in the trade activities occurring between the EU and non-EU

countries. Its effect should, on the one hand, be the proper safeguarding of customs and tax dues, and, on the other, a guarantee of the security of trade and the growth of a legal commercial activity. According to the provisions of the Union Customs Code, the notion of "customs controls" implies specific acts performed by the customs authorities in order to ensure compliance with the customs legislation and other legislation governing the entry, exit, transit, movement, storage and end-use of goods moved between the customs territory of the Union and countries or territories outside that territory, and the presence and movement within the customs territory of the Union of non-Union goods and goods placed under the end-use procedure.[29] Customs controls may, among others, consist in examining goods, taking samples, verifying the accuracy and completeness of the information given in a declaration or notification and the existence, authenticity, accuracy and validity of documents, examining the accounts of economic operators and other records, inspecting means of transport, inspecting luggage and other goods carried by or on persons and carrying out official enquiries and other similar acts.[30] The EU applies the system of selective customs controls, based on the risk analysis of the entities that are selected for it. This approach means that it is not an "absolute control of everything", but rather a selective activity geared towards scrutinising specific areas of interest. Customs controls ought to be balanced with facilitating legitimate trade.[31] The ones that currently allow for the concentration of controls to be carried out in areas where the risk of abuses is high are the highly qualified customs officials, effective methods, as well as modern IT-based tools.

Given the fact that the entities that undergo the controls are frequently treated disapprovingly, a variety of solutions have been launched across the European Union that are aimed primarily at upgrading the methods and tools applied in such processes, a case in point being the area of e-services.[32] The significance of applying information and communication technologies to facilitate trade, and at the same time to ensure the effectiveness of controls by lowering the costs incurred by business enterprises and lowering the risk has been laid down explicitly in the Union Customs

[29] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L. 269 of 10.10.2013, *op. cit*., art. 5 point 3.

[30] *Ibidem*, art. 46.

[31] *Ibidem*, art. 3.

[32] The origins of e-facilitations in customs handling and clearance goes back to 2003, when the Council, in its Resolution of 5 December 2003 on creating a simple environment for customs and trade (Council Resolution of 5 December 2003 on creating a simple and paperless environment for customs and trade, OJ C 305 of 16.12.2003, p. 1.), called on the Commission to develop, in close cooperation with the Member States, a long-standing strategic plan with regard to the creation of coherent and inter-operational electronic customs systems, the so-called electronic environment for customs. This document, termed the Multi Annual Strategic Plan, or MASP (European Commission's document TAXUD/477/2004-Rev.7), was developed by the Commission and became the basis for introducing information technology for the European customs union. What had the major impact on simplifying customs clearance was the decision of the European Parliament and Council related to the launching of a pan-European electronic system of customs clearance (Decision No 70/2008/CE of the European Parliament and of the Council of 15 January 2008 on a paperless environment for customs and trade, OJ L 23/21, 2008), whose implementation was possible thanks to the e-Customs Programme (electronic customs).

Code.[33] It has also been emphasised that the use of information and communication technologies should be accompanied by a harmonised and standardised application of customs controls by the Member States to ensure an equivalent level of customs control throughout the Union in order to provide, among others, a balanced level of these controls.[34] In line with the Union Customs Code, the exchange of information (i.e. the declarations, reports, applications, or decisions) between the traders and the customs authorities – as well as the storage of such information – should be carried out by means of electronic data-processing techniques.[35] To this end, major attempts have been made to upgrade and develop a total of 17 IT systems.[36] Most of the activities scheduled to be carried out in this area will be completed by 2020,[37] but in order to guarantee a comprehensive and fully integrated structure in all the Member States of the EU, this effort will most probably continue until 2025.[38] Having data collected electronically makes it easier to process them, associate them, or search them through according to a set of established criteria. Hence, it is necessary to implement all the IT systems so as to make it possible for the customs administrations to manage financial risk and the risk posed to security, and at the same time facilitate trade.[39]

In cross-border trade, there are specific e-services which are an excellent example that proves that it is possible to facilitate commercial activity and at the same time guarantee high standards of security, e.g. the digital border (which allows for an efficient handling of a participant of a supply chain at border crossings with the use of automatic vehicle identification mechanisms and traffic control); notification (which allows to announce the anticipated arrival at a border along with the transfer of data on the goods in advance so as to enable preliminary preparation of the clearance procedure and reduce the waiting time at the border crossing, as well as repeated use of the transferred data in subsequent processes of customs handling); digital clearance (which allows to carry out customs clearance in line with the requirements set by

[33] Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L. 269 of 10.10.2013, *op. cit*., p. 4.

[34] *Ibidem*.

[35] *Ibidem*, art. 6.

[36] This includes 14 trans-European systems (upgraded systems): Binding Tariff Information (BTI), Authorised Economic Operators (AEO), Economic Operators' Registration and Identification (EORI), common customs tariff and surveillance, New Computerised Transit System (NCTS), Automatic Export System (AES), Import Control System (ICS), and new ones: Registered Exporter System (REX), Customs Decisions System (CDS), and Uniform User Management and Digital Signature (UUM&DS.), Guarantee Management (GUM), Proof of Union Status (PoUS), uniform exchange of information for special purposes (INF), Centralised Clearance for Import (CCI).

[37] Implementation of the following projects carried out within the Union Customs Code will be delayed and will be completed after 2020: Automatic Export System, upgrading the New Computerised Transit System (NCTS), guarantee management, special procedures, centralised clearance for import, confirmation of Union customs status of goods and upgrading the import controls system – European Court of Auditors, *A Series of Delays in Customs IT Systems: What Went Wrong?,* Special Report No 26, Brussels 2018, p. 17.

[38] European Commission, Report from the Commission to the European Parliament and the Council on the IT strategy for customs, COM 178 final, Brussels 2018, p. 7.

[39] *Ibidem*.

the Union Customs Code); e-transit (which makes it possible for the goods subjected to excise duty to transit with the use of electronic documents); single window (which is a facility that guarantees mechanisms of exchange and multiple use of data between the customs authorities and the business entities, along with the coordination of joint controls). Currently, the European Commission is working intensely on the system of the single window, which would allow a commercial entity to transfer the data for the several regulatory purposes – e.g. veterinary, sanitary, environmental purposes – in a standardised format to a number of recipients and through a network of harmonised access points.

Another significant instrument – both from the point of view of customs controls and trade facilitations – worked out as part of the changes introduced in the field of security, is the Authorised Economic Operator (AEO) scheme. The programme became part of EU legislation in 2005,[40] and, practically, it has been effective since 1 January 2008.[41] An authorised AEO trader is an entity who is regarded as trustworthy, reliable and solvent in terms of his/her customs activities. Also, his/her organisation, infrastructure and IT systems security measures applied, and the storage points of the goods guarantee the security of places and goods, and protect them against unauthorised access. An AEO trader is eligible to a number of benefits and privileges laid down in the relevant customs legislation.[42] These include e.g. fewer controls, priority treatment of consignments whenever they have been selected for control, choice of the place of controls in a place outside a customs office, prior notification, customs self-service, or centralised clearance.[43] The strict requirements for those applying for an AEO authorisation make sure that meeting them is definitely not easy for a business entity. As for the AEO authorisation[44] with regard to security and protection, the criteria that have to be met pertain, among others, to the security of buildings (a guarantee that the location of a given building and the materials with which it has been built render intrusion more difficult); appropriate access controls (these should make it impossible for unauthorised persons, vehicles or

[40] Regulation (EC) No 648/2005 of the European Parliament and of the Council of 13 April 2005 amending Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, *op. cit*.

[41] Commission Regulation (EC) No 1875/2006 of 18 December 2006 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, OJ L 360 of 19.12.2006.

[42] It is also worth pointing to other facilitations – the so-called "indirect" benefits. Although they have not been included in the provisions, in practice, they have a positive impact on the commercial activity conducted by helping to cut down on the cases of theft and losses; ensure timely delivery, facilitate planning, improve customer service, build more trust and thereby enhance clients' loyalty, ensure rational stock management, boost employees' engagement, lower the number of incidents related to security and protection, bring down supplier control costs, hone the level of security and improve communication with the partners within a supply chain – European Commission, *Authorised Economic Operators. Guidelines*, *op. cit*., pp. 26–27.

[43] *Ibidem*, pp. 19–25.

[44] The status includes two types of authorisations: 1) authorised trader within customs simplifications (AEOC authorisation), and 2) authorised trader within security and protection (AEOS authorisation). Interestingly, a trader may hold two types of authorisations at the same time, and then in practice, this combination refers to the customs simplifications/security and protection status, marked AEOF. Cf. Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L. 269 of 10.10.2013, *op. cit*., art. 38.

goods to gain access to shipping areas, loading docks, etc.); cargo security (having appropriate measures for the handling of goods that guarantee the inviolability of the cargo); business partner security (identification of and appropriate knowledge about a specific business partners); personnel security (transparent hiring procedures, and periodical controls of the staff employed in security-sensitive positions). In 2019, the number of Authorised Economic Operators stood at almost 17 thousand. At the same time, as many as 673 traders had the AEOS authorisation, and the AEOF status for customs simplification/security and protection was granted to 8,483 entities.[45] One of the positive things in the cross-border movement of goods is the possibility to have one's AEO status recognised in the third countries with which the EU has made relevant agreements. These countries are: Norway, Switzerland, Japan, Andorra, the US, and China. Such a solution helps to create a stable and coordinated structure of movement of goods in international supply chains, and for the traders it translated into a number of advantages, including fewer controls related to security and protection, or priority treatment during customs clearance.[46]

Another element that plays a pivotal role in safeguarding a legitimate movement of goods in cross-border trade is the nature of customs cooperation. Effective and efficient cooperation has a positive impact on the quality of customs clearance. Its specificity changes along with the growing significance of the EU customs authorities within the international security of the supply chain. The spectrum of actions undertaken by the customs administrations is indeed wide and includes both general actions – such as e.g. assistance and cooperation between customs administrations, using information technologies in customs, cooperating in the field of enforcing customs legislation), and specific actions, i.e. those targeted at specific customs offences. The customs administrations of the Member States are a key partner of the security bodies and law enforcement authorities as regards combatting transboundary threats. Therefore, an effective customs cooperation in the European Union would not be possible without collaborating with a network of specialised institutions, which include: the European Police Office (Europol), the European Anti-Fraud Office (OLAF), the European Border and Coats Guard Agency (Frontex), and Eurojust – a judicial coordination and cooperation authority. The numerous discoveries by the customs administrations of the Member States, acting on their own or in cooperation with the above listed bodies, are the best proof of the effectiveness of the actions taken in the field of security and protection the EU market, leaving a positive mark when it comes to the expectations not only of the traders acting in a fully legitimate way, but also of the society and the state. Taking actions related to the development and strengthening of the cooperation between the customs administrations of the Member States, as well as between the customs authorities and other bodies that play a major role from the point of view of the security of cross-border trade in goods and the economic environment, is

[45] As of 25 June 2019, the number of AEO entities stood at 16,889, https://ec.europa.eu/taxation_customs/dds2/eos/aeo_consultation.jsp?Lang=en&holderName=&aeoCountry=&certificatesTypes=AEOC&certificatesTypes=AEOF&certificatesTypes=AEOS&Expand=true&offset=1&showRecordsCount=1 (accessed: 25.07.2019).

[46] European Commission, *Authorised Economic Operators. Guidelines*, *op. cit*., p. 118.

of key importance for the effective implementation of the protective function. Also, from the point of view of the quality of customs handling and clearance, it is also important to enhance the overall capability of customs administrations to act, and to attain an optimal level of coordination with other areas of the EU policies that have an impact on the duties and responsibilities of customs administrations.[47]

Conclusions

Admittedly, supporting international trade and cracking down on customs crime and other undesirable phenomena that are still part of it lie at the core of the modern role of organisations in charge of an effective functioning of the European customs union. The changes that have taken place in the ways in which the customs authorities of the Member States are organised and how they act to streamline their controls deserve a positive assessment when one looks ah them through the prism of the implementation of the protective function in cross-border trade. The solutions that are put into practice within the entire European customs union are a good example of modern and coherent tools whose effect is a protective shield of trade in goods that does not pose obstacles, but rather facilitates customs procedures. The solutions aimed at making controls more efficient, based on state-of-the-art. technologies (e-services), allow for better identification and more efficient discovery of attempts made to abuse the customs and tax system, they improve the financial security of the Member States' budget and the EU budget, and they speed up the pace at which goods move within the international supply chain. A comprehensive knowledge about who sends what, to whom, and where from makes it easier for the customs administrations to identify legitimate trade and, consequently, to avoid unjustified controls and focus on the areas that constitute the major threats. Real-world experience shows that e-services, which are provided as part of the cross-border customs clearance, are instruments that not only translate into easier business processes (in practice, this implies quicker and cheaper fulfilling the customs obligations), but they also have a positive impact on the overall safety and security of entities.

In the future, security in cross-border trade will still require an incessant perfection of the quality of the services provided by removing the barriers that will be emerging, and this will also translate into a further decrease of the costs of running a business activity and boosting the levels of trust of traders and entrepreneurs for the controls carried out by the EU customs administrations. Only a high quality of customs clearance can have a positive impact on the effective performance of all the tasks related to the measurement, controls and collection of public levies both on a domestic level and the EU level. At the same time, against those entities that knowingly and wilfully disregard the laws or take advantage of the control instruments to quickly gain a profit or a competitive advantage, the customs administrations ought

[47] European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Developing the EU Customs Union and Its Governance, Brussels 21.12.2016, COM (2016) 813 final, pp. 7–14.

to act swiftly and consistently in response. Enhancing effective controls at the optimal point of the supply chain, based on maximal automation and electronisation, allows to carry out this process quickly, effectively, and in line with the expectations of the entities that comply with the law, at the same time ensuring a high level of security of the external border of the European Union. These days, striking a balance between facilitating legitimate trade and the protection of supply chains is possibly the greatest challenge for the customs administrations in the EU, as traders generally are not willing to accept promises made to ensure security at the expense of growth. This explains the positive impact that uniform and effective procedures applied in customs clearance across the Member States of the EU have on striking and maintaining a balance between security and the various facilitations provided.

To sum up, it needs to be emphasised that the high quality of customs clearance plays a fundamental role for the security and protection of goods moved within the international supply chain and constitutes a major element that facilitates legitimate trade and the protection of the economic interests of the Union and its Member States.

References

Bugdol M., *Zarządzanie jakością w urzędach administracji publicznej. Teoria i praktyka*, Warszawa 2011.

Commission Regulation (EC) No 1875/2006 of 18 December 2006 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, OJ L 360 of 19.12.2006.

Council Decision of 26 May 2014 on the system of own resources of the European Union, No 2014/335/EU, Euratom, L 168.

Council Resolution of 5 December 2003 on creating a simple and paperless environment for customs and trade, OJ C 305 of 16.12.2003.

Decision of the European Parliament and of the Council No 70/2008/WE of 15 January 2008 on a paperless environment for customs and trade, OJ L 23/21, 2008.

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 011 of 15.01.2002.

European Commission, *Customs sees what you don't… and protects you*, https://ec.europa.eu/taxation_customs/facts-figures/customs-sees-what-you-dont-protects-you_en (accessed: 23.07.2019).

European Commission, Directorate General Environment, *EU Wildlife Trade 2017: Analysis of the European Union's annual reports to CITES 2017*, Brussels 2019.

European Commission, *EU Customs Union – Unique in the World*, https://ec.europa.eu/taxation_customs/facts-figures/eu-customs-union-unique-world_en (accessed: 21.07.2019).

European Commission, *Report from the Commission to the European Parliament and the Council on the IT strategy for customs*, COM 178 final, Brussels 2018.

European Union, *Rapid Alert System for Dangerous Products – 2017 Annual Report*, Luxembourg 2018.

European Commission, *Authorised Economic Operators*. Guidelines, TAXUD/B2/047/2011-REV.6, Brussels 2016.

European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee on Customs Risk Management and Security of the Supply Chain, COM 0793 final, 2012.

European Court of Auditors, *A Series of Delays in Customs IT Systems: What Went Wrong?*, Special Report No 26, Brussels 2018, p. 17.

Gwardzińska A., *Przedstawicielstwo celne w międzynarodowym obrocie towarowym*, Warszawa 2018.

Harrison A., Hoek R. van, *Logistics Management and Strategy: Competing through the Supply Chain*, 3rd ed., Harlow 2008.

Ministerstwo Finansów, *Program e-Cło – e-Usługi*, speech delivered at the conference held on 29.07.2014, Departament Służby Celnej oraz Departament Ceł, Warszawa 2014.

Płonka B., 'Zarządzanie bezpieczeństwem obszaru celnego Unii Europejskiej', *Zeszyt Naukowy Wyższej Szkoły Bezpieczeństwa Publicznego i Indywidualnego APEIRON w Krakowie*, vol. 3, 2009, p. 68, http://bazhum.muzhp.pl/media//files/Zeszyt_Naukowy/Zeszyt_Naukowy-r2009-t3/Zeszyt_Naukowy-r2009-t3-s62-72/Zeszyt_Naukowy-r2009-t3-s62-72.pdf (accessed: 24.07.2019).

Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, OJ L 269 of 10.10.2013.

Regulation (EC) No 648/2005 of the European Parliament and of the Council of 13 April 2005 amending Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, OJ L 117/13 of 04.05.2005.

Świerczyńska J., 'Jakość obsługi celnej a konkurencyjność przedsiębiorstw uczestniczących w obrocie międzynarodowym', in P. Antonowicz, E. Malinowska, J. Siciński (ed.) *Sektorowe uwarunkowania funkcjonowania i rozwoju przedsiębiorstw*, Gdańsk 2019.

Świerczyńska J., 'Bezpieczeństwo i ochrona rynku jako priorytetowy obszar działania europejskiej służby celnej', in J. Rymarczyk, M. Domiter, W. Michalczyk (ed.), *Przemiany strukturalne i koniunkturalne na światowych rynkach*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu No 369, Wrocław 2014.

Top Trading Partners 2018 – Trade Statistics, http://ec.europa.eu/trade/policy/eu-position-in-world-trade (accessed: 21.07.2019).

Wilson N., *Examining the Trade Effect of Certain Customs and Administrative Procedures*, OECD Trade Policy Working Papers, No 42, Paris 2007.

World Customs Organization, *SAFE Framework of Standards to Secure and Facilitate Global Trade*, http://www.wcoomd.org/en/topics/facilitation/instrument-andtools/tools/safe_package.aspx (accessed: 15.06.2019).

World Bank, *Supply Chain Security Guide*, Washington 2009.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004.

Zięba R., 'Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych', in D.B. Bobrow, E. Haliżak, R. Zięba (ed.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Warszawa 1997.

Znaczenie obsługi celnej w procesie zapewniania bezpieczeństwa i ochrony w transgranicznym ruchu towarowym w Unii Europejskiej
Streszczenie

Celem artykułu jest przedstawienie znaczenia obsługi celnej w procesie zapewniania bezpieczeństwa i ochrony w transgranicznym ruchu towarowym w Unii Europejskiej. Hipoteza badawcza została sformułowana następująco: organy celne, jako służby mające pełne kompetencje w zakresie nadzoru i kontroli nad wszystkimi towarami przewożonymi przez granice celne, potrafią wdrażać w ramach europejskiej unii celnej nowoczesne i spójne rozwiązania, których efektem jest skuteczna ochrona obrotu towarowego – nie tworząc przy tym barier, ale usprawniając obsługę celną. Struktura artykułu obejmuje trzy części oraz podsumowanie. W części pierwszej wskazano na istotę i znaczenie funkcji ochronnej realizowanej przez administracje celne państw członkowskich Unii Europejskiej; druga odnosi się do znaczenia obsługi celnej w procesie ochrony transgranicznego przepływu towarów; trzecia prezentuje wybrane instrumenty, które usprawniają obsługę celną, wpływając jednocześnie pozytywnie na poziom bezpieczeństwa. W badaniach wykorzystano analizę opisową, poprzedzoną przeglądem źródeł literaturowych i aktów unijnego i krajowego prawodawstwa wtórnego.
Słowa kluczowe: Unia Europejska, bezpieczeństwo, ochrona, obrót towarowy, usługi celne, organy celne

The Role of Customs Clearance in Ensuring the Security and Protection of Cross-Border Trade in the European Union
Abstract

The goal of the paper is to highlight the relevance of customs clearance in the process of guaranteeing the security and safety of cross-border trade in the European Union. The research hypothesis has been formulated as follows: customs authorities, acting as the bodies that have full competence over the surveillance and control of the goods transited across the customs borders, are able to implement modern and consistent solutions within the European Customs Union. As a result, trade in goods is effectively safeguarded, no barriers are created, and customs clearance is improved, which facilitates commercial activity. The paper consists of three parts, and a summary. The first part looks at the essence and significance of the protective function performed by customs administrations of the Member States; the second part refers to the relevance of customs clearance in the process of the cross-border flow of goods, and the third part elucidates the selected instruments which enhance customs processing and, at the same time, have a positive impact on the overall level of security and safety. The conclusions drawn from the considerations pondered upon in the paper have been included in the summary. The research was based on a descriptive analysis preceded by a review of the subject literature, as well as a selection of national and EU secondary legislation.
Key words: European Union, security, safety, trade, customs services, customs authorities

Bedeutung der Zollabfertigung im Prozess der Sicherheits- und Schutzgewährleistung im grenzüberschreitenden Güterverkehr in der Europäischen Union
Zusammefassung

Das Ziel des Artikels ist die Bedeutung der Zollabfertigung im Prozess der Sicherheits- und Schutzgewährleistung im grenzüberschreitenden Güterverkehr in der Europäischen Union darzustellen. Die Forschungshypothese wurde wie folgt formuliert: Zollbehörde, als die für die Aufsicht und Kontrolle über alle durch die Zollgrenzen beförderten Waren zuständigen Dienste, können im Rahmen der europäischen Zollunion moderne und kohärente Lösungen einführen, welche einen effektiven Schutz des Güterverkehrs zur Folge haben, ohne Schranken dabei zu errichten sondern die Zollabfertigung zu optimieren. Die Struktur des Artikels umfasst drei Teile und eine Zusammenfassung. Im ersten Teil wurde auf das Wesen und die Bedeutung der durch die Zollverwaltungen der EU-Mitgliedsländer ausgeübten Schutzfunktion hingewiesen, der zweite Teil bezieht sich auf die Bedeutung der Zollabfertigung im Prozess der Schutzgewährleistung im grenzüberschreitenden Güterverkehr; der dritte Teil stellt ausgewählte Instrumente dar, die die Zollabwicklung erleichtern und sich positiv auf das Sicherheitsniveau auswirken. In den Untersuchungen wurde die beschreibende Analyse benutzt, deren die Übersicht der Literaturquellen und Rechtsvorschriften der Unions- und Landesrechtsvorschriften vorausgeht.
Schlüsselwörter: Sicherheit, Schutz, Güterverkehr, Zollleistungen, Zollbehörde

Значение таможенного обслуживания в процессе обеспечения безопасности и защиты в трансграничном движении товаров в государствах Европейского Союза
Резюме

В статье рассматривается значение таможенного обслуживания в процессе обеспечения безопасности и защиты в трансграничном движении товаров в Европейском Союзе. Исследовательская гипотеза была сформулирована следующим образом: таможенные органы, имеющие полномочия в области надзора и контроля над всеми товарами, перевозимыми через таможенные границы, могут внедрять, в рамках европейского таможенного союза, современные, комплексные решения, результатом которых является эффективная защита товарооборота – не создавая при этом барьеров, а улучшая таможенное обслуживание. Структура статьи включает в себя три части и резюме. В первой части освящены суть и значимость защитной функции, выполняемой таможенными администрациями государств-членов Европейского Союза; во второй части подчеркнуто значение таможенного обслуживания в процессе защиты трансграничных потоков товаров; в третьей – представлено выбранные инструменты, способствующие повышению качества таможенного обслуживания, что имеет положительное влияние на уровень безопасности. В исследовании был использован описательный анализ, которому предшествовал обзор литературных источников и нормативно-правовых актов законодательства ЕС и Польши.
Ключевые слова: Европейский Союз, безопасность, охрана, товарооборот, таможенные услуги, таможенные органы

BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-005

Sylwia Zawadzka
doktorantka, Uniwersytet Wrocławski
ORCID: 0000-0002-1344-9400

System wjazdu i wyjazdu (EES) i Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS). Rola i znaczenie nowoczesnych systemów w zakresie działań prewencyjnych i wzmacniania bezpieczeństwa UE

Wprowadzenie

Zapewnienie obywatelom bezpieczeństwa jest jednym z priorytetowych obszarów współpracy państw członkowskich UE oraz głównym celem większości inicjatyw podejmowanych na poziomie ponadnarodowym. Mimo iż UE nie jest postrzegana na arenie międzynarodowej jako podmiot typu *hard power* i nie dysponuje tradycyjnymi środkami „twardego" oddziaływania politycznego, tj. własnym potencjałem militarnym, dąży do uzyskania statusu aktora typu *smart power*, głównie poprzez wprowadzanie innowacyjnych projektów z zakresu wzmacniania Unii Bezpieczeństwa (Security Union)[1]. Wiele z tych inicjatyw dotyczy ochrony granic i przeciwdziałania transgranicznym zagrożeniom, takim jak terroryzm czy nielegalna imigracja.

Wzrost zagrożenia terrorystycznego w drugiej dekadzie XXI w. oraz wyzwania związane z napływem imigrantów o nieuregulowanym statusie w konsekwencji kryzysu migracyjnego wymusiły na decydentach unijnych wprowadzenie jakościowych

[1] Szerzej zob. J.S. Nye, *Soft Power*: *The Means to Success in World Politics*, New York 2004, s. 10–21.

zmian w polityce zarządzania granicami zewnętrznymi, której efektywność ściśle związana jest z poziomem bezpieczeństwa UE. Zagrożenia o charakterze transgranicznym potwierdziły potrzebę określenia nowej wizji, celów oraz narzędzi gwarantujących wysokie standardy bezpieczeństwa i ochrony granic[2]. Zostały one wcześniej określone w Strategii bezpieczeństwa wewnętrznego UE z 2010 r. W dokumencie zdefiniowano dziesięć wytycznych działań, których realizacja miała być warunkiem prawidłowego funkcjonowania Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości.

W pierwszej części (poświęconej działaniom strategicznym) zwrócono uwagę na wytyczne związane z kompleksowym podejściem do bezpieczeństwa wewnętrznego w wymiarze horyzontalnym oraz wertykalnym, a także zapewnieniem demokratycznego i sądowego nadzoru nad działaniami z zakresu bezpieczeństwa. Do innych priorytetów zaliczono działania prewencyjne oparte na danych wywiadowczych oraz wypracowanie kompleksowego modelu wymiany informacji między państwami członkowskimi. Zgodnie z założeniami Strategii, usprawnienie wymiany informacji miało być kluczową determinantą zwiększenia skuteczności działań prewencyjnych w kontekście wykrywalności przestępstw i ich sprawców. Podkreślono tym samym konieczność opracowania mechanizmów wymiany informacji opartych na szerokim i szybkim dostępie do danych. W myśl tej koncepcji organy ochrony porządku publicznego powinny dysponować maksymalną ilością informacji w danym momencie. W Strategii podkreślono, że cele te będą mogły zostać zrealizowane, gdy europejski model zarządzania informacjami obejmie całe spektrum unijnych baz danych, kluczowych dla zapewniania bezpieczeństwa obywatelom państw członkowskich, i opierał się będzie na interoperacyjności oraz maksymalnym wykorzystaniu potencjału technologii biometrycznych, tak aby możliwa była szybka i skuteczna wymiana wiarygodnych danych osobowych[3].

Wśród innych wytycznych zdefiniowanych w Strategii z 2010 r. znalazło się wzmocnienie współpracy operacyjnej i współpracy organów wymiaru sprawiedliwości w sprawach karnych oraz zintegrowane zarządzanie granicami. W tej części dokumentu podkreślono potrzebę rozwoju europejskiego systemu nadzoru granic, a także zmaksymalizowania współpracy między Frontexem (Europejską Agencją Straży Granicznej i Przybrzeżnej) a innymi agencjami UE w zakresie zarządzania granicami. Podkreślono, że kluczową rolę w tym obszarze odgrywają nowe technologie, które „zwiększają bezpieczeństwo, gdyż pozwalają zorganizować konieczną kontrolę uniemożliwiającą przedostawanie się osób czy towarów, które stwarzają zagrożenie dla Unii”[4]. Zwrócono także uwagę na konieczność dalszego rozwoju Systemu Informacyjnego Schengen oraz nowych, elektronicznych systemów kontroli granic, w tym Systemu wjazdu i wyjazdu. Z kolei dwie ostatnie wytyczne dotyczyły powiązania bezpieczeństwa wewnętrznego UE z wymiarem

[2] W. Fehler, *Poprawa bezpieczeństwa UE przez zarządzanie granicami*, [w:] *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego. Uwarunkowania, realizacja, wyzwania w drugiej dekadzie XXI wieku*, red. W. Fehler, K.P. Marczuk, Warszawa 2015, s. 191.

[3] Urząd Publikacji Unii Europejskiej, Strategia bezpieczeństwa wewnętrznego Unii Europejskiej, *Dążąc do europejskiego modelu bezpieczeństwa*, Luksemburg 2010, s. 22–24.

[4] *Ibidem*, s. 27.

zewnętrznym oraz elastycznego dostosowania narzędzi i metod jego zapewniania do przyszłych wyzwań[5].

Zgodnie z treścią dokumentu najważniejszym priorytetem budowania bezpieczeństwa powinno być opracowanie innowacyjnych rozwiązań w zakresie kontroli osób na przejściach granicznych oraz wdrożenie nowoczesnych systemów służących wymianie informacji kluczowych w kontekście realizacji działań prewencyjnych. Wizja określona w Strategii bezpieczeństwa wewnętrznego UE rozwijana była w unijnej debacie politycznej w kolejnych latach, natomiast kluczowym wydarzeniem, które przyspieszyło proces reform, był kryzys migracyjny w 2015 r. Skalę wyzwania, z jakim musiała wówczas zmierzyć się Unia, potwierdzają dane Frontexu o ponad 2,3 mln przypadków nielegalnego przekroczenia granicy w 2015 i 2016 r.[6].

Nowe systemy zostały ustanowione w trakcie kadencji przewodniczącego KE Jean-Claude Junckera, jednak pierwsze propozycje nawiązujące do Pakietu Smart Borders zostały wypracowane w 2011 r. w Inicjatywie na rzecz inteligentnych granic, która rozwijała plany zarysowane w Komunikacie Komisji Europejskiej z 2008 r. (*Przygotowanie kolejnych etapów rozwoju zarządzania granicami w Unii Europejskiej*)[7] oraz Strategii bezpieczeństwa wewnętrznego z 2010 r. W dokumentach przedstawiono wizję rozwoju zintegrowanego zarządzania granicami UE, którego efektem miało być opracowanie systemów efektywnego monitorowania obywateli państw trzecich przekraczających granice zewnętrzne UE[8].

Propozycje zostały rozwinięte w oficjalnym wniosku Komisji z 2013 r. w sprawie ustanowienia nowoczesnych systemów administrowania granicami, w tym Systemu wjazdu i wyjazdu (Entry/Exit System, EES) oraz Systemu rejestrowania podróżnych (Registered Traveller Programme, RTP). Zgodnie z założeniami wniosku, głównym celem EES miała być walka z nielegalną imigracją poprzez automatyczne rejestrowanie czasu i miejsca przekroczenia zewnętrznych granic UE przez cudzoziemców oraz obliczanie maksymalnego okresu dozwolonego pobytu na terytorium państw członkowskich. Drugi system miał zostać wdrożony w celu ułatwienia przekraczania granic obcokrajowcom, którzy często podróżują do UE w celach biznesowych czy edukacyjnych.

Wyzwania związane z kryzysem migracyjnym oraz wzrost liczby zamachów terrorystycznych w krajach europejskich rozpoczęły nową debatę na temat zmian w polityce zarządzania granicami. Wstępny projekt Rozporządzenia z 2013 r. został wycofany i zastąpiony nowym, rozszerzonym wnioskiem Komisji z 6 kwietnia 2016 r., którego głównym priorytetem stała się ochrona obywateli w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości oraz przeciwdziałanie potencjalnym zagrożeniom. Ostatecznie system RTP nie został uwzględniony w nowym wniosku,

[5] *Ibidem*, s. 28–30.

[6] European Parliamentary Research Service, *Migration and asylum*, http://www.europarl.europa.eu/thinktank/infographics/migration/public/index.html?page=migration [dostęp: 02.06.2019].

[7] Komunikat Komisji Europejskiej, *Przygotowanie kolejnych etapów rozwoju zarządzania granicami w Unii Europejskiej*, COM(2008) 69; por. Komunikat Komisji Europejskiej, *Kompleksowa wizja zintegrowanego systemu zarządzania granicami na miarę XXI wieku*, IP/08/215, 13.02.2008.

[8] Komunikat Komisji Europejskiej, *Inicjatywa UE na rzecz inteligentnych granic: Komisja dąży do łatwiejszego dostępu i wzmocnionej ochrony*, IP/11/1234, 25.10.2011.

zaproponowano natomiast nowy kształt Rozporządzenia w sprawie zakresu korzystania z EES[9].

W kontekście celów i funkcji, nowe instrumenty ochrony granic zewnętrznych, stanowiące podstawę europejskiej infrastruktury informacyjnej, mają charakter komplementarny wobec trzech istniejących systemów wielkoskalowych: Systemu Informacyjnego Schengen drugiej generacji (Schengen Information System II, SIS II), Systemu Informacji Wizowej (Visa Information System, VIS) oraz Europejskiego Zautomatyzowanego Systemu Rozpoznawania Odcisków Palców (European Dactyloscopy, Eurodac). Pierwszy z nich zawiera informacje dotyczące osób zaginionych i poszukiwanych oraz przedmiotów, które mogły być wykorzystane do celów popełnienia przestępstwa. Po ostatniej reformie w 2018 r. katalog informacji został poszerzony m.in. o wpisy dotyczące dzieci zagrożonych uprowadzeniem; wpisy do celów powrotu, czyli odnotowywanie decyzji nakazujących powrót obywatelom państw trzecich nielegalnie przebywających w UE[10]. System Informacji Wizowej zawiera dane obywateli państw trzecich objętych obowiązkiem wizowym, natomiast w systemie Eurodac przechowywane są dane daktyloskopijne osób ubiegających się o ochronę międzynarodową.

Celem niniejszego artykułu jest zdefiniowanie znaczenia i przydatności nowych systemów wielkoskalowych: Systemu wjazdu i wyjazdu (EES) oraz Europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) w aspekcie poprawy bezpieczeństwa wewnętrznego UE. Praca opiera się na założeniu, że dotychczasowy deficyt informacyjny w odniesieniu do niektórych kategorii obywateli państw trzecich uniemożliwiał właściwą i skuteczną ochronę granic zewnętrznych UE. Poprzez wypełnienie luk informacyjnych, systemy te przyczynią się do pełnej implementacji zintegrowanego zarządzania granicami, a to z kolei – do efektywnego zwalczania przestępstw o charakterze transgranicznym. Artykuł został opracowany na podstawie metody instytucjonalno-prawnej, natomiast główną bazą źródłową były rozporządzenia ustanawiające nowe systemy. Metoda analizy komparatystycznej została zastosowana w celu określenia specyfiki tych dwóch systemów pod względem zasad, kategorii danych oraz oddziaływania na bezpieczeństwo.

[9] Wniosek Komisji Europejskiej w sprawie Rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 562/2006 w związku ze stosowaniem systemu wjazdu/wyjazdu (EES) oraz programu rejestrowania podróżnych (RTP), COM(2013) 96 final, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0096:FIN:PL:PDF [dostęp: 03.06.2019].

[10] Szerzej zob. Rozporządzenie (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, Dz. Urz. UE L 312 z 7.12.2018, s. 56–106; Rozporządzenie (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006, Dz. Urz. UE L 312 z 7.12.2018, s. 14–55; Rozporządzenie (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich, Dz. Urz. UE L 312 z 7.12.2018, s. 1–13.

System wjazdu i wyjazdu (EES) oraz jego wpływ na bezpieczeństwo

Podstawą prawną, która określa cele i zasady funkcjonowania EES, jest Rozporządzenie Parlamentu Europejskiego i Rady z 30 listopada 2017 r.[11]. Zgodnie z postanowieniami dokumentu, system ma zastosowanie do wszystkich obywateli państw trzecich korzystających z prawa krótkiego pobytu. Dotyczy zatem zarówno obcokrajowców objętych obowiązkiem wizowym, jak i obywateli państw trzecich, z którymi UE podpisała umowy o liberalizacji reżimu wizowego w zakresie krótkiego pobytu (do 90 dni w dowolnym okresie 180 dni).

Należy podkreślić, że dane dotyczące osób ubiegających się o wizę przechowywane są w VIS, natomiast do czasu uchwalenia Rozporządzenia o EES nie istniała żadna baza, która mogłaby przetwarzać informacje o osobach zwolnionych z konieczności ubiegania się o wizę Schengen przed podróżą do jednego z państw członkowskich. EES odgrywa zatem kluczową rolę w zakresie wypełnienia luk informacyjnych w odniesieniu do obywateli państw trzecich, których nie dotyczy obowiązek wizowy. Ponadto, nowy system został opracowany na zasadzie interoperacyjności z VIS, którą umożliwić ma wprowadzenie do infrastruktury technicznej specjalnego kanału komunikacyjnego między centralnymi systemami VIS i EES. Oznacza to, że informacje przechowywane w bazach VIS będą dostępne dla organów korzystających z EES w celu tworzenia nowych wpisów lub weryfikowania tożsamości poprzez porównywanie danych. Taka sama procedura dotyczy możliwości przeglądania przez organy wizowe danych EES z poziomu VIS w celu rozpatrywania wniosków wizowych oraz aktualizowania danych w EES w przypadku zmiany statusu wizy[12].

Katalog celów, który został określony w Rozporządzeniu, można podzielić na dwie kategorie ze względu na funkcje spełniane przez nowy system. Pierwsza grupa celów związana jest z zagwarantowaniem efektywnej i szybkiej mobilności osobom podróżującym w dobrej wierze. W tym przypadku celem EES jest przede wszystkim zautomatyzowanie odpraw granicznych i zwiększenie ich efektywności oraz przekazywanie obcokrajowcom informacji na temat czasu, jaki pozostał im do wykorzystania w ramach prawa krótkiego pobytu[13].

Zdecydowanie więcej uwagi poświęcono celom związanym z zapewnieniem bezpieczeństwa poprzez skuteczne administrowanie przepływami migracyjnymi. W tym zakresie system ma ułatwić identyfikację osób, które przekroczyły okres dozwolonego pobytu i przebywają na terytorium państw członkowskich nielegalnie, oraz osób potencjalnie stanowiących poważne zagrożenie dla bezpieczeństwa,

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011, Dz. Urz. UE L 327 z 9.12.2017, s. 20–82.

[12] *Ibidem*, s. 34–35, art. 8.

[13] *Ibidem*, s. 33, art 6.

porządku publicznego i zdrowia obywateli UE. Istotne są zatem funkcje EES związane z identyfikacją osób, które nie spełniają warunków wjazdu do strefy Schengen lub przestali je spełniać, a także możliwością elektronicznego sprawdzania odmowy wjazdu oraz informacji zawartych w VIS[14].

W aspekcie poprawy bezpieczeństwa szczególnie istotne są cele związane z zapobieganiem oraz zwalczaniem ciężkich przestępstw. Mają one coraz częściej charakter transgraniczny, zatem walka z nimi musi opierać się na skutecznej wymianie informacji między państwami członkowskimi oraz organami unijnymi. Współpraca w tym zakresie nie zawsze przynosiła pożądane rezultaty – EES ma pozwolić na skuteczną walkę z zagrożeniami na poziomie ponadnarodowym. Wyznaczone organy państw członkowskich mają dostęp do systemu centralnego, gdzie przechowywane są informacje wprowadzane za pośrednictwem jednostek krajowych, zlokalizowanych we wszystkich państwach korzystających z EES, dzięki czemu upoważniony personel może przeglądać dane dotyczące określonych osób bez względu na miejsce przekraczania przez nie granicy. Pozwoli to na przeciwdziałanie oszustwom opartym na multiplikacji tożsamości oraz nieuprawnionym posługiwaniu się skradzionymi lub sfałszowanymi dokumentami. System umożliwi także działania prewencyjne związane z wykrywaniem sprawców przestępstw oraz osób podejrzanych o ich popełnienie. Może to znacząco przyczynić się do wykrywania i zapobiegania zamachom terrorystycznym, a także ułatwić prowadzenie w ich sprawie postępowań przygotowawczych[15].

Ponadto system może być przydatny w perspektywie długookresowej. EES ułatwi gromadzenie danych statystycznych dotyczących państw, których obywatele najczęściej przekraczają dozwolony okres pobytu lub przebywają na terytorium UE nielegalnie. Umożliwi to opracowanie nowych strategii w zakresie kształtowania polityki migracyjnej wobec poszczególnych państw. Dotychczas UE nie dysponowała takim potencjałem informacyjnym w stosunku do obywateli państw, z którymi zawarła umowy o liberalizacji reżimu wizowego. Opracowywanie raportów i analiza ryzyka na podstawie dostępnych informacji może być kluczowym argumentem dla zaostrzenia polityki migracyjnej wobec tych państw.

Rozporządzenie określa także procedury korzystania z infrastruktury technicznej systemu na przejściach granicznych oraz warunki dostępu określonych organów do danych EES. Zgodnie z analizą celów wdrożenia nowoczesnych systemów opartych na wysokiej technologii przetwarzania danych, państwa korzystające z systemu na granicach zewnętrznych UE mogą zautomatyzować proces wprowadzania, a następnie weryfikacji danych poprzez umożliwienie podróżnym z państw trzecich korzystanie ze stanowisk samoobsługi. Za ich pośrednictwem obcokrajowcy będą mogli sprawdzić swoje dane lub wprowadzić je do systemu w przypadku przekraczania zewnętrznej granicy po raz pierwszy. Wówczas obywatele państw trzecich, co do których ma zastosowanie Rozporządzenie o EES, będą podlegać obowiązkowi utworzenia elektronicznego rejestru indywidualnego, złożonego z rejestru osobowego (zawierającego dane alfanumeryczne oraz biometryczne) i rejestru przekroczeń granicy, w którym system każdorazowo będzie zapisywał czas i miejsce

[14] *Ibidem*, s. 33, art. 6; s. 34, art. 8.

[15] *Ibidem*, s. 29, art. 1.

przekroczenia granicy w celu automatycznego obliczania okresu dozwolonego pobytu. Podczas odprawy granicznej, EES wstępnie zweryfikuje dane pobrane na miejscu i porówna z informacjami zawartymi w systemie. W trakcie procedury skanowania dokumentu podróży uruchamiane są wszystkie niezbędne kontrole baz danych bezpieczeństwa. Jeśli dana osoba zostanie zidentyfikowana w bazach jako stanowiąca potencjalne zagrożenie, EES nie umożliwi jej przekroczenia granicy, co zostanie odnotowane jako odmowa wjazdu. Należy zaznaczyć, iż system dokonuje automatycznej odprawy granicznej i weryfikuje tożsamość podróżnego, natomiast ostateczną decyzję co do zezwolenia na wjazd podejmują obecni w miejscach kontroli funkcjonariusze służb granicznych[16].

Poza danymi personalnymi, takimi jak: imię, nazwisko, data urodzenia, płeć, obywatelstwo, w rejestrze osobowym przechowywane są dane alfanumeryczne związane z dokumentami podróży, tj.: rodzaj i numer; kod państwa, które wydało dany dokument, oraz data jego ważności. W określonych przypadkach wprowadza się także informacje dotyczące wiz. W EES wykorzystuje się również dane biometryczne: wizerunek twarzy oraz odciski palców. Pomimo istnienia wyraźnej przesłanki dotyczącej możliwości naruszenia prywatności obywateli państw trzecich, korzystanie z danych biometrycznych jest uzasadnione względami bezpieczeństwa, zwłaszcza w kontekście poprawy skuteczności działań prewencyjnych. Dane te zapewniają wiarygodną i skuteczną identyfikację cudzoziemców, którzy nie posiadają dokumentów potwierdzających ich tożsamość (taka sytuacja jest typowa dla migracji nieuregulowanej). Ponadto, dane biometryczne pozwalają na zapobieganie i wykrywanie przypadków posługiwania się wieloma tożsamościami. Wszystkie dane wprowadzane do EES mają wzmocnić i usprawnić zarządzanie granicami zewnętrznymi, przeciwdziałać przypadkom nielegalnego przekroczenia granicy, a także ułatwiać realizację decyzji z zakresu polityki powrotowej. Dostęp do danych, oparty na zasadzie konieczności, celowości i proporcjonalności, powinien wzmacniać ochronę obywateli UE pod kątem wykrywania zagrożenia terrorystycznego i zwalczania zorganizowanej przestępczości[17].

Dostęp do systemu w celu przeglądania, wprowadzania, usuwania i zmieniania danych zapewniony jest upoważnionemu personelowi właściwych organów wyznaczonych przez każde państwo członkowskie. Niektóre z tych organów mogą być zobowiązane do korzystania z systemu w przypadku zaistnienia wyraźnej przesłanki zagrożenia porządku publicznego. Funkcjonariusze służb granicznych mogą korzystać z EES w celu rejestracji podróżnego, weryfikacji jego tożsamości lub aktualizacji jego danych. Innymi podmiotami posiadającymi dostęp do danych EES są organy wizowe – upoważnione do przeglądania zawartych tam informacji w celu rozpatrzenia wniosków wizowych oraz podjęcia decyzji odnośnie do statusu wizy. Dostęp zapewniony jest także organom imigracyjnym, które mogą za pośrednictwem systemu zweryfikować tożsamość cudzoziemców i sprawdzić, czy zostały spełnione wszystkie niezbędne warunki wjazdu i pobytu w strefie Schengen. Ze względu na realizację zadań związanych ze wsparciem państw członkowskich w zakresie

[16] *Ibidem*, s. 38–39, art. 14.

[17] *Ibidem*, s. 20–29; s. 35, art. 9; s. 49–50, art. 32.

przeciwdziałania terroryzmowi i innym poważnym przestępstwom, dostęp do danych EES przysługuje również wyznaczonemu organowi Europolu[18].

EES zastępuje jednocześnie system ręcznego stemplowania paszportów, który nie tylko nie pozwala na szybkie wykrywanie osób nielegalnie przedłużających pobyt, ale jest także nieefektywny w kontekście zapobiegania problemom w sytuacji sfałszowania, utraty lub świadomego zniszczenia dokumentów podróży[19]. EES odgrywa zatem kluczową rolę w aspekcie poprawy zarządzania granicami, przeciwdziałania nieuregulowanej imigracji oraz usprawnienia administrowania przepływami migracyjnymi. Biorąc pod uwagę rodzaj przechowywanych danych oraz skuteczny i szybki dostęp właściwych służb bezpieczeństwa, EES jest istotnym narzędziem prewencyjnym w zakresie walki z przestępczością zorganizowaną oraz wczesnego wykrywania zagrożeń, w tym zapobiegania przedostawaniu się na terytorium UE potencjalnych sprawców przestępstw terrorystycznych. Jest tym samym fundamentem europejskiej infrastruktury informacyjnej oraz niezbędnym komponentem polityki migracyjnej.

Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) jako narzędzie prewencji

Drugim systemem, który pozwoli wzmocnić bezpieczeństwo UE poprzez zarządzanie granicami, jest Europejski system informacji o podróży oraz zezwoleń na podróż (European Travel Information and Authorisation System, ETIAS), ustanowiony Rozporządzeniem z 12 września 2018 r.[20]. Oficjalne prace związane z jego implementacją rozpoczęły się w 2016 r., kiedy przygotowano wstępny projekt Rozporządzenia oraz wypracowano analizę możliwości nowego elementu infrastruktury bezpieczeństwa. W odróżnieniu od EES, ETIAS został opracowany w celu zwiększenia potencjału informacyjnego w stosunku do konkretnej kategorii obywateli państw trzecich: osób zwolnionych z obowiązku wizowego, które planują podróż do jednego z państw członkowskich. Ich dane nie były dotychczas przetwarzane w żadnym systemie informacyjnym na poziomie UE. ETIAS może stanowić kluczowy element prewencyjnej infrastruktury bezpieczeństwa: system będzie gromadził dane określonej grupy podróżnych przed ich przybyciem w miejsca kontroli właściwej (przesłanie danych do ETIAS będzie poprzedzało procedurę rejestracji w EES).

Zgodnie z postanowieniami Rozporządzenia z 12 września 2018 r. podstawową funkcją nowego systemu ma być zwiększenie poziomu bezpieczeństwa UE poprzez dokonywanie wstępnej oceny osób składających wniosek o zezwolenie na podróż do jednego z państw członkowskich. W przypadku gdy analiza elektronicznego

[18] *Ibidem*, s. 45–49, art 23–31.

[19] Komunikat Komisji Europejskiej, *Silniejsze i bardziej inteligentne granice w UE: Komisja proponuje ustanowienie systemu wjazdu/wyjazdu*, IP/16/1247, 6.04.2016.

[20] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226, Dz. Urz. UE L 236 z 19.09.2018, s. 1–71.

wniosku wykaże, że obecność danej osoby na terytorium UE może stwarzać zagrożenie dla życia i zdrowia obywateli lub wiąże się z ryzykiem nielegalnej migracji czy też wysokim ryzykiem epidemiologicznym, uruchomione zostaną procedury automatycznego odrzucenia wniosku, co jest równoznaczne z brakiem zezwolenia na odbycie podróży. ETIAS jest zatem instrumentem prewencyjnym, służącym identyfikacji niebezpiecznych osób jeszcze przed ich przybyciem na granice zewnętrzne UE. Ponadto, system wspierać ma zadania SIS II w zakresie wykrywania osób poszukiwanych w celu ich aresztowania lub podjęcia decyzji o ekstradycji, a także innych osób, których dane przechowywane są w tym systemie (przede wszystkim zaginionych, potencjalnych sprawców przestępstw lub ich ofiar). Będzie on skomunikowany z innymi systemami wielkoskalowymi, dlatego na poziomie implementacji kluczowe jest wzmocnienie nowych narzędzi interoperacyjności. Podstawowym celem systemu jest więc „uszczelnienie" granic i zapobieganie przedostawaniu się na terytorium państw członkowskich osób stanowiących zagrożenie. Jest to szczególnie istotne w kontekście działań prewencyjnych mających prowadzić do deeskalacji międzynarodowego terroryzmu[21].

Wniosek o wydanie zezwolenia na podróż do państwa członkowskiego UE składany jest za pośrednictwem strony internetowej lub aplikacji na urządzenia mobilne. Procedura wymaga podania właściwych danych (tj. imię; nazwisko; płeć; miejsce urodzenia i adres zameldowania; dane rodziców; dane dokumentów podróży; obywatelstwo; zawód i poziom wykształcenia; adres e-mail, na który zostanie przesłana odpowiedź zwrotna; kraj UE pierwszego zaplanowanego pobytu) oraz wypełnienia formularza z pytaniami, które pozwolą ustalić, czy obecność danej osoby może stwarzać poważne zagrożenie. Według postanowień Rozporządzenia ustanawiającego ETIAS, wnioskodawca musi odpowiedzieć na trzy kategorie pytań. Pierwsza z nich dotyczy przestępstw popełnionych w ciągu ostatnich 20 lat w przypadku przestępstw terrorystycznych lub 10 lat w przypadku pozostałych, określonych w formularzu[22]. W drugim zestawie pytań wnioskodawca wskazuje, czy w ciągu ostatnich 10 lat przebywał na terytorium kraju ogarniętego wojną lub konfliktem, a także określa przyczyny tego pobytu. Z kolei w trzeciej części udziela odpowiedzi, czy w ciągu ostatnich 10 lat był podmiotem jakichkolwiek decyzji nakazujących mu opuszczenie terytorium określonego państwa lub nakazujących mu powrót. W celu zapobiegania zagrożeniom dla zdrowia publicznego pozostałe informacje mogą dotyczyć także kondycji zdrowotnej wnioskodawcy, przebytych chorób zakaźnych czy faktu przebywania w miejscach wysokiego ryzyka epidemiologicznego[23].

Prawidłowo wypełniony wniosek podlega procedurze rozpatrzenia, która zaczyna się od przetwarzania automatycznego. Polega ono na porównaniu informacji z danymi zawartymi w pozostałych systemach informacyjnych w celu zidentyfikowania osób oznaczonych w tych bazach jako niebezpieczne, stanowiące poważne zagrożenie dla porządku publicznego. Proces kojarzenia danych w różnych systemach ma zweryfikować: czy dany obywatel państwa trzeciego posługuje

[21] *Ibidem*, s. 16, art. 4.

[22] Zob. Załącznik I do Rozporządzenia 2018/1240 z dnia 12 września 2018 r., Dz. Urz. UE L 236 z 19.09.2018, s. 71.

[23] Rozporządzenie 2018/1240, Dz. Urz. UE L 236 z 19.09.2018, s. 22–24, art. 17.

się dokumentami, które w innych systemach oznaczone są jako skradzione lub zaginione; czy w innym systemie został dokonany wpis do celów odmowy wjazdu lub odmowy wydania wizy i jakie były ku temu podstawy; czy dana osoba została oznaczona jako zaginiona lub poszukiwana i czy kiedykolwiek przekroczyła dozwolony okres pobytu[24]. W przypadku gdy przetwarzanie automatyczne nie wykaże międzysystemowych zbieżności informacji, które mogłyby stanowić przesłankę do odmowy wydania zezwolenia, wniosek zostaje rozpatrzony pozytywnie. Natomiast jeśli przetwarzanie wygeneruje określone „trafienia" (tj. skojarzenie informacji z różnych systemów), wówczas wniosek analizowany jest ręcznie przez właściwe jednostki krajowe ETIAS państwa odpowiedzialnego, tzn. państwa, które dostarczyło określone informacje na temat wnioskodawcy. W następstwie tej procedury jednostka krajowa podejmuje decyzję o wydaniu zezwolenia lub odmowie jego wydania[25].

ETIAS jest kluczowym elementem budowania Unii Bezpieczeństwa w dobie kryzysu migracyjnego oraz wysokiego zagrożenia terrorystycznego. Pozwala zapobiegać przedostawaniu się na terytorium Unii osób stanowiących zagrożenie, w tym potencjalnych sprawców zamachów terrorystycznych, przy jednoczesnym utrzymaniu ruchu bezwizowego z poszczególnymi państwami. Jest tym samym ważnym środkiem działań prewencyjnych, służącym wzmacnianiu ochrony obywateli UE bez konieczności zaostrzania polityki migracyjnej dla wszystkich obywateli państw trzecich – również tych podróżujących w dobrej wierze. Współpracujący z innymi systemami ETIAS stanowi istotne uzupełnienie unijnej infrastruktury informacyjnej. Zgodnie z harmonogramem implementacji EES i ETIAS będą w pełni operacyjne na przełomie 2020 i 2021 r.

Zasady interoperacyjności systemów informacyjnych UE w aspekcie poprawy bezpieczeństwa i działań prewencyjnych

Systemy informacyjne UE funkcjonujące w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości nie były dotychczas wystarczająco skomunikowane – informacje były przechowywane oddzielnie w autonomicznych i niepowiązanych ze sobą systemach. Rozwiązanie problemu fragmentaryczności struktur zarządzania informacjami na poziomie unijnym stało się jednym z priorytetów Komisji Europejskiej pod przewodnictwem Jean-Claude Junckera.

Wprowadzenie do dorobku Schengen nowych wielkoskalowych systemów w celu usunięcia istniejących luk informacyjnych zdeterminowało jednocześnie konieczność wprowadzenia mechanizmów interoperacyjności, dzięki którym systemy mogłyby współpracować w bardziej wydajny sposób. W grudniu 2017 r. KE przedstawiła wniosek dotyczący wdrożenia owych mechanizmów. Zgodnie z wypowiedzią Fransa Timmermansa, ówczesnego wiceprzewodniczącego Komisji: „Obecnie

[24] *Ibidem*, s. 25–26, art. 20, 21.

[25] *Ibidem*, s. 29–30, art. 25, 26.

unijne systemy informacyjne dotyczące bezpieczeństwa i zarządzania granicami pracują oddzielnie, przez co egzekwowanie prawa może przebiegać wolniej. Dzięki naszemu wnioskowi systemy te staną się w pełni interoperacyjne. Oznacza to, że organy ścigania w całej UE będą miały bezpośredni i niezwłoczny dostęp do wszelkich istniejących informacji"[26].

Komisja zaproponowała wdrożenie czterech komponentów zapewniających interoperacyjność: 1) europejskiego portalu wyszukiwania, który umożliwiłby wyszukiwanie danych w kilku systemach jednocześnie; 2) wspólnego serwisu kojarzenia danych biometrycznych (porównującego dane biometryczne z kilku systemów); 3) wspólnego repozytorium danych identyfikacyjnych (zawierającego dane obywateli państw trzecich dostępne w kilku systemach) oraz 4) modułu wykrywającego multiplikację tożsamości[27].

Zgodnie z treścią Komunikatu Komisji z 12 grudnia 2017 r. celem nowych instrumentów powinno być przede wszystkim zapobieganie przestępstwom poprzez wykrywanie potencjalnych sprawców zarówno w trakcie przekraczania przez nich granic zewnętrznych UE, jak i w sytuacji gdy przebywają już w strefie Schengen. Ma w tym pomóc tzw. jednoczesna krzyżowa kontrola danych w różnych bazach[28].

Postanowienia te zostały potwierdzone porozumieniem Parlamentu Europejskiego i Rady z 2019 r. w sprawie zamknięcia luk w systemach informacyjnych i poprawy ich interoperacyjności, która stała się tym samym priorytetem politycznym na lata 2018–2019[29]. Nowe narzędzia służące połączeniu istniejących baz danych mają umożliwić funkcjonariuszom odpowiednich służb przeprowadzanie kontroli dokumentów jednocześnie we wszystkich systemach z poziomu europejskiego portalu wyszukiwania. Wyeliminuje to problem każdorazowego przeszukiwania poszczególnych baz. Co więcej, nowe elementy infrastruktury bezpieczeństwa zapewnią bardziej skuteczne wykrywanie oszustw dotyczących tożsamości, gdyż funkcjonariusze policji i służb granicznych będą dysponować zarówno wspólnym serwisem kojarzenia danych biometrycznych, jak i repozytorium przechowującym dane wszystkich obywateli państw trzecich zarejestrowanych w systemach informacyjnych. Dodatkowo moduł multiplikacji tożsamości po dokonaniu kontroli krzyżowej (tj. porównaniu danych z różnych systemów) natychmiast wykryje i wskaże osoby korzystające z wielu tożsamości. Funkcjonariuszom organów ścigania zagwarantowany zostanie szybszy dostęp i bardziej wydajny sposób korzystania z baz danych, oparty na procedurze dwuetapowej. W sytuacji gdy poddawane weryfikacji informacje dotyczące obywateli państw trzecich zostaną skojarzone

[26] Komunikat Komisji Europejskiej, *Unia bezpieczeństwa: Komisja eliminuje luki informacyjne, aby lepiej chronić obywateli UE*, IP/17/5202, 12.12.2017.

[27] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, 2017/0352 (COD), s. 5.

[28] Komunikat Komisji Europejskiej, *Unia bezpieczeństwa: Komisja eliminuje luki informacyjne…*

[29] Working document for the Joint Declaration on the EU's legislative priorities for 2018–19: *31 new initiatives for a More United, Stronger and More Democratic Union*, https://ec.europa.eu/commission/sites/beta-political/files/working-document-joint-declaration-legislative-priorities-2018-19_en.pdf [dostęp: 15.06.2019].

z personaliami zawartymi w jednym z systemów, funkcjonariusz może zwrócić się do właściwych organów o bardziej ukierunkowany dostęp do danych zawartych w tym systemie[30].

Działania Komisji w zakresie wdrażania nowych narzędzi interoperacyjności podsumował Komisarz ds. Unii Bezpieczeństwa Julian King, który stwierdził, że są one „odpowiedzią na postulaty osób działających na linii frontu, funkcjonariuszy policji oraz straży granicznej”[31]. Należy przy tym podkreślić, że komponenty te nie będą generować nowych informacji, ale wykorzystywać dane dostępne z poziomu poszczególnych systemów w bardziej ukierunkowany sposób, który ułatwi służbom bezpieczeństwa realizację ich zadań.

Podsumowanie

Od 2015 r. Unia Europejska zmaga się z wyzwaniami związanymi ze wzrostem zagrożenia terrorystycznego oraz napływem imigrantów o nieuregulowanym statusie. Walka z nielegalną imigracją i przeciwdziałanie zorganizowanej przestępczości o charakterze transgranicznym stały się głównymi determinantami reform strefy Schengen. Przyjęto rozporządzenia ustanawiające innowacyjne systemy oparte na wysokiej technologii przetwarzania informacji, które mają wypełnić istniejące dotychczas luki związane z deficytem informacji na temat obywateli państw trzecich (przede wszystkich zwolnionych z obowiązku wizowego), który uniemożliwiał właściwą i skuteczną ochronę granic zewnętrznych UE. Poprzez wypełnienie luk informacyjnych, systemy przyczynią się do pełnej implementacji zintegrowanego zarządzania granicami, a to z kolei – do efektywnego zapobiegania przestępstwom o charakterze transgranicznym.

W EES będą przetwarzane zarówno dane alfanumeryczne, jak i dane biometryczne (wizerunek twarzy oraz odciski palców) obywateli państw trzecich objętych prawem krótkiego pobytu. Pozwoli to na skuteczną identyfikację osób niebezpiecznych oraz osób, które przebywają w UE nielegalnie. System zastąpi tym samym procedurę ręcznego stemplowania dokumentów podróży, która jest mniej wiarygodna, a także podatna na błędy w przypadku gdy dokumenty są sfałszowane lub skradzione. Biorąc pod uwagę rodzaj danych, które gromadzi system, oraz szybkość dostępu właściwych służb bezpieczeństwa, EES jest wiarygodnym i skutecznym narzędziem prewencji w zakresie walki z przestępczością zorganizowaną oraz wczesnego wykrywania zagrożeń i zapobiegania przedostawaniu się na terytorium UE potencjalnych sprawców przestępstw terrorystycznych.

ETIAS w przeciwieństwie do EES ma zastosowanie wyłącznie do obywateli państw trzecich, których nie dotyczy obowiązek ubiegania się o wizę krótkoterminową (tzw. wizę Schengen). Te osoby przed przyjazdem do UE będą zobligowane do złożenia elektronicznego wniosku o wydanie zezwolenia na podróż. Ma to pomóc we wstępnej weryfikacji tożsamości podróżnego oraz dokonaniu analizy ryzyka

[30] Komunikat Komisji Europejskiej, *Unia bezpieczeństwa: Komisja z zadowoleniem przyjmuje porozumienie polityczne w sprawie zamknięcia luk w systemach informacyjnych*, IP/19/846, 5.02.2019.

[31] *Ibidem*.

pod kątem potencjalnego zagrożenia, jakie stanowić może jego obecność na terytorium kraju docelowego. Osoba niebezpieczna zostanie zidentyfikowana jeszcze przed pojawieniem się na przejściach granicznych, co może zwiększyć prawdopodobieństwo „zamknięcia” granic dla osób stanowiących poważne zagrożenie.

EES i ETIAS to istotne elementy europejskiej infrastruktury informacyjnej i kolejny etap budowania Unii Bezpieczeństwa. Odgrywają kluczową rolę w zakresie wzmocnienia bezpieczeństwa poprzez skuteczne zarządzanie przepływami migracyjnymi. Należy jednak podkreślić, że specyfika funkcjonowania EES, oparta na wysokiej technologii przetwarzania informacji, w tym danych biometrycznych, może być odbierana przez obywateli państw trzecich jako zagrażająca bezpieczeństwu danych wrażliwych oraz podatna na tzw. incydenty bezpieczeństwa – związane z możliwością uszkodzenia, utraty lub nieuprawnionego dostępu do danych[32]. Z kolei ETIAS może być postrzegany jako elektroniczna wiza, będąca elementem zaostrzenia polityki migracyjnej wobec państw, z którymi UE podpisała umowy o ruchu bezwizowym. Może to wpłynąć negatywnie na dotychczasową politykę tych państw wobec UE. Niemniej jednak, ze względu na funkcje, jakie spełniać mają nowe systemy, należy uznać je za niezbędne narzędzia podnoszenia poziomu bezpieczeństwa.

Bibliografia

European Parliamentary Research Service, *Migration and asylum*, http://www.europarl.europa.eu/thinktank/infographics/migration/public/index.html?page=migration [dostęp: 02.06.2019].

Fehler W., *Poprawa bezpieczeństwa UE przez zarządzanie granicami*, [w:] *Polityka Unii Europejskiej w zakresie bezpieczeństwa wewnętrznego. Uwarunkowania, realizacja, wyzwania w drugiej dekadzie XXI wieku*, red. W. Fehler, K.P. Marczuk, Warszawa 2015.

Komunikat Komisji Europejskiej, *Inicjatywa UE na rzecz inteligentnych granic: Komisja dąży do łatwiejszego dostępu i wzmocnionej ochrony*, IP/11/1234, 25.10.2011.

Komunikat Komisji Europejskiej, *Kompleksowa wizja zintegrowanego systemu zarządzania granicami na miarę XXI wieku*, IP/08/215, 13.02.2008.

Komunikat Komisji Europejskiej, *Przygotowanie kolejnych etapów rozwoju zarządzania granicami w Unii Europejskiej*, COM(2008) 69.

Komunikat Komisji Europejskiej, *Silniejsze i bardziej inteligentne granice w UE: Komisja proponuje ustanowienie systemu wjazdu/wyjazdu*, IP/16/1247, 6.04.2016.

Komunikat Komisji Europejskiej, *Unia bezpieczeństwa: Komisja eliminuje luki informacyjne, aby lepiej chronić obywateli UE*, IP/17/5202, 12.12 2017.

Komunikat Komisji Europejskiej, *Unia bezpieczeństwa: Komisja z zadowoleniem przyjmuje porozumienie polityczne w sprawie zamknięcia luk w systemach informacyjnych*, IP/19/846, 5.02.2019.

Nye J.S., *Soft Power: The Means to Success in World Politics*, New York 2004.

Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), COM(2017) 794 final, 2017/0352 (COD).

[32] Szerzej zob. Rozporządzenie 2018/1240, Dz. Urz. UE L 236 z 19.09.2018, s. 50–51, art. 60.

Rozporządzenie (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich, Dz. Urz. UE L 312 z 7.12.2018, s. 1–13.

Rozporządzenie (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006, Dz. Urz. UE L 312 z 7.12.2018, s. 14–55.

Rozporządzenie (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, Dz. Urz. UE L 312 z 7.12.2018, s. 56–106.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011, Dz. Urz. UE L 327 z 9.12.2017, s. 20–82.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226, Dz. Urz. UE L 236 z 19.09.2018, s. 1–71.

Urząd Publikacji Unii Europejskiej, Strategia bezpieczeństwa wewnętrznego Unii Europejskiej, *Dążąc do europejskiego modelu bezpieczeństwa*, Luksemburg 2010, s. 22–30.

Wniosek Komisji Europejskiej w sprawie Rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 562/2006 w związku ze stosowaniem systemu wjazdu/wyjazdu (EES) oraz programu rejestrowania podróżnych (RTP), COM(2013) 96 final, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0096:FIN:PL:PDF [dostęp: 03.06.19].

Working document for the Joint Declaration on the EU's legislative priorities for 2018–19: *31 new initiatives for a More United, Stronger and More Democratic Union*, https://ec.europa.eu/commission/sites/beta-political/files/working-document-joint-declaration-legislative-priorities-2018-19_en.pdf [dostęp: 15.06.2019].

System wjazdu i wyjazdu (EES) i Europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS). Rola i znaczenie nowoczesnych systemów w zakresie działań prewencyjnych i wzmacniania bezpieczeństwa UE
Streszczenie

Celem artykułu jest zdefiniowanie znaczenia i przydatności nowych systemów wielkoskalowych: Systemu wjazdu i wyjazdu (EES) oraz Europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) w aspekcie poprawy bezpieczeństwa

wewnętrznego UE. Praca opiera się na założeniu, że dotychczasowy deficyt informacyjny w odniesieniu do niektórych kategorii obywateli państw trzecich uniemożliwiał właściwą i skuteczną ochronę granic zewnętrznych UE. Poprzez wypełnienie luk informacyjnych, systemy przyczynią się do pełnej implementacji zintegrowanego zarządzania granicami, a to z kolei – do efektywnego zwalczania przestępstw o charakterze transgranicznym. Artykuł został opracowany na podstawie metody instytucjonalno-prawnej, natomiast główną bazą źródłową były rozporządzenia ustanawiające nowe systemy. Metoda analizy komparatystycznej została zastosowana w celu określenia specyfiki tych dwóch systemów pod względem zasad, kategorii danych oraz oddziaływania na bezpieczeństwo.

Słowa kluczowe: System wjazdu i wyjazdu (EES), Europejski system informacji o podróży oraz zezwoleń na podróż, systemy informacyjne, strefa Schengen

Entry/Exit System (EES) and European Travel Information and Authorisation System (ETIAS): The Role and Importance of Modern Systems in the Area of Preventive and Strengthening of EU Security
Abstract

The purpose of the article is to define the importance and usefulness of new large-scale systems: Entry/Exit System and European Travel Information and Authorisation System in the aspect of improving the EU's internal security. The work is based on the assumption that the current information deficit in relation to certain categories of third-country nationals prevented the proper and effective protection of EU's external borders. By filling information gaps, systems will contribute to the full implementation of integrated border management, which in turn will effectively combat cross-border crimes. The article was compiled on the basis of the institutional and legal method, while the main source database were Regulations establishing new systems. The comparative method was used to determine the specificity of two systems in terms of principles, data categories and impact on safety.

Key words: Entry/Exit System (EES), European Travel Information and Authorisation System (ETIAS), information systems, Schengen Area

Europäisches Einreise-/ Ausreisesystem (EES) und Europäisches Reiseinformations- und Autorisierungssystem (ETIAS) – Rolle und Bedeutung der modernen Systeme im Bereich der Präventionsmaßnahmen und Verstärkung der EU-Sicherheit
Zusammefassung

Das Ziel des Artikels ist die Bedeutung und den Nutzen der neuen Großsysteme: Europäisches Einreise-/ Ausreisesystem (EES) und Europäisches Reiseinformations- und Autorisierungssystem (ETIAS) im Aspekt der Verbesserung der EU-Innensicherheit zu definieren. Der Artikel beruht auf der Annahme, dass das bisherige Informationsdefizit in Bezug auf manche Kategorien der Bürger der Drittländer einen richtigen und wirksamen Schutz der EU-Außengrenzen unmöglich machte. Wenn die Informationslücken

geschlossen werden, tragen die Systeme der vollen Implementierung der integrierten Verwaltung über die Grenzen bei und dadurch können die Strafftaten von einem grenzüberschreitenden Charakter effektiv bekämpft werden. Der Artikel wurde aufgrund einer institutionellen und rechtlichen Methode bearbeitet, die grundlegende Quellenbasis waren dagegen die die neuen Systeme festlegenden Rechtsvorschriften. Die Methode einer vergleichenden Untersuchung wurde zur Festlegung von zwei Systemen hinsichtlich der Prinzipien, der Kategorien und Auswirkung auf die Sicherheit verwendet.
Schlüsselwörter: Europäisches Einreise-/ Ausreisesystem (EES), Europäisches Reiseinformations- und Autorisierungssystem (ETIAS), Informationssysteme, Schengen-Raum

Система въезда и выезда (EES) и Европейская система авторизации и информации о путешествии (ETIAS). Роль и значение современных систем в области профилактических действий и обеспечения безопасности ЕС

Резюме

В статье рассматривается значение и полезность новых широкомасштабных систем: Системы въезда и выезда (EES) и Европейской системы авторизации и информации о путешествии (ETIAS) в области обеспечения внутренней безопасности ЕС. Исследование базируется на предположении, что существующий дефицит информации о некоторых категориях граждан третьих государств был причиной недостаточно надежной и эффективной защиты внешних границ ЕС. Ликвидация пробелов в информационных системах будет способствовать созданию системы целостного управления границами, что поможет в эффективной борьбе с трансграничной преступностью. В статье был использован институционально-правовой метод. Исследование базировалось на анализе нормативно-правовых актов, устанавливающих новые системы. Метод компаративистского анализа был использован для указания специфики этих двух систем с точки зрения их принципов, категорий данных и влияния на обеспечение безопасности.
Ключевые слова: Система въезда и выезда (EES), Европейская система авторизации и информации о путешествии (ETIAS), информационные системы, Шенгенская зона

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-006

Elżbieta Majchrowska
PhD, Andrzej Frycz Modrzewski Krakow University
ORCID: 0000-0001-5980-2903

Asian Development Bank and its Impact on Improving Security in the Asia-Pacific Region

Introduction

The modern world economy has been undergoing substantial changes over the last decades. They mainly result from the growing globalization, the rise of the Asia-Pacific region as the global economic center of gravity, increased competition of the emerging markets, the crisis of the World Trade Organization (WTO) forum, and, in turn, intensification of trade regionalism. The shift of the economic development pole towards the dynamically expanding region of Asia-Pacific, as well as the strengthening of integration processes, accompanied by the transforming international environment and the multifaceted diversity of this region's economies is becoming a source of a number of threats, and, at the same time, constituting a serious challenge not only regionally, but, owing to the size and significance of this area, also on the global scale.

A crucial fact, in this context, is that since the end of the Cold War, issues of non-military relevance have markedly gained in importance in the environment of international security. As a result, it is greatly influenced by the economic situation as well as the natural environment.[1]

The aforementioned heterogeneity of the countries of the region, particularly, the extreme disparities in economic development and the resulting increased

[1] Cf. B. Drelich-Skulska, P. Skulski (eds.), *Bezpieczeństwo międzynarodowe w regionie Azji i Pacyfiku. Wybrane zagadnienia*, Wrocław 2010.

vulnerability of many areas of functioning of the states, make them significant issues from the perspective of this sub-system of world economy, thus, in need of thorough investigation and the focal point of considerations of the present paper. The article constitutes an attempt at an in-depth reflection on the problem of security in the Asia-Pacific region, in particular, in the economic and ecological dimension.

An issue of great significance is, therefore, the activity of organizations which, by making efforts to mitigate threats and react quickly in case they appear, improve the level of security. The organization whose activity merits special attention, in this context, is the Asian Development Bank (ADB).

The paper concentrates on very important and topical problems from the point of view of transformations that are taking place in the area of international relations. The aim of the article is to analyze and assess operations of ADB in the Asia-Pacific region, particularly, in the context of threats to the economic and ecological security. The main point of this article is a statement that the activity of the Asian Development Bank contributes significantly to increasing security in this region. The principal method employed to achieve the aims of this article was the analytical and descriptive method. The research is based on the data originating from resources of international organizations, chiefly the Asian Development Bank and the World Trade Organization. The discussion is accompanied by the information presented in the tabular form.

Characteristics of the Asia-Pacific region

In geographical terms, the Asia-Pacific region is the largest area in the world.[2] Due to lack of a uniform definition, it is difficult to accurately delineate its borders, and accounts related to the countries of the region that are present in the subject literature are made in different frameworks. As is usual, the generally accepted distinction between the East Asia and Asia-Pacific implies excluding Australia, New Zealand and the countries of Oceania from the former area. However, there is a noticeable tendency to treat these economies as a consistent sub-system of world economy, i.e. the area of Asia-Pacific, which is also reflected in the approach of international organizations such as WTO.[3] Another categorization that may be found in the subject literature is the division into three sub-regions: North-East Asia, South-East Asia and Oceania.[4] When attempting to further specify the boundaries of the region one may also employ the criterion of APEC (Asia-Pacific Economic

[2] B. Drelich-Skulska, 'Charakterystyka regionu Azji i Pacyfiku', in B. Drelich-Skulska (ed.), *Azja-Pacyfik. Obraz gospodarczy regionu*, Wrocław 2007, p. 19.

[3] For instance, WTO classifies Australia, New Zealand and Oceania to Asia or East Asia. Cf. P. Kozielski, *Australia i jej rola w kształtowaniu procesów integracyjnych w obszarze Azji Pacyfiku*, Warszawa 2015, p. 172; WTO, World Trade Report 2011, *The WTO and preferential trade agreements: from co-existence to coherence*, Geneva 2011, pp. 239–240, https://www.wto.org/english/res_e/booksp_e/anrep_e/world_trade_report11_e.pdf (accessed 27.06.2019).

[4] P.W. Preston, *Pacific Asia in the Global System*, Oxford 1998, p. 4, as cited in K. Starzyk (ed.), *Zagraniczne inwestycje bezpośrednie w gospodarkach Azji Pacyfiku*, Warszawa 2001, p. 12.

Co-operation) membership, currently counting 21 countries.[5] In line with the ADB typology, it is assumed in the present article that Asia-Pacific consists of regional and non-regional members.[6]

The region's size is directly related to the immense diversity of countries comprising it. The area combines countries of dissimilar history, tradition, culture and various political systems and levels of economic development, however, one may also observe a relative degree of convergence of interests, which are building awareness and a need for regional affiliation. We may encounter there countries that are enormous in terms of population or territory, but also those that belong to the smallest states in the world, varied in relation to their ethnicity, religion (the majority of the world's religions), system (from constitutional monarchies, through democratic republics, to communist states and military dictatorships) or the social order (e.g. disparate levels of education). Taking into account the economic potential, this region's countries do not make up a uniform group.[7] We may find there economies which are highly developed and rich, even of the superpower status, as well as those which are of the lowest level of development, with GDP *per capita* not exceeding USD 1000.[8] The economic disparities of such a magnitude between countries and regions pose a serious threat to their economic security. It is also connected with the issue of ecological security since the majority of threats of this sort are caused by human activity, what's more, striving for rapid economic growth is often accompanied by environmental degradation. Furthermore, the ecological security in some regions is threatened by a variety of climatic and natural conditions.[9] Thus, due to the specificity of this vast region, originating in its multifaceted diversity in combination with the process of emerging as the global economic center of gravity, the region faces a number of dangers, which pose considerable challenges in terms of security both, on the regional, as well as the global level.

Concept and essence of security

The subject literature offers numerous definitions of security. This notion may be defined simply as a state without any threats. It is, at the same time, the most

[5] Cf. E. Haliżak, *Stosunki międzynarodowe w regionie Azji i Pacyfiku*, Warszawa 1999, p. 51; APEC, https://www.apec.org (accessed 25.06.2019).

[6] Details pertaining to this division have been explained thoroughly in the subsequent part of this paper.

[7] The founding countries of ASEAN, i.e. Indonesia, Malaysia, Philippines, Singapore and Thailand may be regarded as the least diverse regional group. However, as new members joined the bloc over the following years, the group was becoming less homogeneous, which resulted in the emergence of two sub-groups: ASEAN-5 (original members) as well as CLMV (Cambodia, Laos, Myanmar, Vietnam). Cf. ASEAN, https://asean.org (accessed 25.06.2019).

[8] According to the World Bank data (at current prices, USD). *The World Bank*, https://data.worldbank.org (accessed 26.06.2019).

[9] Natural and climatic conditions in the region are the reason for a relatively small share of the agricultural land in the total acreage. Severe floods ruining the farmland and adversely affecting economic growth are often a consequence of artificial irrigation of large areas and river watercourses regulation. This situation has a negative influence on the level of ecological security in some regions of Asia-Pacific, particularly in Indonesia, China or India.

universal definition, which can be referred to a wide array of threats that may have a destabilizing effect on a given country or region.[10]

The problem of security was traditionally the point of interest for strategic studies, which may be defined as studies on the threat, use and control of the military force.[11] Nevertheless, the ending of the Cold War contributed to the growth of studies on security, also including its aspects that go beyond the purely military considerations.[12] In the typology by B. Buzan, accentuating the multidimensional approach to security, one may differentiate between five large, interrelated sectors, namely the military, political, socio-cultural, economic and ecological sector.[13]

It may, thus, be stated that the concept of security refers to virtually all aspects of life and is currently more extensive in its scope than in the past, it also undergoes continual transformations. What it more, it refers to different levels – global, regional, local as well as the level of a social group or an individual.[14]

Being a key category in international relations, security is subject to considerable changes, particularly, since the beginning of the 1990s. The processes of globalization as well as strengthening ties between entities in world economy contribute to the emergence of new threats, which prompts the inclusion of non-military aspects, especially those of the economic or ecological nature, in security analyses.

Economic security[15] consists in "unrestricted access to markets, financial means and natural resources, which guarantee the continual growth of the country as well as sustaining its position"[16]. As mentioned before, it is inextricably linked to the matter of ecological security since threats in this regard often result from the economic activity of man and it concerns such issues as the pollution of water, air and soil. This situation is clearly visible in the examined region and requires taking active measures, which constitutes a great share of activities of numerous organizations, in particular, ADB.

[10] See more: Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (accessed 30.11.2019); K. Żukrowska, M. Grącik (eds.), *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, Warszawa 2005, p. 21.

[11] *Ibidem*.

[12] J. Czaputowicz, *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998, p. 23.

[13] B. Buzan, *People, States and Fear: The National Security Problem in International Relations*, Brighton 1983; 2nd ed., revised.: *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, London 1991; K. Żukrowska, M. Grącik (eds.), *Bezpieczeństwo międzynarodowe…*, *op. cit.*, p. 74.

[14] B. Drelich-Skulska, P. Skulski (eds.), *Bezpieczeństwo międzynarodowe w regionie Azji i Pacyfiku…*, *op. cit.*, p. 22.

[15] Certainly, the dominant threat to the economic security of the Asia-Pacific region are the enormous disparities in economic development between regions, countries and within borders of one country, e.g. China (between the Eastern and Western provinces). Cf. *Ibidem*, p. 28.

[16] J. Czaputowicz, *System czy nieład? Bezpieczeństwo europejskie…*, *op. cit.*, p. 24.

Origins and evolution of Asian Development Bank activities in the region

Since the end of the Cold War, institutions have played a key role in shaping security both, in the global, as well as the regional dimension. Thus, while analyzing the problem of security in the Asia-Pacific region, the significance of international organizations ought to be emphasized since their activities are instrumental in both, minimizing potential dangers, as well as resolving dilemmas in some areas of functioning of states. A crucial role is, therefore, played by the United Nations (UN), as well as regional organizations such as ASEAN (Association of South-East Asian Nations). One of the fundamental conditions for eliminating potential threats to security in the region is cooperation of all countries, which is expected to providing sustainable development. It needs to me stressed that the prime mover and coordinator of activities for the collaboration in the region of Asia-Pacific is the Asian Development Bank, which also provides a substantial part of funding.[17]

The idea of establishing a development bank for the region of Asia-Pacific first emerged as early as the late 1950s[18], however, a concrete outline of the concept of founding such an institution was presented at the 1963 'Ministerial Conference on Asian Economic Cooperation', convened on the initiative of the United Nations Economic Commission for Asia and the Far East (ECAFE). Two years later, during the second Ministerial Conference, the agreement establishing the Asian Development Bank was signed and the bank started its operations by the end of 1966. Its registered office is situated in Manila. The organizational structure comprises: the Board of Governors, the Board of Directors and the President. The first president of the bank was the Japanese vice-minister and the executive director of the International Monetary Fund and the World Bank – Mr. Takeshi Watanabe.[19]

In accordance with its statute, membership in ADB may be granted to countries which are members of ECAFE, its associate members as well as to other countries of the region or even those which lie beyond it, providing they belong to UN or specialized agencies.[20]

The ADB's founders were 31 countries, currently, it comprises 68 entities, including 49 countries of the region of Asia-Pacific (regional members) and 19 of the so-called non-regional members (the USA, Canada, countries of the Western Europe and Turkey).[21] A crucial distinction is also made within the group of regional members, i.e. into the sub-group of the developed member economies, consisting of Australia, Japan and New Zealand, and the sub-group of the developing member economies (developing Asia) – the remaining 46 countries belong to this group.

[17] As regards the issue of global security, the institution of key importance is the United Nations, and it is this organization which holds the superior position in the system of international organizations in relation to other entities of the regional character. Cf. Drelich-Skulska B., Skulski P. (eds.), *Bezpieczeństwo międzynarodowe w regionie Azji i Pacyfiku…*, *op. cit.*, pp. 281ff.

[18] UNESCO, *Guide to Archives of International Organizations*, https://unesdoc.unesco.org/archives (accessed 30.06.2019); ADB History, https://www.adb.org/about/history (accessed 20.06.2019).

[19] *Ibidem*.

[20] E. Oziewicz, T. Michałowski (eds.), *Międzynarodowe stosunki gospodarcze*, Warszawa 2013, p. 372.

[21] *ADB Members*, https://www.adb.org/about/members (accessed 20.06.2019).

The principal goal of activities of the organization was combating poverty and contributing to the improvement of functioning of the population. The rationale for founding the bank was a necessity for establishing a financial institution that would contribute to increasing the level of economic development as well as strengthening cooperation in this region of the world by providing financing.[22] The adopted aims have been achieved mainly by managing the available resources and making use of them for financing economic development while taking into account predominantly the needs of the least developed and poorest countries of the region, as well as supporting development-oriented projects. Another important aspect worth noting is the fact that the member countries are assisted in harmonizing their development policies, taking into consideration more effective management of available resources, increasing the degree of complementarity of economies as well as facilitating the sustainable development of foreign trade, in particular, the intra-regional trade. The bank is also expected to provide technical assistance related to the implementation of development projects.[23]

As the years passed and adjustments were made in order to cope with the current world economy problems, the scope of the bank's activities also evolved. Over the following decades, this institution's operations were involved in the implementation of numerous projects that had been intended to spur development in the region. What could be observed, however, were the changes in the approach towards financing such initiatives as well as areas for which these funds were allocated. The initial stage of the bank's operations, i.e. 1960s, was a period when ADB's efforts concentrated on the production of food and the development of rural areas.[24] In the 70s, however, the area of high interest for the institution was the development of educational and healthcare programs, then, also infrastructural initiatives, which involved primarily building networks of roads and electricity, which, in turn, impacts economic progress.[25] It is worth mentioning that the outcomes of the first oil shock of 1973 resulted in increased support for projects involving power industry, particularly, those promoting the development of domestic sources of energy. A milestone was the establishment of the Asian Development Fund (ADF) in 1974, whose purpose is to support the poorest members of the bank. It is relevant that until the end of the decade in question, the situation of some countries improved substantially and they were not forced to use the bank's assistance. As a consequence of the second oil shock in the 1980s, the bank continued implementation of projects reinforcing infrastructure, particularly, power industry.

[22] The aims of the Bank's activities have been defined in Article 1 of the Statute. Cf. E. Oziewicz, T. Michałowski (eds.), *Międzynarodowe stosunki gospodarcze*, *op. cit.*, p. 372; B. Drelich-Skulska, P. Skulski (eds.), *Bezpieczeństwo międzynarodowe w regionie Azji i Pacyfiku*…, s. 311–312.

[23] E. Oziewicz, T. Michałowski (eds.), *Międzynarodowe stosunki gospodarcze*, *op. cit.*, p. 373.

[24] In 1960s and 70s, the Special Agricultural Fund operated alongside ADB and its main goal was financing, among other things, the program for the development of agriculture in Asia under the name "Green Revolution".

[25] B. Drelich-Skulska, 'Rola organizacji międzynarodowych w procesach integracyjnych Azji Wschodniej na przykładzie Azjatyckiego Banku Rozwoju', *Zeszyty Naukowe Kolegium Gospodarki Światowej*, no. 25, 2009, p. 72.

More support was also allotted to social infrastructure, environment, education, urban planning or the issue of healthcare. In 1982, the first field office was opened in Bangladesh in order to move the bank's operations closer to the people in need. Next, ADB started cooperation non-governmental organizations. In the 1990s, ADB's activity focused on facilitating regional cooperation. Following the end of the Cold War, the number of members was growing owing to the inclusion of countries of Central Asia. A vital move of ADB, a response to the 1997 Asian crisis, was the implementation of programs and projects supporting the financial sectors in the countries of region as well as establishing a network of social security for the poorest. At the end of the decade, in 1999, seeing that economic growth bypasses some parts of the region, an overarching goal of poverty reduction was adopted. With the beginning of the new century, assistance in achieving the 'Millennium Development Goals' of the bank's members became the focal point. It was necessary in that time to face a number of unexpected incidents related to numerous epidemics or devastating natural disasters, which demanded enormous regional collaboration. They constituted a serious threat to e.g. ecological security. The assistance to combat those threats that was rendered by ADB both, on the national, as well as the regional level, was of paramount importance.[26]

Despite overcoming the aftermath of the 2008+ economic crisis by the majority of countries of the region, which was a considerable threat to their economic security, and a relatively high average GDP growth rate[27], this region is still largely inhabited by the poor population and the problem of inequality continues to remain a pressing issue. As a result of the wide gap between the rich and the poor, the primary focus of ADB's activities has been put on promoting development that facilitates social inclusion in the region.

It must also be stressed that the level of achievement of the 'Millennium Development Goals' was not spread out evenly between particular regions and countries. In spite of the fact that the bank's assistance greatly contributed to reducing extreme poverty, this region is still inhabited by 1.2 billion people living on less than USD 3 per day.[28] Furthermore, facing up to challenges such as sustainable development and protection of the environment is still seen as a necessity, which, in turn, is related to reducing dangers originating from human activity.

[26] ADB allocated over USD 850 million to recovery aid for selected areas of India, Indonesia, Sri Lanka, among others, which were hit by the tsunami in December 2004. Over USD 1 billion was allotted to help victims of the earthquake in Pakistan, in 2005. In 2009, the capital base was tripled (from 55 to USD 165 billion), which offers more financial means to react to outcomes of the world economic crisis. *ADB History*, https://www.adb.org/about/history (accessed 20.06.2019).

[27] In 2010, the regional average GDP growth rate stood at 9%. The pace and level of economic recovery were astonishing, China was referred to as the engine of economic growth. Cf. E. Majchrowska, *Wpływ członkostwa w WTO na handel zagraniczny Chin. Implikacje dla gospodarki światowej*, Kraków 2014, p. 181.

[28] *ADB History*, https://www.adb.org/about/history (accessed 20.06.2019).

Asian Development Bank's methods of providing economic and ecological security

The projects financed by the bank are related to infrastructure (a key element in the process of growth); strengthening economic cooperation in the regional dimension; protection against degradation of the natural environment; development in the financial sector, food policy and education. They are instrumental in mitigating threats e.g. of the economic or ecological nature, and, in turn, a significant increase in the level of security in these areas, which is critical owing to the specificity of countries of this region. Infrastructural investments are a key element in achieving economic growth, and, consequently, eliminating poverty. What is more, they result in strengthening the integration processes in the region.[29]

The principal methods of providing financial aid by ADB include loans, grants, equity investments and guarantees. Over the period 2010–2017, the bank successfully carried out over 340 projects in 33 countries, totaling over USD 100 billion. The largest number of projects were implemented in China (51), Bangladesh (29), Indonesia (28), Vietnam (27) and India (25). The sectors that received the biggest support were transport and communication, power industry, finance, agriculture and natural resources.[30]

As regards the sources of financing of the bank's operations, they comprise the so-called ordinary capital resources[31] and the special funds. The former include ADB's own funds (paid-in capital of member countries) as well as funds borrowed by this institution, acquired by issuing bonds into international capital markets. However, among the special funds, the most important role is played by the above-mentioned Asian Development Fund by means of which grants are distributed and loans with very low interest-rates are offered to the most impoverished countries of the region. Besides the ADF, there are other special funds such as Technical Assistance Special Fund, ADB Institute Special Fund, Asian Tsunami Fund, Asia Pacific Disaster Response Fund as well as the High-Level Technology Fund, established in 2017.[32]

The countries with the highest share in the basic capital of ADB include Japan and the USA (each 15.57%), Australia (5.77%), Canada (5.21%), Germany (4.31%), China (6.43%), India (6.32%), Indonesia (5.43%) and South Korea (5.03%). The regional members hold 63.39%, and the non-regional members have 36.61% of the total share, as of 2018.[33]

[29] ADB, *Strategy 2020: The Long-Term Strategic Framework of the Asian Development Bank 2008–2020,* Mandaluyong City 2008, https://www.adb.org/sites/default/files/institutional-document/32121/strategy2020-print.pdf (accessed 15.06.2019).

[30] ADB, *Successful ADB Projects*, https://www.adb.org/about/our-work (accessed 25.06.2019); E. Oziewicz, T. Michałowski (eds.), *Międzynarodowe stosunki gospodarcze*, *op. cit.*, p. 373.

[31] They are used for financing loans, which are granted on terms comparable to market terms. Cf. *Ibidem*.

[32] *High-Level Technology Fund*, https://www.adb.org/site/funds/funds/high-level-technology-fund (accessed 25.06.2019); E. Oziewicz, T. Michałowski (eds.), *Międzynarodowe stosunki gospodarcze*, *op. cit.*, pp. 373–374.

[33] *ADB Annual Report 2018*, http://www.adb.org/ar2018 (accessed 15.06.2019).

ADB also provides technical assistance, which involves project preparation as well as conducting advanced research in the general area of economic aspects pertaining to the countries of the region. The effect of these analyses are numerous research papers and reports aiding business practice in the countries of the region. The value of the total ADB's financial aid is presented in the table 1.

Table 1. The value of the total financial aid (loans, equity investments, grants, guarantees, technical assistance) provided by ADB (including co-financing) over the years 2010–2018 (USD million)

Year	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Value	17,936	20,374	20,925	20,991	22,841	26,540	25,468	31,818	35,817

Source: Author's own elaboration, based on: *ADB Annual Report 2014*, https://www.adb.org/documents/adb-annual-report-2014; *ADB Annual Report 2018*, http://www.adb.org/ar2018 (accessed 15.06.2019).

It needs to be noted that the beginning of the 1990s revealed some problems related to the projects initiated by ADB. Due to the substantial scattering of these projects, some of them were characterized by low effectiveness and the financial resources were simply wasted. At the same time, it was also a period of growing tendencies associated with the liberalization of trade in world economy[34], moreover, the number of ADB members was rising consistently after the Cold War had come to an end.[35] These aspects contributed to the process of drawing up the 1994 'Regional Cooperation Policy', which, alongside other ADB programs, constituted the basis for the 'Regional Cooperation and Integration' (RCI). It is in favor of the 'open regionalism' in the Asia-Pacific, regarding it as the foundation of the 'liberal global economy'.[36]

RCI is a process thanks to which individual countries become more affiliated to their region. It plays a key role in accelerating economic growth, eliminating poverty and economic inequalities, and, in turn, contributes to improving economic security. On account of closer integration in trade, as well as intra-regional supply chains, the developmental gaps between developing member economies of ADB become narrower, which allows economies to spur their own expansion.[37]

It must be emphasized at this point that the Asia-Pacific countries actively participate in integration processes, both on the regional scale and globally (see table 2). The countries of the region first joined these initiatives in the mid-nineties. Despite the significant diversity, the economic interdependence between countries of the region is growing due to the development and bolstering of trade in

[34] It concerns the establishment of the WTO and an almost simultaneous onset of the third wave of trade regionalism.

[35] In the 90s, ADB was joined by countries of Central Asia, among others.

[36] B. Drelich-Skulska, *Rola organizacji międzynarodowych w procesach integracyjnych Azji Wschodniej…*, *op. cit.*, p. 74; *ADB's Focus on Regional Cooperation and Integration*, https://www.adb.org/themes/regional-cooperation/main (accessed 30.06.2019).

[37] *Ibidem*.

the region. Benefits derived from this cooperation compel the countries to intensify these efforts.[38]

Table 2. FTAs by scope (cumulative) in Asia-Pacific countries (1980–2019)

Year	1980	1995	2000	2005	2010	2015	2019
Bilateral	0	27	46	98	135	158	178
Plurilateral	2	4	5	25	42	63	76

Source: Author's own elaboration, based on: *Asia Regional Integration Center*, https://aric.adb.org (accessed 20.06.2019).

Making the countries of the region come closer together by means of projects promoting regional cooperation and integration is one of the cornerstones of this bank since its founding. The effects of these activities in the region such as roads, power plants or bridges positively impact economic growth by, among other things, increasing the volume of trade.[39]

On the basis of the fundamental provisions of RCI, in 2008, ADB adopted the document *Strategy 2020: The Long-Term Strategic Framework of the Asian Development Bank 2008–2020*[40], which specified the course and future operations of the bank in the following decade. In the adopted document, the overarching goal of ADB was re-affirmed, which was the reduction of poverty ("Asia and Pacific region free of poverty"). Other challenges that were identified for the region are e.g. social aspects (inequalities, demographic transformations, the necessity of improving education), limitations stemming from the deficit of the infrastructure, and, above all, threats to the natural environment resulting from the rapid economic growth. As a side note, it needs to be stressed that according to the estimated figures the degradation of the natural environment connected with pollution may decrease the GDP of the Asia-Pacific region countries by approximately 5% over the following 40 years.[41]

[38] P. Pasierbiak, 'Chiny a wschodnioajatycka integracja gospodarcza de iure', *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, no. 266, 2016, p. 170.

[39] In 2008, in Laos the construction of the Route 3 Highway was completed, it stretches from the country's northern border with China to the southern border, near Thailand. In 2013, the Fourth Thai–Lao Friendship Bridge, which links the banks of the river Mekong, was finished. It was instrumental in increasing the volume of trade between countries of the region. Both the road and the bridge are part of the project financed by ADB, i.e. 'The Greater Mekong Subregion North–South Economic Corridor Project', which is meant to link Kunming in China with Bangkok via the northwest part of Laos. The project involves modernization of roads, construction of bridges as well as taking other measures to facilitate cooperation in terms of trade between these three countries. It's one of tens of projects in the Asia-Pacific region in which ADB promotes regional collaboration and integration as a foundation for operations of this institution in the region. Cf. *ADB's Focus on Regional Cooperation and Integration*, https://www.adb.org/themes/regional-cooperation/main (accessed 25.06.2019).

[40] ADB, *Strategy 2020: The Long-Term Strategic Framework…*, *op. cit.*, https://www.adb.org/sites/default/files/institutional-document/32121/strategy2020-print.pdf (accessed 15.06.2019).

[41] Z.W. Puślecki, *Unia Europejska – Chiny. Nowe zjawiska w stosunkach handlowo-ekonomicznych*, Poznań 2018, p. 488.

As mentioned before, the purpose of the bank is to support countries in implementing projects focused on development be means of integration and strengthening ties with the neighboring countries. Building larger regional markets is aimed at improving effectiveness of resources use as well as increasing the competitiveness of the region. Closer cooperation in the region is meant to enhance capacities of the countries and regions in terms of reacting more efficiently to sudden and unexpected changes in the economic situation, which may pose a serious threat to the economic security in the region.[42] Rapid changes in this area force ADB to always keep in step and adjust to new needs and requirements of the developing member states.

The countries of the Asia-Pacific region have made great strides in poverty reduction and economic growth over the last 50 years (see table 3), ADB, on the other hand, has remained the key partner in the course of all these transformations. Nevertheless, some issues require further steps and continuing development projects, what is more, new tendencies emerging in world economy, i.e. technical advances, urbanization or demographic changes constitute considerable challenges that this institution needs to face. The new long-term strategy of the bank is expected to aid in these endeavors.

Table 3. Population and GDP in developing Asia (1966–2015)

Year	1966	1976	1986	1996	2006	2015
GDP ($ billion)	163	426	1,014	2,937	6,412	18,063
Population (million)	1,718	2,173	2,626	3,124	3,555	3,903
GDP per capita ($)	95	196	386	940	1,804	4,628
Share of world GDP (%)	8	7	7	9	13	25
Share of world population (%)	51	52	53	54	54	53

Source: *ADB through the decades – ADB's Fifth decade (2007–2016)*, https://www.adb.org/sites/default/files/publication/216306/adb-fifth-decade-updated-edition.pdf (accessed 17.06.2019).

The 2030 Strategy[43] sets out new directions for the development of the bank that will meet the changing needs of the region. According to the strategy adopted for the following decade, measures aimed at eliminating extreme poverty will remain to be taken, as well as the concept of achieving the prosperous, inclusive, resilient and sustainable region of Asia-Pacific will be developed. ADB will make its contribution by combining financing, knowledge and the broadly-defined cooperation. The ambitious plans of growth ought to be dovetailed with the specificity of local conditions of individual members of the bank. It is related to increasing

[42] The occurrence of such threats is plausible. The deteriorating conflict between China and the USA may adversely affect the economic growth in the region (in 2018, China's GDP rose by 6.6%, which has been the lowest result for nearly three decades), and, due to the openness of economies, the transmission of the crisis to other countries cannot be ruled out.

[43] ADB, *Strategy 2030. Achieving a Prosperous, Inclusive, Resilient, and Sustainable Asia and the Pacific*, Mandaluyong City, July 2018, https://www.adb.org/sites/default/files/institutional-document/435391/strategy-2030-main-document.pdf (accessed 12.06.2019).

the importance of the 'country-focused approach', which is particularly significant owing to the diversity of these countries. It will entail granting long-term financial assistance by the bank, which will support countries of low and lower-middle income. However, financial aid for the middle-income countries will be provided selectively, for singled-out areas, and allocated to places where it is expected to impact the accomplishment of the priority goals, i.e. supporting the underdeveloped areas and poverty pockets. Measures taken in this way will be instrumental in the mitigation of threats of the economic and ecological nature and, at the same time, improving the security level in these areas.

The bank's support (including operations of the public and private sector, advisory services and knowledge) will concern the following, seven key operational priorities:

- further reduction of poverty and elimination of social inequalities;
- fostering progress in gender equality;
- combating climate change, reinforcing natural disasters resilience[44], augmenting environmental sustainability[45];
- making cities more accommodating;
- promoting development of rural areas and providing food security;
- strengthening governance and institutional capacity;
- facilitating regional cooperation and integration.[46]

To conclude, it is worth pointing out that on the account of the size of the Asia-Pacific region and its significance to world economy, achieving the primary global commitments such as the 'Sustainable Development Goals' or implementation of the provisions of the climate agreement in Paris[47], will largely depend on the success in this region.

Conclusions

Despite the multifaceted heterogeneity of the countries of Asia-Pacific, we may observe this region's emergence as the new global economic center of gravity, and dynamic transformations that occur in this area, e.g. the intensive trade regionalism. These aspects are a contributing factor in the inclusion of these countries in the mainstream of world economy, which is currently one of the most important characteristics of its development. The diversity of the countries as well as the widespread involvement in global economy, however, constitute a considerable

[44] Over the period 2000–2018, an average of nearly 38 thousand fatalities per year were reported in the countries of the region, as a result of natural disasters. Cf. ADB, *Asian Development Outlook (ADO) 2019: Strengthening Disaster Resilience*, April 2019, https://www.adb.org/publications/asian-development-outlook-2019-strengthening-disaster-resilience (accessed 05.07.2019).

[45] Over the years 2019–2030, ADB will allocate a total of approximately USD 80 trillion from their own funds to finance operations related to climate.

[46] ADB, *Strategy 2030. Achieving a Prosperous…*, *op. cit.*, https://www.adb.org/sites/default/files/institutional-document/435391/strategy-2030-main-document.pdf (accessed 12.06.2019).

[47] At the Paris climate conference in December 2015, 195 countries adopted the first-ever universal, legally binding global climate deal. Cf. *Paris Agreement,* https://ec.europa.eu/clima/policies/international/negotiations/paris_en (accessed 15.06.2019).

source of threats to security, in particular, from the economic and ecological perspective, and, at the same time, are a challenge for individual countries, as well as international organizations, in terms of mitigation of these risks.

The analysis of main areas of activities of the Asian Development Bank as well as the adopted methods, presented in the paper, provides for the conclusion that this institution is instrumental in increasing the level of security in the region, particularly within the discussed scope. Therefore, it may be stated that ADB provides added value to processes strengthening the stability of the region, which, owing to its significance, may also have a positive impact on the entire world economy.

References

ADB Annual Report 2018, http://www.adb.org/ar2018 (accessed 15.06.2019).

ADB's Focus on Regional Cooperation and Integration, https://www.adb.org/themes/regional-cooperation/main (accessed 30.06.2019).

ADB History, https://www.adb.org/about/history (accessed 20.06.2019).

ADB Members, https://www.adb.org/about/members (accessed 20.06.2019).

ADB through the decades – ADB's Fifth decade (2007–2016), https://www.adb.org/sites/default/files/publication/216306/adb-fifth-decade-updated-edition.pdf (accessed 17.06.2019).

ADB, *Asian Development Outlook (ADO) 2019: Strengthening Disaster Resilience*, April 2019, https://www.adb.org/publications/asian-development-outlook-2019-strengthening-disaster-resilience (accessed 05.07.2019).

ADB, *Regional Cooperation and Integration Strategy*, July 2006, https://www.adb.org/sites/default/files/institutional-document/32091/final-rci-strategy-paper.pdf (accessed 15.06.2019).

ADB, *Strategy 2020: The Long-Term Strategic Framework of the Asian Development Bank 2008–2020*, Mandaluyong City 2008, https://www.adb.org/sites/default/files/institutional-document/32121/strategy2020-print.pdf (accessed 15.06.2019).

ADB, *Strategy 2030. Achieving a Prosperous, Inclusive, Resilient, and Sustainable Asia and the Pacific*, Mandaluyong City, July 2018, https://www.adb.org/sites/default/files/institutional-document/435391/strategy-2030-main-document.pdf (accessed 12.06.2019).

ADB, *Successful ADB Projects*, https://www.adb.org/about/our-work (accessed 25.06.2019).

Czaputowicz J., *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998.

Drelich-Skulska B., 'Charakterystyka regionu Azji i Pacyfiku', in B. Drelich-Skulska (ed.), *Azja-Pacyfik. Obraz gospodarczy regionu*, Wrocław 2007.

Drelich-Skulska B., 'Rola organizacji międzynarodowych w procesach integracyjnych Azji Wschodniej na przykładzie Azjatyckiego Banku Rozwoju', *Zeszyty Naukowe Kolegium Gospodarki Światowej*, no. 25, 2009.

Drelich-Skulska B., Skulski P. (eds.), *Bezpieczeństwo międzynarodowe w regionie Azji i Pacyfiku. Wybrane zagadnienia*, Wrocław 2010.

Haliżak E., *Stosunki międzynarodowe w regionie Azji i Pacyfiku*, Warszawa 1999.

Kozielski P., *Australia i jej rola w kształtowaniu procesów integracyjnych w obszarze Azji Pacyfiku*, Warszawa 2015.

Majchrowska E., *Wpływ członkostwa w WTO na handel zagraniczny Chin. Implikacje dla gospodarki światowej*, Kraków 2014.
Oziewicz E., Michałowski T. (eds.), *Międzynarodowe stosunki gospodarcze*, Warszawa 2013.
Paris Agreement, https://ec.europa.eu/clima/policies/international/negotiations/paris_en (accessed 15.06.2019).
Pasierbiak P., 'Chiny a wschodnioajatycka integracja gospodarcza de iure', *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, no. 266, 2016.
Preston P.W., *Pacific Asia in the Global System*, Oxford 1998.
Puślecki Z.W., *Unia Europejska – Chiny. Nowe zjawiska w stosunkach handlowo-ekonomicznych*, Poznań 2018.
Starzyk K. (ed.), *Zagraniczne inwestycje bezpośrednie w gospodarkach Azji Pacyfiku*, Warszawa 2001.
Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf (accessed 30.11.2019).
The World Bank, https://data.worldbank.org (accessed 26.06.2019).
UNESCO, *Guide to Archives of International Organizations*, https://unesdoc.unesco.org/archives (accessed 20.06.2019).
WTO, *Regional trade agreements and the WTO*, https://www.wto.org/english/tratop_e/region_e/scope_rta_e.htm (accessed 20.06.2019).
WTO, World Trade Report 2011, *The WTO and preferential trade agreements: from co-existence to coherence*, Geneva 2011, https://www.wto.org/english/res_e/booksp_e/anrep_e/world_trade_report11_e.pdf (accessed 27.06.2019).
Żukrowska K., Grącik M. (eds.), *Bezpieczeństwo międzynarodowe. Teoria i praktyka*, Warszawa 2005.

Azjatycki Bank Rozwoju i jego wpływ na podnoszenie poziomu bezpieczeństwa w regionie Azji i Pacyfiku
Streszczenie

Wielowymiarowe zróżnicowanie krajów Azji i Pacyfiku oraz ich szerokie powiązania z gospodarką globalną stanowią istotne źródło zagrożeń dla bezpieczeństwa, szczególnie w wymiarze ekonomicznym i ekologicznym, a jednocześnie są wyzwaniem, zarówno dla poszczególnych państw, jak i organizacji międzynarodowych. Dlatego też wszelkie podejmowane działania mające na celu ograniczanie potencjalnych zagrożeń nabierają obecnie szczególnie istotnego znaczenia. W tym kontekście kluczowa staje się rola działających w regionie organizacji międzynarodowych. Wśród nich na uwagę zasługuje działalność Azjatyckiego Banku Rozwoju (Asian Development Bank, ADB), który stanowi główne forum umożliwiające podejmowanie współpracy oraz harmonizujące kooperację państw w regionie. Przedsięwzięcia finansowane przez ADB skupiają się m.in. wokół infrastruktury, wzmacniania regionalnej współpracy gospodarczej, ochrony środowiska naturalnego czy zapewnienia bezpieczeństwa żywnościowego. Poprzez wdrażanie licznych projektów (np. Strategia 2030) działalność tej organizacji w znacznym stopniu przyczynia się do poprawy poziomu bezpieczeństwa regionalnego. ADB wnosi wartość dodaną do procesów wzmacniających stabilność regionu, co – ze względu na jego znaczenie – może także wpływać w sposób pozytywny na całą gospodarkę światową.
Słowa kluczowe: Azjatycki Bank Rozwoju, bezpieczeństwo międzynarodowe, region Azji i Pacyfiku

Asian Development Bank and its Impact on Improving Security in the Asia-Pacific Region
Abstract

The multifaceted heterogeneity of the countries of Asia-Pacific as well as strong ties with economies worldwide constitute a considerable source of threats to security, in particular, from the economic and ecological perspective, and, at the same time, are a challenge for individual countries, as well as international organizations. Therefore, all activities undertaken to mitigate potential threats are becoming critical. In this context, the key role is played by international organizations functioning in the region. Among them, one that merits particular attention is the Asian Development Bank (ADB), which constitutes the premier forum that caters for undertaking joint efforts and harmonizing cooperation among the countries in the region. Initiatives financed by ADB focus on such issues as infrastructure, reinforcing regional economic cooperation, preservation of the natural environment and ensuring food security. Through implementation of numerous projects (e.g. Strategy 2030), activities of this organization greatly contribute to improving the regional security. ADB provides added value to processes strengthening the stability of the region, which, owing to its significance, may also have a positive impact on the entire world economy.
Key words: Asian Development Bank, international security, Asia-Pacific region

Die Asiatische Entwicklungsbank und ihr Einfluss auf die Verbesserung des Sicherheitsniveaus in der Asien-Pazifik-Region
Zusammefassung

Die mehrdimensionale Differenzierung der Länder in der Asien-Pazifik-Region und umfangreiche Verbindungen dieser Länder zur globalen Wirtschaft sind eine bedeutende Quelle für die Bedrohung der Sicherheit, besonders auf ökonomischer und ökologischen Ebene und sind gleichzeitig eine Herausforderung, sowohl für einzelne Staaten, als auch für internationale Organisationen. Deswegen sind zur Zeit alle Maßnahmen, die es zum Ziel haben potenzielle Risiken zu vermeiden, besonders wichtig. Diesbezüglich wird die Rolle der in dieser Region tätigen internationalen Organisationen entscheidend. Unter ihnen verdient Aufmerksamkeit die Tätigkeit der Asiatischen Entwicklungsbank (Asian Development Bank, ADB), die ein Forum für die Aufnahme der Zusammenarbeit und für die Harmonisierung der Kooperation der Länder in dieser Region ist. Die von ADB finanzierten Unternehmungen konzentrieren sich u.a. auf die Infrastruktur, Verstärkung der regionalen wirtschaftlichen Zusammenarbeit, auf den Umweltschutz oder Gewährleistung der Ernährungssicherheit. Durch die Einführung zahlreicher Projekte (z. B. Strategie 2030) trägt die Tätigkeit dieser Organisation der Verbesserung der Sicherheit in dieser Region bei. ADB leistet einen Mehrwert zu den

Prozessen, welche die Stabilität in dieser Region verstärken, was – hinsichtlich der Bedeutung der Bank – sich positiv auf die globale Wirtschaft auswirken kann.
Schlüsselwörter: Asiatische Entwicklungsbank, internationale Sicherheit, Asien-Pazifik-Region

Азиатский банк развития и его влияние на повышение уровня безопасности в Азиатско-Тихоокеанском регионе

Резюме

Многообразие стран Азиатско-Тихоокеанского региона и их широкие связи с мировой экономикой являются существенным источником угроз для безопасности, особенно экономического и экологического характера, а также проблемой для отдельных государств и международных организаций. Поэтому любые принимаемые меры, направленные на снижение потенциальных рисков приобретают особо важное значение. В этом контексте действующие в регионе международные организации стали играть ключевую роль. Среди них особого внимания заслуживает деятельность Азиатского банка развития (Asian Development Bank, ADB), который является основной площадкой для установления сотрудничества и гармонизации действий государств региона. Проекты, финансируемые ADB, в частности, связаны с развитием инфраструктуры, укреплением регионального экономического сотрудничества, охраной окружающей среды, обеспечением продовольственной безопасности. Благодаря внедрению многочисленных проектов (напр. «Стратегия 2030») деятельность этой организации способствует повышению уровня региональной безопасности. ADB поддерживает процессы, усиливающие стабильность региона, что положительно влияет на всю мировую экономику.
Ключевые слова: Азиатский банк развития, международная безопасность, Азиатско-Тихоокеанский регион

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-007

Mirosław Laszczak
dr inż., Wyższa Szkoła Ekonomiczno-Humanistyczna w Bielsku-Białej
ORCID: 0000-0001-6060-4285

Zarządzanie bezpieczeństwem w erze cyfrowej

Wprowadzenie

Postępująca cyfryzacja zmieniła gospodarkę. Przestrzeń i czas utraciły swój bezwzględny paradygmat, a dostęp do informacji i przetwarzanie danych stało się łatwe jak nigdy wcześniej. Nie bez powodu mówi się o rewolucji cyfrowej przenicowującej kulturę, ekonomię, a przede wszystkim świadomość. Świat nie jest już taki przed pięćdziesięciu laty – warunki prowadzenia biznesu trudno porównywać nawet do tych z końca XX w. Cyfryzacja przeorała każdą dziedzinę życia, dokonując nieodwracalnej konwergencji wirtualnego i rzeczywistego świata. Pojawia się internet rzeczy (*Internet of Things*, IoT) – będący siecią przedmiotów, procesów i ludzi ciągle podłączonych do internetu. Dochodzi do hiperkomunikacji (*hyperconnectivity*). Urządzenia bez przerwy przetwarzają ogromne ilości informacji (*big date analylics*, BDA), a część usług dokonuje się w obliczeniowej chmurze (*cloud computing*). Normą staje się automatyzacja i robotyzacja. Przyzwyczailiśmy się do wielokanałowości i wszechkanałowości dystrybucji produktów (*omni channel*). Przez 24 godziny na dobę konsumenci korzystają z cyfrowego dostępu do dóbr i usług (*digital customer access*).

Obserwowane zmiany mają charakter rewolucyjny, formy biznesu znane z poprzedniego stulecia stają się nie tylko niewydolne, ale wręcz nie przystają do nowych czasów. Wiele osób, także tych, którzy zarządzają przedsiębiorstwami, nie do końca zdaje sobie sprawę z charakteru dokonujących się zmian. Coraz więcej informacji przetwarzanych jest poza umysłem decydenta, intuicja przestała mieć znaczenie, a pomiędzy zarządzającymi i konsumentami pojawili się informatycy, korzystający z systemów tak złożonych, że dla większości użytkowników niezrozumiałych.

Przez ostatnich pięćdziesiąt lat moc obliczeniowa procesorów podwaja się z każdym mijającym rokiem. Koszty przetwarzania informacji maleją w tym samym tempie, a co dwa lata pojawia się więcej informacji niż w całej wcześniejszej historii. Bez ustanku generujemy nowe informacje, łączymy się z bankami, wysyłamy wiadomości tekstowe, publikujemy prace naukowe, a przede wszystkim w zapisie binarnym składujemy dane finansowe. W każdym dowolnym momencie ktoś dokonuje operacji bankowych, a liczbę sprzedanych smartfonów mierzy się w miliardach. Nie należy się łudzić – biznesowe połączenia są smakowitym kąskiem nie tylko dla domorosłych przestępców rekrutujących się spośród znudzonych studentów informatyki. Kradzieżą informacji zajmują wyspecjalizowane działy poważnych i praworządnych zdawałoby się instytucji. Firma General Electric wielokrotnie skarżyła się na podsłuchiwanie przez zagranicznych konkurentów. Po koniec lat 80. XX w. przegrała wiele przetargów w Europie, czasem różnicą zaledwie kilku tysięcy dolarów. Wynajęci przez firmę eksperci dość szybko znaleźli przyczynę: konkurenci uważnie śledzili satelitarną łączność General Motors i podsłuchiwali rozmowy. Firma zakupiła wówczas tak zwane telefony bezpieczne, szyfrujące połączenia. Wydatek rzędu stu tysięcy dolarów opłacił się: GE znowu zaczęła wygrywać przetargi na Starym Kontynencie[1].

Ten i podobne przypadki utorowały drogę nowemu myśleniu o bezpieczeństwie w czasach powszechnej informatyzacji, komputeryzacji i digitalizacji zarchiwizowanych danych. Stało się jasne, że należy wyjść poza znane dotychczas metody bronienia dostępu do zgromadzonej w organizacji wiedzy, a sposób ochrony winien przyjąć formę systemowego zarządzania bezpieczeństwem.

Celem niniejszego artykułu jest przedstawienie niebezpieczeństw związanych z powszechną cyfryzacją gospodarki oraz wskazanie podstawowych elementów odpowiedzialnych za bezpieczeństwo organizacji na poziomie cyfrowym. Przyjęto hipotezę badawczą, zgodnie z którą zarządzanie bezpieczeństwem w erze cyfrowej odbiega od klasycznych konotacji związanych z tym pojęciem, gdyż koncentruje się na zagrożeniach wynikłych z informatyzacji procesów zarządzania i komunikowania się ze światem zewnętrznym. Zarządzanie bezpieczeństwem w erze cyfrowej wymaga podejścia systemowego i oprócz sprecyzowania zbioru najważniejszych zasad, konieczna jest koncentracja wysiłków na kluczowych i dających się wyodrębnić obszarach aktywności organizacji.

Formy zagrożeń

Przechytrzyć system, wedrzeć się poza zaporę bezpieczeństwa i nie ruszając się z fotela, uzyskać dostęp do cudzych pieniędzy lub zastrzeżonych informacji. W 2008 r. świat obiegła interesująca wiadomość. W ręce amerykańskiej policji wpadł haker, który wniknął do systemu informatycznego sieci marketów i jednocześnie przeniknął do firmy produkującej karty kredytowe. Nie ruszając się z domu skradł – bagatela − 130 mln USD. Oczywiście nie działał sam, do dyspozycji miał gang zorganizowany z nastoletnich hakerów, którzy nie znalazłszy dla siebie zatrudnienia

[1] P. Schweizer, *Szpiedzy wśród przyjaciół. Jak sojusznicy wykradają Amerykanom tajemnice technologiczne*, tłum. J. Lobman, Z. Słomkowski, Warszawa 1997, s. 287.

pośród „białych kapeluszy”[2], zdecydowali się wykorzystywać swe umiejętności w mniej szlachetny sposób. Ze swobodą poruszali się w galimatiasie informatycznych komend, wynajdywali luki w systemach komputerowych, włamywali się na konta bankowe i przejmowali tajne informacje. Wśród zatrzymanych znajdował się młody człowiek, który jako nastolatek zhakował komputery NASA, za co otrzymał wyrok sześciu miesięcy poprawczaka. Ktoś taki i jemu podobni nigdy nie przestaną buszować w sieci; w ten sposób zaspakajają atawistyczne pragnienie polowania – o tyle wygodnie, że nie trzeba ruszać się z domu, można siedzieć w ulubionym fotelu, jeść pizzę i popijać colę. Młodzi informatycy, dla których sieć jest labiryntem z oznaczonymi ścieżkami, mają szansę na udowodnienie intelektualnej przewagi nad twórcami zabezpieczeń. Zabawa miesza się z przygodą, przyzwyczajenie zahacza o uzależnienie, a łatwość dużego zarobku kusi. Z czasem hakerzy okazali się także prawdziwymi specjalistami od ludzkiej psychiki. Zwerbowani przez nich przeciętni konsumenci zostali się „słupami” przyjmującymi przelewy i depozyty bankowe oraz wysyłającymi je do odległych geograficznie banków. Ten rodzaj oszustwa rozpowszechnił się w 2009 r.: banki i ich klienci stracili wówczas znacznie ponad 120 mln USD[3].

Współcześnie nie ma już kraju, firmy ani organizacji, które nie byłyby zagrożone hakerskim atakiem. W sukurs nieczystym intencjom idą technologie pomagające zachować anonimowość w sieci. Jedną z nich jest sieć TOR (The Onion Router) działająca w najbardziej zakamuflowanych i najciemniejszych miejsca w sieci. Pozwala ona na anonimowe korzystanie z dostępnych zasobów w sieci powierzchniowej, a także ułatwia dostęp do zaszyfrowanych treści[4]. Czy może zatem dziwić dynamika wzrostu przestępczości internetowej?

Komenda Główna Policji informuje, że w 2018 r, w porównaniu z rokiem 2017 nastąpił stuprocentowy wzrost liczby przestępstw odnoszących się do e-bankowości i phishingu.

Tabela 1. Wzrost liczby przestępstw dotyczących bankowości elektronicznej na tle ogólnej liczby przestępstw bankowych

Rok	**2014**	**2017**	**2018**
Przestępstwa o charakterze bankowym	2,5 tys.	6 tys.	7,4 tys.
Przestępstwa z zakresu phishingu i e-bankowości	585	1,8 tys.	3,6 tys.
Skimming*	brak danych	433	743

* przestępstwo polegające na nielegalnym skopiowaniu karty płatniczej (np. poprzez umieszczenie dodatkowego czytnika i nadajnika w konstrukcji bankomatu).

Źródło: opracowanie własne na podstawie: W. Boczoń, *100 proc. wzrost liczby przestępstw dotyczących e-bankowości. Statystyki policji*, PRNews.pl, https://prnews.pl/100-proc-wzrost-przestepstw-dotyczacych-e-bankowosci-statystyki-policji-441137 [dostęp: 12.06.2019].

[2] „Białe kapelusze” to hakerzy, którzy sprawdzają oprogramowanie pod kątem luk w zabezpieczeniach, a znalezione niedoróbki zgłaszają producentowi, aby pomóc uszczelnić program i zabezpieczyć go przed ingerencją tych „złych” – czyli „czarnych kapeluszy”.

[3] K. Poulsen, *Haker. Prawdziwa historia szefa cybermafii*, tłum. T. Macios, Kraków 2011, s. 266.

[4] A. Nastuła, *Fałszerstwo dokumentów ze szczególnym uwzględnieniem przestępczości internetowej jako wyzwanie dla organów państwa*, „Polonia Journal” 2018, nr 8, s. 80–83.

Banki oraz ich klienci atakowani są na różne sposoby. Oprócz tradycyjnego phishingu przestępcy wykorzystują jego mutacje, sięgają więc po vishing i smishing. Dochodzi do wyłudzeń z wykorzystaniem Blika i metody SIM-swap[5], tworzone są fałszywe aplikacje bankowe, które wzbudzają zaufanie, gdyż udostępniane są w markecie Google Play.

Nieskończona jest pomysłowość oszustów, którzy z sieci informatycznych uczynili wygodne narzędzie, o tyleż bardziej perfidne, że bazujące na naiwności i braku wiedzy niektórych użytkowników, wierzących w tajemną moc systemów informatycznych i bezgranicznie ufających witrynom internetowym.

Zagrożeń jest tak wiele, że jakakolwiek ich lista nigdy nie będzie kompletna. Ogólnie wyróżnia się[6]:

- kradzież lub niszczenie danych,
- podszywanie się pod inną osobę, kradzież wizerunku,
- propagowanie fałszywych informacji, tworzenie wirtualnych organizacji z myślą o dokonywaniu wyłudzeń,
- sabotaż i szantaż komputerowy,
- hacking,
- szpiegostwo komputerowe,
- piractwo komputerowe i kradzież myśli technicznej,
- manipulacje finansowe, w tym przede wszystkim fałszowanie operacji rozrachunkowych, dokonywanie zmian w stanach kont, malwersacje z użyciem kart bankomatowych,
- oszustwa teleinformatyczne i telekomunikacyjne.

Szczególnym rodzajem zagrożeń jest APT (*advanced persistent threats*), będący zorganizowanym, niemal masowym atakiem na systemy informatyczne. Obiektem ataków są zazwyczaj organizacje o kluczowym znaczeniu dla gospodarki. Ofiarami padają instytucje finansowe, organizacje społeczne, rządowe, systemy energetyczne i wojskowe. Forma ataku jest wielostopniowa i bardzo dobrze zakamuflowana. Rzadko kiedy chodzi wyłącznie o pieniądze, częściej – o sparaliżowanie ważnej gałęzi gospodarki, zaszantażowanie instytucji, a jeszcze częściej o szpiegostwo[7]. Ten rodzaj ataków stanowi jedno z największych niebezpieczeństw, nie dziwi zatem, że jest wykorzystywany w konfliktach międzypaństwowych. Za pomocą APT udaje się wywołać chaos i zakłócić obieg pieniądza w gospodarce, można uzyskać przewagę ekonomiczną i militarną, doprowadzić do sparaliżowania systemów

[5] Phising – metoda polegająca na wysyłaniu fałszywych e-maili (pochodzących jakoby z banku), informujących o konieczności pilnego przekazania poufnych danych lub przelania kwoty na określony rachunek; vishing – telefoniczne wyłudzanie danych wrażliwych (numerów kont, loginów, haseł, kodów dostępu) pod pozorem ich weryfikacji, audytu zewnętrznego lub modernizacji systemu komputerowego; smishing – wysyłanie fałszywych SMS-ów nakłaniających ofiarę do połączenia z podanym numerem lub wejścia na określoną stronę internetową, zawierającą np. wirusy i trojany; SIM-swap – oszustwo polegające na wyrabianiu duplikatu karty SIM telefonu służącego do autoryzacji transakcji w systemach bankowości internetowej i wyprowadzaniu w ten sposób środków z konta.

[6] M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4 (113), http://www.ebib.pl/2010/113/a.php?nowak [dostęp: 12.06.2019].

[7] I. Ghafir, V. Prenosil, *Advanced Persistent Threat Attack Detection: An Overview*, [w:] *Proceedings of International Conference on Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur 2014, s. 154, www.seekdl.org/nm.php?id=3901 [dostęp: 12.06.2019].

obronnych. W dodatku jest to atak trudny do odparcia, a generowane straty są poważne: zniszczeniu mogą ulec zgromadzone dane, serwery stają się niewydolne, następuje utrata łączności ze światem zewnętrznym. Dodatkowo trzeba uwzględnić całkiem realną kradzież informacji – w takiej sytuacji możliwe materialne i wizerunkowe szkody są trudne do oszacowania.

Wyróżnia się dwa zasadnicze rodzaje cyberataków:

- DDoS – czyli atak z zamiarem zablokowania serwisów i dokonania kradzieży danych;
- kradzież informacji wrażliwych z myślą o późniejszym publikowaniu ich w sieci, głównie w serwisach i portalach społecznościowych.

Szczególnym miejscem, w którym kumulują się ryzyka związane z cyberprzestępczością, jest chmura. *Cloud computing*, czyli przetwarzanie informacji na zewnątrz organizacji, może budzić zrozumiały niepokój, tym bardziej że:

- wciąż ograniczone są możliwości egzekwowania wymogów bezpieczeństwa na najwyższym poziomie u właścicieli chmury;
- organizacje, z którymi dana organizacja wymienia się informacjami, stanowią zagrożenie dla ochrony informacji zdeponowanych w chmurze;
- brakuje dobrze ustrukturalizowanej architektury i strategii rozwoju środowiska chmury, która gwarantowałaby stuprocentowe bezpieczeństwo zdeponowanych danych;
- występują luki w interfejsie obsługi. Za bezpieczeństwo API (*application programming interface*) odpowiadają dostawcy usług chmurowych, natomiast wykorzystanie kluczy, które powiązane są z interfejsami programistycznymi, znajduje się w gestii użytkowników usług chmurowych[8];
- wymóg korzystania wyłącznie ze sprawdzonych usługodawców nie zawsze może być spełniony.

Nie tylko wielość oraz różnorodność przestępstw w cyberprzestrzeni sprawia, że statystyki policyjne nie są dokładne. Wpływają też na to inne przyczyny:

- nie wszystkie przestępstwa zostają zgłoszone;
- dane ujawniają jedynie naruszenia prawa otagowane przez policjantów jako cyberprzestępstwo, w rzeczywistości nie wszystkie przypadki otrzymują tego typu opis;
- od wejścia w życie obowiązującej ustawy o świadczeniu usług drogą elektroniczną[9] z 2002 r. w technologii cyfrowej minęła cała epoka. Część popełnianych obecnie przestępstw nie była znana w czasie przygotowywania ustawy.

Wbrew obiegowym opiniom kradzieże bankowe, choć niewątpliwie bolesne, nie są największą zmorą osób odpowiedzialnych za bezpieczeństwo w sieci. Wykradanie informacji biznesowych i danych wrażliwych, transfer technologii – staje się problemem więcej niż palącym.

Słabość informatycznych zabezpieczeń ma dwa źródła. Pierwszym są luki w systemach komputerowych, które choćby i dokładnie sprawdzone, zawsze będą

[8] P. Waszczuk, *11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance*, https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance [dostęp: 12.06.2019].

[9] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r., nr 144, poz. 1204.

zawierać błędy pozostawione przez programistów. Drugim – jeszcze poważniejszym – jest sam człowiek ze swym roztargnieniem, lenistwem, ze swymi przyzwyczajeniami i skłonnością do robienia wszystkiego na skróty. Dotyczy to nawet pracowników, którzy na co dzień zajmują się bezpieczeństwem przesyłania danych w systemach informatycznych. Wystarczy na dowolnej stronie otworzyć *Sztukę infiltracji* Kevina D. Mitnicka i Williama L. Simona[10], by przekonać się o ludzkich słabościach, nazbyt łatwo wystawiających na szwank dane wrażliwe o trudnej do przecenienia wartości – i w swej nieroztropności narażających mienie tysięcy osób.

Ludzie zajmujący się bezpieczeństwem w branżach IT nie są w stanie pracować ciągle na najwyższych obrotach, wyczulona pierwotnie wrażliwość z czasem słabnie, ostrożność ulega stępieniu. Praca nie jest już wyzwaniem, lecz rutyną. Pracownicy przychodzą do swoich biur, siadają w wygodnych obrotowych fotelach, sprawdzają pocztę, przeglądają ulubione strony www i ani myślą o drobiazgowym sprawdzaniu logów, aby dowiedzieć się, kto przez noc zmienił hasło. Niewiele pomagają szkolenia. Wciąż są tacy, którzy dają się nabrać na starą sztuczkę z podrzuconym pendrive'em. Przypadkowo znaleziony (lecz celowo podrzucony) np. na parkingu nośnik danych uruchamiany jest na firmowych komputerach. Umieszczone na pendrivie szpiegowskie oprogramowanie natychmiast przenika do systemu całej instytucji. Niefrasobliwość bierze górę nad zasadami bezpieczeństwa, ciekawość dominuje nad zdrowym rozsądkiem. A wszystko to dzieje się przy pełnej świadomości niebezpieczeństwa związanego z uruchamianiem plików nieznanego pochodzenia, w instytucjach wysyłających pracowników na drogie szkolenia z bezpieczeństwa.

Nie trzeba jednak przypadkowo znalezionego pendrive'a. Pracownicy nazbyt łatwo przynoszą do pracy własne, domowe nośniki danych. Zabierają pracę do domu, chcą się pochwalić zdjęciami z wakacji, może zamierzają wydrukować w firmie prywatny dokument – możliwości jest bez liku, a z każdą związane jest niebezpieczeństwa zainfekowania systemu.

W grę wchodzi jeszcze jedno, wcale nie tak marginalne niebezpieczeństwo: chęć łatwego zarobku. „Jeśli tylko zaoferuje się odpowiednią cenę, wszyscy pracownicy, począwszy od dyrektora, a na gońcach i sprzątaczkach kończąc, okazują się potencjalnymi szpiegami"[11] – przekonuje jeden z konsultantów do spraw bezpieczeństwa. Nie bez wpływu na postawę pracowników jest panująca w firmie kultura organizacyjna oraz pewien rodzaj przyzwolenia na kradzież informacji. W zalewie danych, gdy codziennie mamy do czynienia z niekończącym się strumieniem informacji, gdy wydaje się, że jest ich tak wiele, że stają się bezwartościowe, trzeba doprawdy bardzo silnego charakteru lub bardzo restrykcyjnych kar, aby powstrzymać pracowników przed bagatelizowaniem poufnych wiadomości. Ważne są oczywiście przyzwyczajenia zawodowe i rozumienie samego pojęcia lojalności. U Amerykanów jest z tym różnie. Łatwo ich przekonać do wyniesienia poufnych danych. Osobiste kłopoty finansowe i nagłe potrzeby gotówkowe czynią z nich

[10] K.D. Mitnick, W.L. Simon, *Sztuka infiltracji*, tłum. C. Frąc, Warszawa 2006. Mitnick to były haker, skazany na wiele lat więzienia. W swojej książce opisuje techniki włamań i podkreśla, że najsłabszym ogniwem najdroższych i najbardziej wyrafinowanych systemów zabezpieczeń jest zawsze człowiek.

[11] P. Schweizer, *op. cit.*, s. 47.

stosunkowo łatwe źródło informacji. Nieuprawnione przekazywanie danych sojusznikom traktują co najwyżej jako formę wstydliwej transakcji. Dopiero przekazywanie informacji agentom rosyjskim lub chińskim jest uznawane za znacznie poważniejszy uszczerbek na honorze i złamanie obywatelskich norm[12].

Jak to wygląda w Polsce? Obserwacje nie są optymistyczne. Lojalność polskich pracowników jest niepewna i efemeryczna – bo i zatrudnienie bywa krótkotrwałe, uzależnione od wynagrodzenia, z opcją opuszczenia obecnego pracodawcy, gdy tylko pojawi się lepsza propozycja.

O ile *baby boomers* i pracownicy z pokolenia X szukają stałego zatrudnienia i wielce pociąga ich wizja pracy w jednym miejscu aż do emerytury, o tyle 63 % młodszych pracowników, w wieku pomiędzy 18 a 35 lat, nie wyobraża sobie, że zestarzeją się, pracując w jednej firmie[13]. Takie podejście osłabia lojalność, co dokumentują statystyki przestępczości. Według danych z 2018 r. połowa polskich przedsiębiorców zetknęła się w ciągu poprzednich dwóch lat z przypadkami nadużyć, z tego ponad połowę (55 %) popełnili zatrudnieni w firmie pracownicy[14].

Najbardziej wrażliwe na ataki cyberprzestępców są innowacyjne firmy oraz instytucje finansowe, zwłaszcza banki. Przeprowadzone przez Institute of International Finance i McKinsey & Company badania ujawniły, że 70 % banków uważa ryzyko związane z cyberatakami za główne zagrożenie, na które należy uwrażliwiać menedżerów średniego szczebla, 10 % ankietowanych stawia ten rodzaj ryzyka na czele listy wszelkich zagrożeń[15]. Nic dziwnego, że co trzeci bank w Europie czwartą część swojego budżetu na obniżanie ryzyka bankowego przeznacza na zarządzanie ryzykiem cyfrowym.

Bezpieczeństwu nie sprzyjają towarzyszące cyfryzacji współczesne trendy, zgodnie z którymi dąży się do jak najszerszego otwarcia na potrzeby klienta i dba się o zwiększenie dostępności usług.

Pierwszym takim trendem jest personalizacja dostępu. E-commerce i dostęp poprzez media społecznościowe jest jak wołanie: „Mamy dla was zawsze otwarte drzwi, zajrzyjcie, sprawdźcie, rozejrzyjcie się". Niechcący zaprasza się w ten sposób także osoby niepożądane, wraz z ich niszczycielskimi narzędziami i dążeniami. Drugi rynkowy trend odnosi się do nacisku konkurencji. W przypadku bankowości są to instytucje pożyczkowe, parabankowe. Chcąc sprostać wymaganiom klientów, banki uruchamiają nowe rozwiązania, nie zawsze właściwie zabezpieczone, a bywa, że przygotowane zbyt pospiesznie. Kolejnym trendem jest pogoń za obniżką kosztów. Informatyka znacznie w tym pomaga. Część czynności wykonują sami klienci – logują się na kontach, organizują przelewy – zastępując rzeszę pracowników.

[12] *Ibidem*, s. 48.

[13] Randstad, *Monitor Rynku Pracy*, 35 edycja, 2019, [za:] *Rośnie zadowolenie pracowników, maleje ich lojalność*, PRNews.pl, https://prnews.pl/rosnie-zadowolenie-pracownikow-maleje-ich-lojalnosc-444497 [dostęp: 12.06.2019].

[14] M. Klimczak, *Kto i jak okrada polskie firmy? 8. edycja badania przestępczości gospodarczej w Polsce*, PwC Polska, https://www.pwc.pl/pl/publikacje/2018/badanie-przestepczosci-gospodarczej-2018-raport-pwc.html [dostęp: 12.06.2019].

[15] *The future of risk management in the digital era*, McKinsey & Company, https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era [dostęp: 14.06.2019].

Czwarty trend jest ściśle związany z poprzednim i wynika wprost z nowego modelu biznesu. Informatyczne kanały przepływu informacji, funduszy i wiedzy oraz możliwość dotarcia do nich z dowolnego miejsca na świecie czyni je wrażliwymi na cyberataki. Trend piąty to deregulacje. Ułatwianie dostępu klientom, chęć zdobycia ich zaufania, upraszczanie procedur – za tym wszystkim idą deregulacje, ustępstwa, które mogą wystawiać na szwank bezpieczeństwo instytucji. I doprawdy trudno ustalić granicę pomiędzy konieczną sztywnością reguł, które utrudniają współpracę z klientem, a otwarciem się na klienta i sprowokowaniem niepotrzebnego ryzyka. Przecież rezygnacja z możliwości, jakie daje gospodarka cyfrowa, i pominięcie wymogu marketingowego podejścia do klienta, byłaby krokiem w tył. Klienci przyzwyczaili się do przyjaznych systemów, w których wpłat, wypłat i innych operacji dokonuje się łatwo i szybko, bez utrudnień i dodatkowych weryfikacji – które byłyby ceną za zwiększenie szczelności systemu. Jest też trend szósty: część funkcji związanych z bezpieczeństwem zostało przerzuconych na wyrafinowane systemy informatyczne. Nie człowiek, lecz skomplikowane i dla większości ludzi niezrozumiałe oprogramowanie stoi na straży bezpieczeństwa. Tyle tylko, że ufność w te systemy może być przesadzona. Wciąż pojawiają się doskonalsze narzędzia hakerskie, a i pomysłowość cybernetycznych przestępców zdaje się nie mieć granic. Dlatego od samego początku, gdy tylko pojawili się hakerzy, byli oni przekupywani przez firmy i zatrudniani z myślą o poprawie bezpieczeństwa.

Działania zaradcze

Nie ma oprogramowania doskonale chroniącego zdigitalizowane informacje. Nic nie da stuprocentowej pewności, że zarządzający systemami informatycznymi będą lojalni i czujni. Mylne jest przeświadczenie, że jakieś doraźne działania (jak choćby kupno lepszego pakietu informatycznego) zabezpieczają przed cyberprzestępstwami. Gdy zagrożenie jest realne i totalne, trzeba tworzyć kompleksowe zabezpieczenia. W takim przypadku mówi się o zarządzaniu ryzykiem cyfrowym (*digital risk management*). Jest to o tyle trudne, że zagrożenia mogą pojawić się w każdej chwili i w dowolnym miejscu. Ich źródło może tkwić w czynniku ludzkim, materialnym i wirtualnym.

Funkcję zapór bezpieczeństwa, niczym średniowieczne fosy, pełnią obecnie firewalle. Osoba, która nimi administruje, sprawdza konfigurację zapory, przygląda się logowaniom, identyfikuje ewentualne nielegalne zmiany. Ktoś, kto zinfiltruje zaporę sieciową, dokona także innych zmian w systemie i zapewni sobie dostęp do zastrzeżonych informacji. Największym grzechem administratora jest ufność w program komputerowy i w szczelność zapory. Z upływem czasu zawsze ujawnią się jej słabości. Naprawa w jednym miejscu prowadzi do powstania dziur gdzieś indziej. Niektóre porty pozostają niepotrzebnie otwarte, a serwery sieci web bywają źle skonfigurowane. Dlatego żaden firewall nigdy nie jest całkowicie szczelny. Gościnność, chęć stworzenia środowiska pracy, które jest przyjazne dla pracowników i partnerów biznesowych, rozmywa granice ochrony. Internetowi przestępcy szukają szczelin i luk, rozglądają się za słabościami, korzystając – przynajmniej na początku – z legalnych środków i przyjazności samego programu.

Wiele przedsiębiorstw stosuje programy odnotowujące próby włamań i zapobiegające infiltracji. Wszyscy oczekują, że te programy poradzą sobie same. Tymczasem są procedury, których firewall nie chroni. Wynika to z wygody używania sprzętu komputerowego, z posiadanych uprawnień, czasem z konieczności komunikowania się ze światem zewnętrznym i pobierania z zewnątrz pakietów danych. Dlatego tak ważne jest konstruowanie reguł, dzięki którym można filtrować pakiety przychodzące i wychodzące.

Firewalle skonfigurowane są już w taki sposób, aby identyfikować skanowanie portów z myślą o włamaniu. System samoczynnie odłącza takie połączenia oraz informuje o tego typu aktywności – ale tylko jeśli zastosowana przez hakera technika nie jest zbyt wyrafinowana. Stąd cały zestaw zaleceń dla personelu zajmującego się bezpieczeństwem. Chodzi o sprawdzanie listy procesów z intencją wykrycia tych, które nie są znane. Przeczesuje się programy w poszukiwaniu nieautoryzowanych dodatków. W plikach szuka się zmodyfikowanych binariów, skryptów i aplikacji. Usuwa się konta uśpione i nieznane. Reaguje się wzmożoną uwagą na zdalny dostęp z nieznanego miejsca.

Przezorni administratorzy nie ufają domyślnym konfiguracjom. Gdy instalują oprogramowanie pochodzące od zewnętrznej „niezależnej" firmy, z góry zakładają, że w programie znajdują się rozwiązania o charakterze szpiegowskim. Dotyczy to przede wszystkim przedsiębiorstw działających w branży finansowej, w branżach zaawansowanych technologii tudzież w przemyśle wojskowym, farmaceutycznym i biotechnologii. Dokonać infiltracji atrakcyjnej rynkowo firmy i poznać jej sekrety – to nie lada gratka i całkiem zyskowny interes.

Administratorzy co jakiś czas organizują spotkania z pracownikami: instruują ich, uczulają na zagrożenia, podają zbiory zasad. Część z tych zasad jest najczęściej ignorowana i obchodzona. Pracownicy wciąż nazywają pliki zgodnie z ich zawartością, wskazując drogę osobom zainteresowanym infiltracją. Każdy haker zajrzy przede wszystkim do plików opisanych jako „wyniki badań", spenetruje „kopie bezpieczeństwa", pomijając „harmonogram urlopów". Szyfrowanie plików poufnych jest wymogiem, od którego nie może być odstępstw. Istnieją do tego specjalne programy, oczywiście można je obejść i odszyfrować tajne informacje, wiąże się to jednak z koniecznością nieco dłuższego przebywania w sieci, a wszelka manipulacja przy tego typu plikach prędzej lub później obudzi jednak czujność administratora.

Lata wojny pomiędzy hakerami a zatrudnionymi w firmie informatykami oraz „białymi kapeluszami" nie pozostały bez wpływu na podniesienie standardów bezpieczeństwa. Teraz już wiadomo, że po zainstalowaniu oprogramowania koniecznie trzeba usunąć skrypty instalacyjne. Zdarzało się bowiem, że hakerzy zdobywali listy adresowe, wykorzystując słabości w domyślnym skrypcie instalacyjnym aplikacji.

Ryzyko cyfrowe a zarządzanie bezpieczeństwem

Cyberprzestrzeń jest tyleż intratnym, co wygodnym obszarem do działań przestępczych. Jest też obszarem wrażliwym, gdyż nawet niewielka ingerencja w zgromadzone dane uruchamia lawinę strat. Powiązane z sobą różnorodne formy ryzyka, niemal jak ułożone kostki domina, uruchamiają lawinę zdarzeń o trudnych do

wyobrażenia konsekwencjach. Rodzajów ryzyka jest tu bardzo wiele, wystarczy wymienić najważniejsze:

- ryzyko utraty dobrego imienia,
- ryzyko utraty wiarygodności,
- ryzyko kradzieży danych o charakterze badawczo-rozwojowym,
- ryzyko utraty danych klientów i narażenie się na procesy sądowe,
- ryzyko modyfikacji danych,
- ryzyko wycieku danych,
- ryzyko uszkodzenia systemów informatycznych,
- przerwa w działalności,
- ryzyko utraty pozycji rynkowej.

Wyłudzanie informacji, podszywanie się pod cudzą tożsamość, stawanie się „słupem" w nielegalnym procederze prania pieniędzy to kolejne, wcale nierzadkie zdarzenia. Dlatego także informatyka dopracowała się swojej definicji ryzyka – pod postacią normy IEC 61508, zgodnie z którą jest ono miarą zagrożenia tajności, integralności i dostępności informacji. Ryzyko należy traktować jako iloczyn prawdopodobieństwa wystąpienia sytuacji stwarzającej zagrożenie i skutków wyrażonych w wielkości poniesionych strat.

Stąd już tylko krok do zdefiniowania systemu zarządzania bezpieczeństwem danych, który znany jest jako norma ISO/IEC 27001[16]. Norma ta stała się punktem wyjścia dla tworzenia systemów zarządzania bezpieczeństwem informacji (*Information Security Management System*, ISMS). Istota zarządzania sprowadza się do utrzymywania ryzyka na poziomie akceptowalnym przez organizację, czyli zapewniającym efektywne osiąganie celów biznesowych przy jednoczesnym nienarażaniu na szwank rzeczowych i niematerialnych składników organizacji. Zarządzanie próbuje skłonność do ryzyka pogodzić z otwarciem się na potrzeby klienta, a sprawną interakcję pomiędzy rynkiem i organizacją – z długofalowym bezpieczeństwem.

Zarządzanie ryzykiem przyjmuje dwie formy[17]:

1) prewencji – rozumianej jako przygotowanie organizacji na cyberataki, monitorowanie sieci w organizacji, sprawdzanie podatności na zagrożenia, identyfikowanie możliwych zagrożeń,
2) minimalizacji strat wynikłych z cyberataków.

Prewencja jest tu najważniejsza. O tyle o nią trudno, że część zagrożeń nie jest nawet znana, część metod – nie dość rozpoznana, a kreatywność cyberprzestępców nie ma sobie równych. Najłatwiej określić podstawowy zestaw działań zaradczych. W grę wchodzi bowiem reglamentacja dostępu do sprzętu, oprogramowania, sieci zewnętrznych i wewnętrznych, a przede wszystkim – wglądu do zgromadzonych informacji. Ważne jest także ustalenie wymogów jakościowych odnośnie do sprzętu

[16] ISO/IEC 27001:2013(en): *Information technology – Security techniques – Information security management systems – Requirements*, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en [dostęp: 12.06.2019].

[17] E.I. Szczepankiewicz, P. Szczepankiewicz, *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, cz. 3: *Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów" 2006, nr 8, https://czasopisma.beck.pl/monitor-rachunkowosci-i-finansow/artykul/analiza-ryzyka-w-srodowisku-informatycznym-do-celow-zarzadzania-ryzykiem-operacyjnymbr-czesc-3-strategie-postepowania-z-ryzykiem-operacyjnym [dostęp: 12.06.2019].

i oprogramowania. Usługi IT zlecane czy wykonywane siłami samej organizacji to także jeden z obszarów, gdzie często dochodzi do powstania ryzykownych sytuacji. Nie można zapominać o aktualnych i odpowiednio sprawnych systemach wykrywania i usuwania złośliwego oprogramowania. Poprzestanie na uaktualnionej wersji programu antywirusowego może nie wystarczyć, warto go dostosować do specyfiki prowadzonej działalności. Organizacje ubezpieczają się od szkód, ale chyba najistotniejsze są szkolenia dla personelu i ugruntowane mechanizmy kontroli wewnętrznej. Nie daje to oczywiście stuprocentowej pewności, lecz znacznie utrudnia pracę cyberprzestępcom.

Kiedy już dojdzie do ataku hakerskiego, nie pozostaje nic innego jak uruchomić działania minimalizujące szkody. Przebiegają one wielotorowo i obejmują:

- aktywność marketingową, podejmowaną głównie przez dział PR z zadaniem zniwelowania ewentualnych strat wizerunkowych,
- identyfikację i szacowanie poniesionych szkód,
- ustalenie przyczyny, źródła wycieku danych i winowajców,
- wyodrębnienie puli środków na ewentualne odszkodowania,
- jak najszybsze uruchomienie planów awaryjnych i wdrożenie działań naprawczych,
- skorzystanie z urządzeń zapasowych (backupów).

Próbę skonstruowania modelu zarządzania bezpieczeństwem podjęto w firmie doradczej McKinsey & Company. Nie zbudowano co prawda spójnej koncepcji, wskazano jednak na zbiór elementów uważanych za podstawowe w dążeniu do zmniejszenia ryzyka[18].

Wszystko zaczyna się na poziomie zarządzania danymi. Posiadane przez przedsiębiorstwo informacje podlegają ścisłej klasyfikacji, dokonuje się taksonomicznych podziałów, uwzględnia wartość i wagę posiadanych danych, a następnie przypisuje do nich poziom ryzyka. Jest on zmienny, zależny od ilości danych, od źródeł ich pochodzenia i od sposobu wykorzystania. W nadmiarze informacji kryje się poważne niebezpieczeństwo. Gdy jest ich bardzo dużo, przestaje się dostrzegać ich wyjątkowość i rangę, a stąd tylko krok do ignorowania zasad bezpieczeństwa.

Drugim składnikiem zarządzania bezpieczeństwem cyfrowym jest automatyzacja i komputeryzacja procesów. Przywykliśmy już, że łącząc się z firmą, w słuchawce słyszymy przede wszystkim głos z automatu. Od tej tendencji nie ma odwrotu, czynnik kosztowy wygrywa. Klienci i kontrahenci samodzielnie wprowadzają dane do systemu, dzięki temu mają wrażenie, że wszystko dzieje się szybciej, że panują nad toczącymi się procesami. Dane te przechodzą następnie do środowiska pracy, są dostępne w dowolnym miejscu na niemal dowolnym stanowisku. Jest to znaczące udogodnienie, lecz równocześnie wzrasta możliwość penetracji systemu informatycznego. Jeśli firma wpuszcza do sieci każdego, kto tylko zechce, musi liczyć się z tym, że oprócz klientów znajdzie się tam haker, próbujący przetestować własne pomysły na cudzych zabezpieczeniach.

Na trzeci element zarządzania bezpieczeństwem składają się zaawansowane techniki analizowania procesów. Wyrafinowane algorytmy, samouczące się oprogramowanie − wysublimowane narzędzia informatyczne są tu stosowane z myślą

[18] *The future of risk management…*

o wynajdywaniu złożonych wzorców zachowań charakterystycznych dla niedozwolonych transakcji i komputerowych oszustw. Takie narzędzia są ogromnie pomocne. Menedżerowie zatrudnieni w banku są przekonani, że skraca to procedury kredytowe i wpływa na zmniejszenie zatrudnienia. W bankowych oddziałach nie trzeba już zatrudniać tak wielu pracowników. Dzięki szerokopasmowym łączom i podłączeniom do różnorodnych baz danych klienci w krótkiej chwili zostają „prześwietleni" – i okazują się bardziej lub mniej wiarygodni. Również możliwość pomyłki jest tu zapewne mniejsza, aniżeli wówczas, gdy ryzyko kredytu miałby ustalać pracownik banku. Ostateczna decyzja bazować będzie na danych pozyskanych z każdego rodzaju aktywności potencjalnego kredytobiorcy, nie ujdą uwadze nawet dokonywane przez niego zakupy w hipermarkecie. Informatyczne algorytmy podpowiedzą, jaką decyzję podjąć, zdejmując część troski o bezpieczeństwo z zatrudnionych w banku pracowników.

Takie działania nie byłyby możliwe bez rozwoju cybernetycznej infrastruktury. Spójna, elastyczna, bezpieczna, wygodna staje się koniecznością − i to zarówno z marketingowego, jak i technicznego punktu widzenia. Komfortowe, intuicyjnie działające interfejsy, łatwiejszy dostęp do kontrahentów, innowacyjne rozwiązania przechowywania i udostępniania danych, do tego ciągła łączność i podtrzymywanie wszystkich elementów systemu staje się podstawą każdej sprawnie działającej organizacji. Zarządzanie bezpieczeństwem sprowadza się do ustalenia równowagi pomiędzy wygodą użytkowania systemów a możliwością pojawienia się chętnych do ingerencji w infrastrukturę.

W systemie zarządzania bezpieczeństwem cyfrowym nie można pominąć jeszcze jednego elementu. Chodzi o podejście do ryzyka samych pracowników[19]. Posługiwanie się na co dzień terminologią ryzyka biznesowego i świadomość zagrożeń przenosi się na bezpieczeństwo funkcjonowania firmy we współczesnym, zdigitalizowanym świecie. Lecz wcale nie jest tak, że korzystanie z wyrafinowanych programów komputerowych usuwa pracowników w cień, zdejmuje z nich część odpowiedzialności za bezpieczeństwo cyfrowe. Wręcz odwrotnie, nabierają oni kluczowego znaczenia. Liczy się ich wykształcenie i doświadczenie zawodowe – im bardziej różnorodne, tym lepiej. Istotne, by pracownicy uwzględniali zagrożenia w swej bieżącej pracy i przebywali w kulturze organizacyjnej ceniącej eksperymentowanie. Przydaje się ich obycie z systemami informatycznymi i z pracą polegającą na obróbce informacji. W ten sposób odpowiednia polityka rekrutacyjna oraz szkolenia podnoszą bezpieczeństwo cyfrowe, a przy okazji obniżają koszty prowadzenia działalności – osoby zatrudnione na co dzień w firmie są o wiele tańsze niż zewnętrzni specjaliści i eksperci, którzy często nie znają specyfiki danego miejsca i charakteru przetwarzanych w nim informacji.

Mądra postawa pracowników staje się tym ważniejsza, gdy w grę wchodzi zagrożenie wynikające z ataków socjotechnicznych – przed którymi nie zabezpiecza żaden program antywirusowy i które są najtrudniejsze do wykrycia.

[19] Mówią też o tym przywoływane badania, zob. *ibidem*.

Podsumowanie

Nawet pobieżne przejrzenie statystyk zaskakuje dynamiką przyrostu liczby ataków hakerskich, ich różnorodnością i pomysłami przenikania przez szczelne zapory firewalli. Wzrasta liczba destrukcyjnych oddziaływań na systemy informatyczne pojedynczych firm i instytucji rządowych. Cyberprzestępczość wyszła z kart powieści fantastycznych i zadomowiła się w gospodarce. W sukurs przychodzą coraz doskonalsze systemy wykrywania niechcianych ataków, przedsiębiorstwa uczą się minimalizowania ryzyka. Dziś wiadomo, że dbałość o bezpieczeństwo jest trwałym składnikiem procesu zarządzania i wymaga traktowania systemowego. Świadome tego zarządy tworzą wyspecjalizowane komórki organizacyjne, a uczelnie – wychodząc naprzeciw oczekiwaniom rynku – uruchamiają nowe kierunki i specjalności koncentrujące się na zarządzaniu bezpieczeństwem. Bo choć nie da się wyeliminować zagrożeń, to podejście systemowe i doskonalenie zarządzania w kluczowych obszarach odpowiedzialnych za ryzyko umożliwiają prowadzenie stabilnego biznesu we współczesnej, coraz bardziej zdigitalizowanej erze.

Bibliografia

Boczoń W., *100 proc. wzrost liczby przestępstw dotyczących e-bankowości. Statystyki policji*, PRNews.pl, https://prnews.pl/100-proc-wzrost-przestepstw-dotyczacych-e-bankowosci-statystyki-policji-441137 [dostęp: 12.06.2019].

Ghafir I., Prenosil V., *Advanced Persistent Threat Attack Detection: An Overview*, [w:] *Proceedings of International Conference on Advances in Computing, Electronics and Electrical Technology*, Kuala Lumpur 2014, www.seekdl.org/nm.php?id=3901 [dostęp: 12.06.2019].

Klimczak M., *Kto i jak okrada polskie firmy? 8. edycja badania przestępczości gospodarczej w Polsce*, PwC Polska, https://www.pwc.pl/pl/publikacje/2018/badanie-przestepczosci-gospodarczej-2018-raport-pwc.html [dostęp: 12.06.2019].

Mitnick K.D., Simon W.L., *Sztuka infiltracji*, tłum. C. Frąc, Warszawa 2006.

Nastuła A., *Fałszerstwo dokumentów ze szczególnym uwzględnieniem przestępczości internetowej jako wyzwanie dla organów państwa*, „Polonia Journal" 2018, nr 8.

Nowak M., *Cybernetyczne przestępstwa – definicje i przepisy prawne*, „Biuletyn EBIB" 2010, nr 4 (113), http://www.ebib.pl/2010/113/a.php?nowak [dostęp: 12.06.2019].

Poulsen K., *Haker. Prawdziwa historia szefa cybermafii*, tłum. T. Macios, Kraków 2011.

Rośnie zadowolenie pracowników, maleje ich lojalność, PRNews.pl, https://prnews.pl/rosnie-zadowolenie-pracownikow-maleje-ich-lojalnosc-444497 [dostęp: 12.06.2019].

Schweizer P., *Szpiedzy wśród przyjaciół. Jak sojusznicy wykradają Amerykanom tajemnice technologiczne*, tłum. J. Lobman, Z. Słomkowski, Warszawa 1997.

Szczepankiewicz E.I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, cz. 3: *Strategie postępowania z ryzykiem operacyjnym*, „Monitor Rachunkowości i Finansów" 2006, nr 8, https://czasopisma.beck.pl/monitor-rachunkowosci-i-finansow/artykul/analiza-ryzyka-w-srodowisku-informatycznym-do-celow-zarzadzania-ryzykiem-operacyjnymbr-czesc-3-strategie-postepowania-z-ryzykiem-operacyjnym [dostęp: 12.06.2019].

The future of risk management in the digital era, McKinsey & Company, https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era [dostęp: 14.06.2019].

Waszczuk P., *11 zagrożeń dla bezpieczeństwa rozwiązań chmurowych według Cloud Security Alliance*, https://itwiz.pl/11-zagrozen-dla-bezpieczenstwa-rozwiazan-chmurowych-wedlug-cloud-security-alliance/ [dostęp: 12.06.2019].

Zarządzanie bezpieczeństwem w erze cyfrowej
Streszczenie

Era cyfrowa, przez przyspieszenie wymiany informacji i zmianę formy obiegu dokumentów, stworzyła nowe wejścia do przedsiębiorstw i urzędów. Już nie oszklone frontowe drzwi, lecz internetowe łącza prowadzą w głąb organizacji. Pracowników ochrony zastąpiły komputerowe systemy zabezpieczenia informacji, programy antywirusowe i firewalle. Światłowodami można dotrzeć znacznie dalej, przeniknąć w struktury organizacji nieporównanie głębiej i wyrządzić szkody wielokrotnie większe od tych, które mogli poczynić „klasyczni" złoczyńcy.

Zagrożeń jest tak wiele, że nie sposób ich wszystkich wymienić, a codziennie powstają nowe formy ataku i nieznane wcześniej sposoby wyłudzeń informacji i pieniędzy. Początkowo tworzono zbiory zasad, z którymi zaznajamiano pracowników. Dotyczyły one ochrony kopii i plików poufnych, sposobów tworzenia haseł dostępu, postępowania z informacjami. W stosunkowo krótkim czasie okazało się jednak, że ochrona przed cyberprzestępczością domaga się systemowego potraktowania. Pojawiło się pojęcie zarządzania bezpieczeństwem w erze cyfrowej – zagadnienie to jest usystematyzowane i skoncentrowane na jasno wyodrębnionych obszarach. Obejmuje: zarządzanie danymi, zarządzanie procesem przepływu informacji, zautomatyzowane procesy decyzyjne, zarządzanie infrastrukturą, inteligentne interfejsy, zarządzanie zewnętrznym „ekosystemem" informatycznym i zarządzanie umiejętnościami pracowników oraz kulturą organizacyjną. Koncentracja na tych obszarach na pewno nie wyeliminuje zagrożeń, lecz znacząco poprawi bezpieczeństwo, od którego często zależy dalsze trwanie organizacji.

Słowa kluczowe: era cyfrowa, bezpieczeństwo, cyberprzestępczość, zarządzanie bezpieczeństwem, ochrona danych

Security Management in the Digital Era
Abstract

The digital era, accelerating the exchange of information and changing the form of document circulation, have created new entrances to any organisations. No longer the glazed front door, but internet links lead someone deep into the organization. Guards and security services have been replaced by computer systems, anti-virus programs and firewalls. Using fiber optics some black-hat can reach much further, penetrate the structure of the organization incomparably deeper, causing damage many times greater than that occurred in the past.

There are so many threats that it is impossible to list them, every day new forms of attack and previously unknown ways of phishing information and form of stealing money are invented. Initially, sets of rules were created to familiarize employees with dangers.

They focused on the protection of confidential copies and files, on ways of creating access passwords and forms of handling information. In a relatively short time, however, it turned out that the digitized economy requires systematic treatment. The concept of security management in the digital era has emerged; it is systematized and focused on clearly identified areas. The security management in digitalized world includes such areas as: data management, process and work-flow automation, advanced decision-making automation, infrastructure management, intelligent interfaces, management of the external IT ecosystem and management of employee skills and organizational culture. Continuous improvement in the management of these areas will certainly not eliminate threats, but will significantly improve security, which is contemporary „to be or not to be" for any organization.

Key words: digital era, security, cyber crime, management, data protection

Sicherheitsmanagement im digitalen Zeitalter
Zusammenfassung

Das digitale Zeitalter schuf neue Eingänge in die Unternehmen und Ämter durch Beschleunigung des Informationsaustauschs und Wechsel der Dokumentationsabläufe. Zugang in die Tiefe der Organisation bietet nicht mehr eine Glaseingangstür sondern das Internet. Das Sicherheitspersonal wurde durch die computergestützten Systeme zum Schutz von Informationen, Antivirenprogramme und Firewalls ersetzt. Über die Glasfaserleitungen kann man wesentlich weiter vordringen, unvergleichbar tiefer die Organisationsstrukturen durchdringen und viel schlimmer schädigen, als die „klassischen" Verbrecher schädigen könnten.

Es gibt so viele Gefahren, dass unmöglich ist alle zu nennen und jeden Tag entstehen neue Angriffsformen und früher nicht bekannte Methoden, wie Informationen zu ergattern und Geld zu erpressen. Anfänglich wurden Grundregeln aufgestellt, mit denen sich die Mitarbeiter vertraut machen sollten. Dies betraf den Schutz von Kopien und vertraulichen Dateien, Methoden der Erstellung der Zugangscodes, Behandlung von Informationen. In kurzer Zeit zeigte sich aber, dass der Schutz vor der Cyberkriminalität eine Systembehandlung erfordert. Es tauchte das Phänomen des Sicherheitsmanagements im digitalen Zeitalter auf – dieses Problem wurde systematisiert und auf klar gegliederte Gebiete konzentriert. Es umfasst: Datenverwaltung, Informationsflussverwaltung, automatisierte Entscheidungen, Verwaltung der Infrastruktur, intelligente Schnittstellen, Verwaltung des äußeren „IT-Ökosystems" und Verwaltung der Fähigkeiten der Mitarbeiter und der Organisationskultur. Die Konzentration auf diese Gebiete behebt nicht die Risiken, aber verbessert wesentlich die Sicherheit, von der oft das Fortbestehen der Organisation abhängt.

Schlüsselwörter: das digitale Zeitalter, Sicherheit, Cyberkriminalität, Sicherheitsmanagement, Datenschutz

Управление безопасностью в эре цифровых технологий
Резюме

Цифровая или информационная эра, благодаря ускорению обмену информацией и изменениям форм документооборота, создала новые возможности доступа к предприятиям и государственным учреждениям. Сегодня, не стеклянная

входная дверь, а интернет соединения, дают доступ к организации. Сотрудников службы охраны заместили компьютерные системы информационной безопасности, антивирусные программы и файрволы. Оптическими волокнами можно проникнуть гораздо дальше, проникнуть в структуры организации глубже и нанести ущерб, во много раз превышающий тот, который могли причинить «классические» преступники.

Существует так много угроз, что невозможно их всех перечислить. Ежедневно возникают их новые формы, ранее неизвестные способы хищения информации и денег. Изначально, создавались правила и инструкции, с которыми должны были ознакомиться сотрудники. Эти правила касались защиты файлов, конфиденциальных файлов, способов создания паролей доступа, обработки информации. Однако, за относительно короткий промежуток времени выяснилось, что защита от киберпреступности требует системного подхода. Появилась концепция управления безопасностью в эру цифровых технологий – эта проблема была систематизирована и сосредоточивается на четко выделенных областях. Концепция охватывает следующие области и процессы: управление данными, управление информационными потоками, автоматизация принятия решений, управление инфраструктурой, использование интеллектуальных интерфейсов, управление внешней информационной «экосистемой», управление навыками сотрудников и организационной культурой. Безусловно, концентрация внимания на вышеуказанных областях не устранит угрозы, но значительно повысит безопасность, от которой часто зависит дальнейшее существование организации, предприятия, учреждения.

Ключевые слова: цифровая (информационная) эра, безопасность, киберпреступность, управление безопасностью, защита данных

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-008

Piotr Komsta
dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0002-0162-5518

Koncepcja modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych a bezpieczeństwo procesów biznesowych przy realizacji projektów IT

Wprowadzenie

Celem artykułu jest zaprezentowanie koncepcji modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych jako narzędzia wspomagającego proces utrzymania i poprawy bezpieczeństwa procesów biznesowych w kontekście wdrożenia systemu informatycznego wspomagającego zarządzanie. Powyższe zagadnienie przedstawiono na przykładzie budowy specyfikacji wymagań funkcjonalnych systemu. Prace związane z budową specyfikacji wymagań funkcjonalnych systemu były prowadzone na jednej z uczelni wyższych w Polsce w 2018 r. i dotyczyły wdrożenia systemu informatycznego wspomagającego pracę uczelni w obszarze naukowo-dydaktycznym.

W artykule przyjęto następującą tezę: wykorzystanie koncepcji modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych do budowy specyfikacji wymagań funkcjonalnych systemu informatycznego stanowi narzędzie wspierające utrzymanie i poprawę poziomu bezpieczeństwa procesów biznesowych w organizacji.

Wdrażanie systemów informatycznych jest trudnym przedsięwzięciem. Wiele projektów informatycznych nie kończy się w założonym czasie i założonym budżecie, a wdrożenia systemów w wielu przypadkach nie przynoszą spodziewanych efektów. W celu szerszego zapoznania się problematyką sprawności realizowanych projektów informatycznych Autor odsyła do wyników badań zawartych w raportach Standish Group[1]. Niepowodzenie projektu informatycznego może skutkować dużymi stratami finansowymi łącznie z zagrożeniem bezpieczeństwa finansowego firmy[2]. Jako jedną z głównych przyczyn niepowodzeń projektów informatycznych wspomagających zarządzanie należy wskazać nieadekwatność procedur wdrożenia systemu w stosunku do uwarunkowań implementacyjnych, jak również niską jakość prac w obszarach okołoprojektowych, w tym – niewłaściwe przygotowanie przedsiębiorstw do wdrożenia systemu informatycznego. Budowa specyfikacji wymagań funkcjonalnych wdrażanych rozwiązań informatycznych wymaga z jednej strony uwzględnienia potrzeb wynikających z zapewnienia ciągłości realizowanych procesów, a z drugiej – spojrzenia projakościowego i doboru narzędzi umożliwiających dynamiczny rozwój firmy w dłuższej perspektywie czasowej.

Bezpieczeństwo procesów biznesowych a realizacja projektu informatycznego

Realizacja projektów informatycznych obarczona jest bardzo dużym ryzykiem. Niepowodzenie może w tym przypadku skutkować nie tylko brakiem efektów wdrożenia systemu (brakiem poprawy sprawności funkcjonowania firmy) – niedopasowanie systemu do wymagań procesowych może zagrozić ciągłości ich realizacji, co wiąże się zazwyczaj z dużymi stratami finansowymi. Dlatego przy realizacji projektów informatycznych aspekt bezpieczeństwa procesów biznesowych powinien być szczególnie istotny. Dbałość o bezpieczeństwo procesów biznesowych w kontekście realizacji projektu informatycznego rozpoczyna się już w momencie konstruowania wymagań odnośnie do funkcjonowania przyszłych rozwiązań informatycznych w firmie, czyli na samym początku prac związanych z ich wyborem. Świadectwem tej dbałości w przedmiotowym zakresie jest dokładne rozpoznanie obszarów będących przedmiotem implementacji systemu informatycznego, w tym umiejętność powiązania wymagań funkcjonalnych systemu z reżimem proceduralnym, wskazania procedur, a co za tym idzie – funkcjonalności rozwiązania informatycznego, które są krytyczne z punktu widzenia realizowanych przez firmę zadań. Dbałość o bezpieczeństwo procesów biznesowych to również dążenie do poprawy sprawności realizowanych procedur przy wykorzystaniu nowych rozwiązań informatycznych. Oczywiście ryzyka związane z realizacją projektu informatycznego nie można do końca wyeliminować, ale można je w znacznym stopniu

[1] *Sample Research*, The Standish Group, https://www.standishgroup.com/sample_research [dostęp: 27.05.2019].

[2] S. Jituri, B. Fleck, R. Ahmad, *A Methodology to Satisfy Key Performance Indicators for Successful ERP Implementation in Small and Medium Enterprises*, „International Journal of Innovation, Management and Technology" 2018, vol. 9, nr 2, s. 79.

ograniczyć poprzez dobór odpowiednich narzędzi. Narzędzia te powinny stanowić solidny fundament, na którym w zmieniających się uwarunkowaniach działalności przedsiębiorstwa możliwe będzie permanentne budowanie jakości w wymiarze proceduralno-technologicznym.

Koncepcja modelowania dynamicznego

Koncepcja modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych opiera się na badaniu istotności i adekwatności procedur wdrożenia systemu informatycznego w stosunku do uwarunkowań implementacyjnych. Efektem tych badań jest stworzenie optymalnej ścieżki implementacji systemu informatycznego – dopasowanej do uwarunkowań realizowanych prac w określonym środowisku projektowym[3]. Koncepcja modelowania dynamicznego ma również zastosowanie w obszarach okołoprojektowych, w tym w analizie przedwdrożeniowej i dotyczy procedur podlegających procesom implementacyjnym. Jak już wspomniano, obszarem mającym szczególny wpływ na jakość realizowanych projektów informatycznych jest obszar działań okołoprojektowych, w tym – jakość analizy przedwdrożeniowej. Kluczowym efektem przeprowadzenia analizy przedwdrożeniowej jest specyfikacja wymagań funkcjonalnych systemu, niezbędna do oceny dopasowania oferowanych rozwiązań informatycznych do potrzeb informacyjnych przedsiębiorstwa – zarówno bieżących, jak i przyszłych.

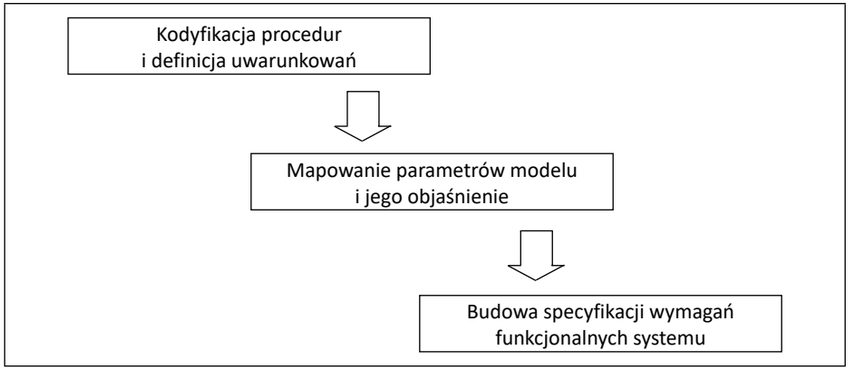
Specyfikacja wymagań funkcjonalnych powinna być skonstruowana tak, by umożliwiać prowadzenie w przyszłości działań optymalizujących funkcjonowanie firmy w dynamicznie zmieniającym się środowisku biznesowym (determinując tym samym zwrot z inwestycji w zakup systemu informatycznego) oraz zapewniać bezpieczeństwo realizowanych procesów biznesowych. Proces budowy specyfikacji wymagań funkcjonalnych systemu zgodnie z koncepcją modelowania dynamicznego został przedstawiony na rysunku 1. Przebiega wg trzech zasadniczych kroków: 1) kodyfikacja procedur i definicja uwarunkowań, 2) mapowane parametrów modelu

[3] Szerzej zob. P. Komsta, *Uwarunkowania i obszary modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych*, [w:] *IT w organizacjach gospodarczych. Wybrane zagadnienia*, red. L. Kiełtyka, R. Kucęba, W. Jędrzejczyk, Toruń 2010, s. 39–45; idem, *Kształtowanie procedur implementacyjnych systemów zintegrowanych w koncepcji modelowania dynamicznego*, [w:] *Narzędzia informatyczne w gospodarce elektronicznej i systemach wspomagania decyzji. Wybrane zagadnienia*, red. L. Kiełtyka, Częstochowa 2011, s. 88–93; idem, *Mapowanie i analiza parametrów w dynamicznym modelu implementacji systemów zintegrowanych*, [w:] *Wykorzystanie wybranych technologii komunikacji w zarządzaniu wartością organizacji*, red. L. Kiełtyka, Częstochowa 2012, s. 277–282; idem, *Punkty węzłowe w modelowaniu dynamicznym procesów implementacyjnych systemów zintegrowanych*, [w:] *Technologie informacyjne w funkcjonowaniu organizacji: Zarządzanie z wykorzystaniem multimediów*, red. L. Kiełtyka, Toruń 2013, s. 521–528; idem, *Czynniki sprawności modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych*, [w:] *Wybrane zastosowania technologii informacyjnych wspomagających zarządzanie w organizacjach*, red. L. Kiełtyka, R. Niedbał, Częstochowa 2015, s. 42–50; idem, *Cele modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych*, [w:] *Innowacje i przedsiębiorczość. Ujęcie makro- i mikroekonomiczne*, red. A. Francik, V. Maráková, K. Szczepańska-Woszczyna, Dąbrowa Górnicza 2016, s. 189–196.

oraz jego objaśnienie, 3) budowa specyfikacji wymagań funkcjonalnych systemu w oparciu o zbudowany model.

W procesie modelowania wyodrębniono następujące punkty węzłowe realizowanych prac: rozpoznanie obszarów analizy, kodyfikację procedur, rozpoznanie centrów odpowiedzialności, definicję uwarunkowań, analizę istotności i adekwatności procedur, budowę modelu referencyjnego funkcjonowania Uczelni w przedmiotowym zakresie oraz budowę specyfikacji wymagań funkcjonalnych systemu w oparciu o zbudowany model.

Rysunek 1. Proces budowy specyfikacji wymagań funkcjonalnych systemu przy wykorzystaniu koncepcji modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych



Źródło: opracowanie własne.

Kodyfikacja procedur i definicja uwarunkowań

Budowa specyfikacji wymagań funkcjonalnych systemu w oparciu o koncepcję modelowania dynamicznego wymaga przeprowadzenia procesu kodyfikacji procedur. Kodyfikacja procedur jest niezbędnym elementem implikującym działania optymalizujące funkcjonalności wdrażanego systemu informatycznego, a co za tym idzie – funkcjonowanie firmy. Kodyfikacja procedur ma szczególne znaczenie z perspektywy budowy bazy wiedzy, która w wielu firmach ma charakter rozproszony, mało udokumentowany oraz wymagający aktualizacji. Jej efektem ma być nie tylko inwentaryzacja procedur i procesów realizowanych w firmie – kodyfikacja procedur ma wywołać u pracowników refleksję w zakresie realizowanych czynności i zachęcić do zgłaszania propozycji ich usprawnienia. Zakres danych do kodyfikacji powinien uwzględniać nie tylko aspekt procedur i centrów odpowiedzialności oraz propozycje zmian i usprawnień, ale również aspekt uwarunkowań realizacyjnych – w tym przypadku jest on bardzo istotny, bo właśnie zmienność uwarunkowań realizacyjnych determinuje dokonywanie zmian prosprawnościowych zarówno w aspekcie organizacyjnym, jak technologicznym. W wyniku przeprowadzonej analizy wyodrębniono jednostki organizacyjne biorące udział w procesach oraz centra odpowiedzialności (stanowiska i funkcje w procesie). Dokonano kodyfikacji prac (czynności)

wykonywanych w ramach realizowanych procedur, przeprowadzono analizę częstotliwości wykonywanych procedur, wskazano problemy i propozycje zmian pod kątem organizacyjnym, dokonano również szacowania poziomu pracochłonności realizowanych procedur. Do uwarunkowań realizacyjnych zaliczono obowiązujące uregulowania prawne (ustawy i rozporządzenia oraz przepisy wewnętrzne) determinujące funkcjonowanie Uczelni w obszarze naukowo-dydaktycznym i wynikające z nich zadania ewidencyjno-sprawozdawcze[4]. Do głównych zadań w przedmiotowym zakresie zaliczono: ocenę procesu dydaktycznego wykładowcy, ocenę okresową pracownika naukowego, ocenę przez absolwentów i interesariuszy programu studiów, kodyfikację i zasilanie bazy PBN publikacjami pracowników, rejestrację oświadczeń pracowników o zaliczeniu do liczby N, pozyskanie i rozliczenie środków na utrzymanie potencjału badawczego, dofinansowanie działalności naukowej z środków własnych i ich rozliczenie, przygotowanie projektów NCN i rozliczenie z ich realizacji, organizację i rozliczenie wyjazdów w ramach programu Erasmus+, organizację i rozliczenie konferencji naukowych, przygotowanie publikacji pokonferencyjnych.

Mapowanie parametrów modelu

Mapowanie parametrów modelu polegało na wskazaniu istotności i adekwatności procedur ze względu na uwarunkowania realizacyjne. Analiza istotności miała wykazać, które procedury są krytyczne z punktu widzenia realizacji poszczególnych zadań i realizacja których zadań angażuje najwięcej środków w postaci obciążenia procedurami oraz obciążenia jednostek organizacyjnych zaangażowanych w ich realizację. Analiza adekwatności miała wykazać stopień dopasowania stosowanych procedur pod kątem organizacyjnym i sprawnościowym.

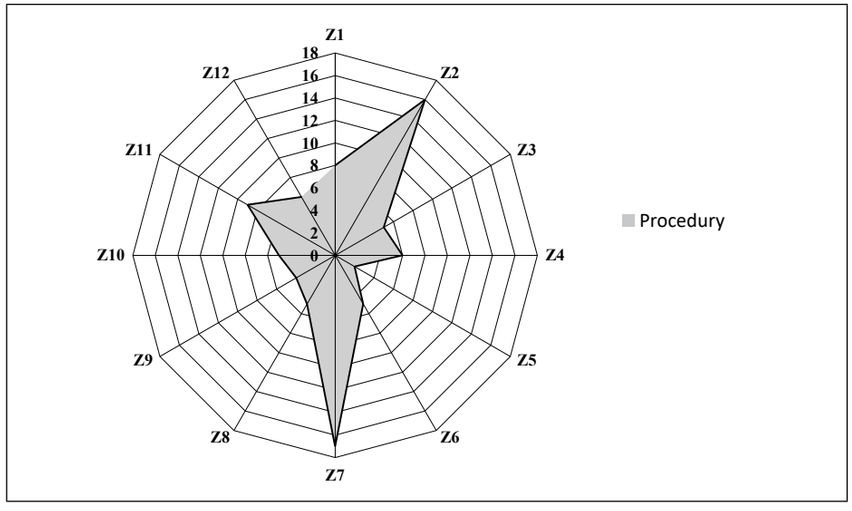
Analiza istotności wykazała nierównomierność w zakresie obciążenia proceduralnego realizowanych zadań. Największe obciążenie procedurami dotyczyło zadań Z7, Z2, Z11 oraz Z1, dotyczących odpowiednio pozyskiwania i rozliczenia środków na utrzymanie potencjału badawczego (17 procedur), oceny okresowej pracownika naukowego (16 procedur), prac związanych z organizacją i rozliczeniem konferencji (9 procedur) oraz prac związanych z ewaluacją zajęć dydaktycznych (8 procedur). Dane dotyczące obciążenia proceduralnego zadań przedstawiono na wykresie 1.

Analiza istotności wykazała, że zadania Z2 i Z1 dotyczące odpowiednio oceny okresowej pracownika naukowego oraz oceny procesu dydaktycznego wykładowcy, angażowały największą liczbę jednostek organizacyjnych (Z2 – 8 jednostek organizacyjnych, Z1 – 5 jednostek organizacyjnych)[5]. Dane dotyczące obciążenia jednostek organizacyjnych zaangażowanych w realizację poszczególnych zadań zostały przedstawione na wykresie 2.

[4] W czasie przeprowadzania analiz Uczelnia funkcjonowała w ramach poprzedniego stanu prawnego (Ustawa z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym, Dz.U. z 2005 r., nr 164, poz. 1365), przed wejściem w życie obowiązującej obecnie Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, Dz.U. z 2018 r., poz. 1668.

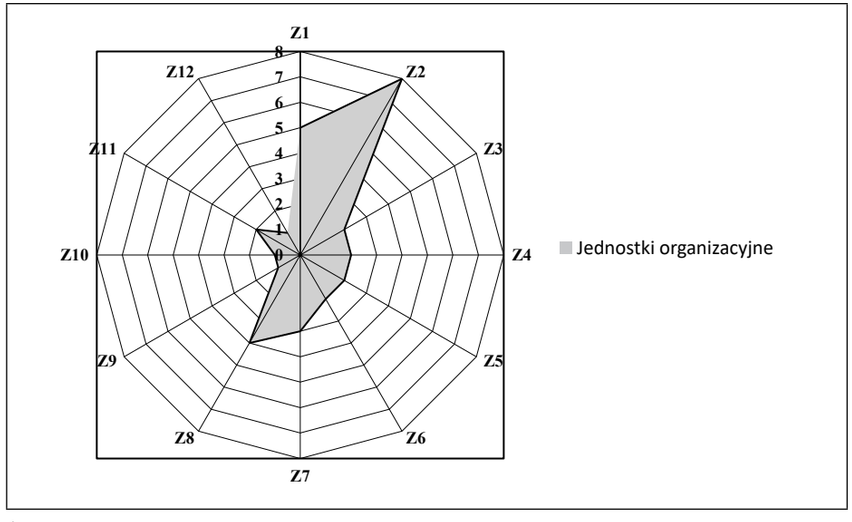
[5] Dotyczy zarówno struktur działających w ramach wydziału, jak i ogólnouczelnianych (np. specjalnie powołane Komisje).

Wykres 1. Rozkład obciążenia proceduralnego zadań



Źródło: opracowanie własne.

Wykres 2. Obciążenie jednostek organizacyjnych zaangażowanych w realizację poszczególnych zadań



Źródło: opracowanie własne.

Drugim istotnym elementem procesu mapowania parametrów modelu była analiza adekwatności. Miała na celu wykazać, jaki jest stopień dopasowania procedur pod kątem organizacyjnym oraz sprawnościowym. Przy ocenie adekwatności

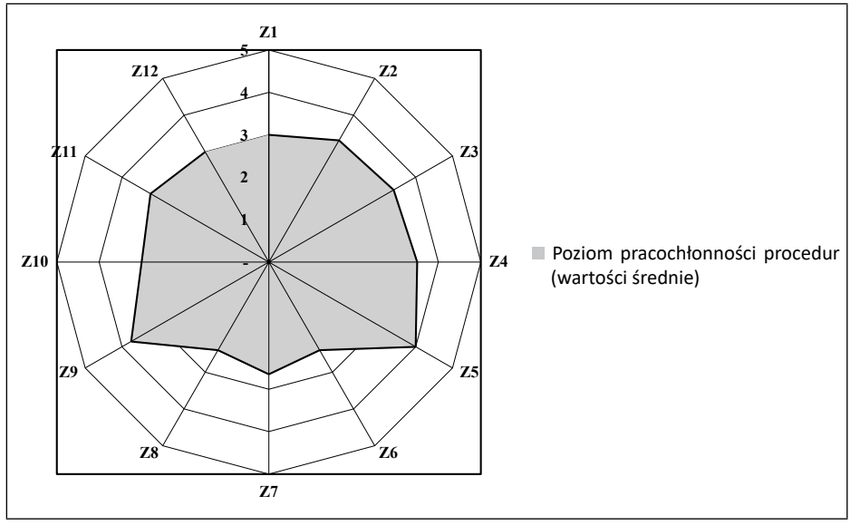
procedur pod kątem organizacyjnym dokonano analizy częstotliwości realizowanych zadań w odniesieniu do wartości referencyjnych (jeśli takie zostały określone przepisami) wynikających z zewnętrznych uregulowań prawnych lub przepisów wewnętrznych oraz oceny liczby zgłoszonych przez pracowników zmian dotyczących usprawnień realizowanych procedur.

Analiza odchyleń częstotliwości wykonywanych procedur od wartości referencyjnych pozwoliła stwierdzić, że Uczelnia realizowała zadania zgodnie z przepisami, a nawet – w przypadku procedur związanych z ewaluacją zajęć dydaktycznych oraz oceną pracownika naukowego – procedury wykonywane były częściej, niż wynikało to z wartości referencyjnych.

Z analizy liczby procedur zgłoszonych jako wymagające przeprowadzenia usprawnień i zmian w zakresie realizowanych czynności wynika, że realizacja każdego z zadań zawierała procedury, które powinny ulec modyfikacjom.

Ocena poziomu pracochłonności realizowanych procedur została wykonana przez pracowników w trakcie ich kodyfikacji. Przyjęto skalę oceny od 1 do 5, gdzie 1 oznaczało procedurę o bardzo niskiej pracochłonności, a 5 – procedurę o bardzo wysokiej pracochłonności. Z analizy oceny poziomu pracochłonności wykonywanych prac wynika, że rozkład pracochłonności związanej z realizacją poszczególnych zadań nie był równomierny. Większość realizowanych zadań związana była w ocenie pracowników ze średnim i dużym nakładem pracy. Największą pracochłonna była realizacja zadań Z5 i Z9, dotyczących odpowiednio kodyfikacji danych i zasilania bazy PBN publikacjami pracowników oraz przygotowania i rozliczenia projektów NCN. Graficzna prezentacja wyników została przedstawiona na wykresie 3.

Wykres 3. Ocena pracochłonności procedur związanych z realizacją poszczególnych zadań



Źródło: opracowanie własne.

Budowa specyfikacji wymagań funkcjonalnych systemu

Jasno sprecyzowane cele wdrożenia systemu informatycznego są bardzo istotne z punktu widzenia powodzenia projektu informatycznego[6]. Specyfikacja wymagań funkcjonalnych systemu informatycznego jest mapą drogową jego dalszego rozwoju i fundamentem oceny dopasowania nowego rozwiązania do potrzeb przedsiębiorstwa. Stanowi punkt odniesienia łączący potrzeby informacyjne przedsiębiorstwa z rozwiązaniami oferowanymi przez dostawców oprogramowania. Proces budowy specyfikacji wymagań funkcjonalnych systemu informatycznego powinien opierać się na dogłębnej analizie potrzeb przedsiębiorstwa – zarówno pod względem zapewnienia ciągłości realizowanych procesów, jak i możliwych zmian pozwalających na poprawę ich funkcjonowania. Wdrożenie systemu informatycznego powinno przynosić nową jakość – będącą efektem zmian, które muszą być zrozumiałe i zaakceptowane przez pracowników przedsiębiorstwa[7]. Fundamentem budowy specyfikacji wymagań funkcjonalnych systemu jest analiza przedwdrożeniowa, która pozwala na identyfikację obszarów funkcjonalnych systemu oraz zmian, jakich należy dokonać, aby poprawić sprawność funkcjonowania firmy, a co za tym idzie – zapewnić zwrot kosztów z inwestycji i bezpieczeństwo procesów. Niewłaściwie przeprowadzona analiza przedwdrożeniowa może skutkować tym, że zasadnicze cele wdrożenia systemu nie zostaną osiągnięte[8]. Specyfikacja wymagań funkcjonalnych systemu informatycznego nie jest jedynym narzędziem służącym do oceny dopasowania systemu do potrzeb przedsiębiorstwa, lecz jest niewątpliwie narzędziem podstawowym, stanowiącym punkt wyjścia do procesu oceny prezentowanych rozwiązań informatycznych.

Budowa specyfikacji wymagań funkcjonalnych systemu wymaga nie tylko znajomości funkcjonowania procedur w przedsiębiorstwie, ale również wiedzy na temat wykorzystania współczesnych technologii informatycznych. Specyfikacja nie może być zbyt szczegółowa – nie powinna określać sposobu rozwiązania danego problemu, a jedynie definiować problem dziedzinowy w przedmiotowym zakresie. Taka budowa specyfikacji wymagań funkcjonalnych daje możliwość oferowania przez firmy informatyczne szerokiego spektrum rozwiązań danego problemu. Specyfikacja powinna mieć charakter dynamiczny – powinna być uszczegóławiana w trakcie procesu negocjacyjnego. W przedmiotowym przypadku specyfikacja wymagań funkcjonalnych systemu została stworzona w oparciu o wcześniej zbudowany wielowymiarowy model funkcjonowania Uczelni, uwzględniający przeprowadzone wcześniej analizy istotności i adekwatności, w tym propozycje zmian w funkcjonowaniu procedur odpowiedzialnych za realizacje poszczególnych zadań. Do budowy specyfikacji wymagań systemu informatycznego wykorzystano matrycę powiązań wymaganych funkcjonalności systemu z realizacją konkretnych procedur zdefiniowanych w procesie mapowania modelu. Matryca powiązań stanowiła

[6] Y. Lee, J. Do, Y. Choe, *Study on Factors for Improving the Effectiveness of ERP within Korea Agricultural Products Processing Center*, „Journal of Research in Business and Management" 2017, vol. 5, nr 2, s. 91.

[7] Ch.A. Rajan, R. Baral, *Adoption of ERP System: An Empirical Study of Factors Influencing the Usage of ERP and its Impact on End User*, „IIMB Management Review" 2015, vol. 27, nr 2, s. 107.

[8] M. Moś, *Analiza przedwdrożeniowa a realizacja projektów IT*, „Zarządzanie i Finanse" 2012, nr 1, cz. 1, s. 399–400.

szkielet pozwalający określić, które wymagania funkcjonalne systemu są krytyczne z punktu widzenia sprawności realizowanych przez Uczelnię zadań, czyli na które funkcjonalności trzeba zwrócić szczególną uwagę w procesie negocjacyjnym z dostawcą oprogramowania.

Do parametrów modelu zaliczono: zadania Uczelni wynikające z obowiązujących uregulowań prawnych (ustaw, rozporządzeń oraz przepisów wewnętrznych), procedury związane z realizacją powyższych zadań, komórki organizacyjne, centra odpowiedzialności oraz obszary dziedzinowe będące przedmiotem analizy przedwdrożeniowej systemu. Jako zmienne modelu przyjęto: poziom pracochłonności realizacji poszczególnych procedur, częstotliwość realizowanych procedur i ich wartości referencyjne oraz poziom adekwatności procedur w zakresie rekomendacji dokonania zmian w celu ich usprawnienia.

Podsumowanie

Dbałość o bezpieczeństwo procesów biznesowych w kontekście wdrożeń systemów informatycznych nabiera szczególnego znaczenia. Niewłaściwe dopasowanie systemu informatycznego do realizowanych procesów w firmie może zagrozić brakiem zachowania ich ciągłości i sprawności, i tym samym narazić firmę na poważne konsekwencje. Zastosowanie koncepcji modelowania dynamicznego do budowy specyfikacji wymagań funkcjonalnych systemu pozwoliło nie tylko określić wymagania funkcjonalne systemu informatycznego, które pozwolą na zachowanie ciągłości realizacji procesów oraz poprawią ich sprawność, ale również zbudować solidne fundamenty do dalszych działań optymalizujących funkcjonowanie Uczelni w wymiarze procesowym uwzględniającym dynamikę zmieniających się uwarunkowań (np. przepisów wynikających z nowej ustawy o szkolnictwie wyższym). Przeprowadzona analiza istotności pozwoliła określić, które procedury są krytyczne z punktu widzenia realizowanych przez Uczelnię zadań, określić poziom obciążenia proceduralnego tychże zadań oraz wskazać centra odpowiedzialności za ich realizację. Analiza adekwatności pozwoliła ustalić, które zadania realizowane przez Uczelnię wymagają dużych, a które mniejszych nakładów pracy, wskazać na tej podstawie priorytetowe działania optymalizujące, a także określić poziom dopasowania częstotliwości wykonywanych procedur do wartości referencyjnych wynikających z obowiązujących wymogów sprawozdawczych. Przeprowadzona analiza adekwatności pozwoliła zbudować bazę wiedzy na temat problemów wynikających z realizowanych procedur i propozycji ich rozwiązania przy wykorzystaniu nowych narzędzi informatycznych. Zbudowany w ten sposób model funkcjonowania Uczelni pozwolił na dokonywanie analiz o charakterze wielowymiarowym i stał się narzędziem monitorowania funkcjonowania Uczelni w aspekcie sprawnościowym – umożliwiał elastyczne dopasowywanie procedur do zmieniających się uwarunkowań ich funkcjonowania, a także późniejszy pomiar efektów wdrożenia systemu informatycznego. W związku z powyższym należy stwierdzić, że zastosowanie koncepcji modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych w procesie budowy wymagań funkcjonalnych systemu informatycznego stanowi narzędzie wspierające utrzymanie i poprawę poziomu bezpieczeństwa procesów biznesowych w organizacji.

Bibliografia

Jituri S., Fleck B., Ahmad R., *A Methodology to Satisfy Key Performance Indicators for Successful ERP Implementation in Small and Medium Enterprises*, „International Journal of Innovation, Management and Technology" 2018, vol. 9, nr 2, s. 79.

Komsta P., *Uwarunkowania i obszary modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych*, [w:] *IT w organizacjach gospodarczych. Wybrane zagadnienia*, red. L. Kiełtyka, R. Kucęba, W. Jędrzejczyk, Toruń 2010.

Komsta P., *Kształtowanie procedur implementacyjnych systemów zintegrowanych w koncepcji modelowania dynamicznego*, [w:] *Narzędzia informatyczne w gospodarce elektronicznej i systemach wspomagania decyzji. Wybrane zagadnienia*, red. L. Kiełtyka, Częstochowa 2011.

Komsta P., *Mapowanie i analiza parametrów w dynamicznym modelu implementacji systemów zintegrowanych*, [w:] *Wykorzystanie wybranych technologii komunikacji w zarządzaniu wartością organizacji*, red. L. Kiełtyka, Częstochowa 2012.

Komsta P., *Punkty węzłowe w modelowaniu dynamicznym procesów implementacyjnych systemów zintegrowanych*, [w:] *Technologie informacyjne w funkcjonowaniu organizacji: Zarządzanie z wykorzystaniem multimediów*, red. L. Kiełtyka, Toruń 2013.

Komsta P., *Czynniki sprawności modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych*, [w:] *Wybrane zastosowania technologii informacyjnych wspomagających zarządzanie w organizacjach*, red. L. Kiełtyka, R. Niedbał, Częstochowa 2015.

Komsta P., *Cele modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych*, [w:] *Innowacje i przedsiębiorczość. Ujęcie makro- i mikroekonomiczne*, red. A. Francik, V. Maráková, K. Szczepańska-Woszczyna, Dąbrowa Górnicza 2016.

Lee Y., Do J., Choe Y., *Study on Factors for Improving The Effectiveness of ERP within Korea Agricultural Products Processing Center*, „Journal of Research in Business and Management" 2017, vol. 5, nr 2.

Moś M., *Analiza przedwdrożeniowa a realizacja projektów IT*, „Zarządzanie i Finanse" 2012, nr 1, cz. 1.

Rajan Ch.A., Baral R., *Adoption of ERP System: An Empirical Study of Factors Influencing the Usage of ERP and its Impact on End User*, „IIMB Management Review" 2015, vol. 27, nr 2.

Sample Research, The Standish Group, https://www.standishgroup.com/sample_research [dostęp: 27.05.2019].

Koncepcja modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych a bezpieczeństwo procesów biznesowych przy realizacji projektów IT

Streszczenie

Artykuł jest efektem doświadczeń Autora w zakresie zastosowania koncepcji modelowania dynamicznego procesów implementacyjnych systemów zintegrowanych w procesie budowy specyfikacji wymagań funkcjonalnych systemu informatycznego. W artykule przedstawiono zagadnienie bezpieczeństwa procesów biznesowych w kontekście realizacji projektu informatycznego, istotę koncepcji modelowania dynamicznego oraz punkty węzłowe realizowanego zadania, w tym: kodyfikację procedur i definicję uwarunkowań, mapowanie parametrów modelu oraz budowę specyfikacji wymagań funkcjonalnych systemu w oparciu o zbudowany model. Zaprezentowano również wyniki analiz istotności i adekwatności procedur będących przedmiotem implementacji systemu informatycznego.

Słowa kluczowe: projekt informatyczny, bezpieczeństwo procesów biznesowych, system informatyczny wspomagający zarządzanie, wdrażanie systemów informatycznych

The Concept of Dynamic Modeling of Implementation Processes of Integrated Systems and the Safety of Business Processes in Connection with the Implementation of the IT Project

Abstract

The article is the result of the author's experience in the application of the concept of dynamic modeling of implementation processes of integrated systems in the process of building the specification of functional requirements of the IT system. The article presents the issues of business processes safety in the context of the implementation of an IT project, presents the essence of the concept of dynamic modeling and the milestones of the implemented task, including the codification of procedures, the definition of conditions, mapping of model parameters and the construction of the system's functional requirements specification based on the model. The article presents the results of significance and adequacy analysis of procedures being the subject of IT system implementation.

Key words: IT project, business process safety, IT management solutions, implementations of IT management solutions

Das Konzept zur dynamischen Modellierung der Umsetzungsprozesse der integrierten Systeme und die Sicherheit der Geschäftsprozesse bei der Ausführung von IT-Projekten

Zusammenfassung

Der Artikel entstand aufgrund der Erfahrungen des Autors im Bereich der Anwendung des Konzepts zur dynamischen Modellierung der Umsetzungsprozesse der integrierten Systeme im Prozess des Aufbaus der Spezifikation der funktionellen Anforderungen eines IT-Systems. Im Artikel wurde das Problem der Sicherheit der Geschäftsprozesse im Zusammenhang mit der Ausführung eines IT-Projekts, das Wesen des Konzepts zur dynamischen Modellierung und Knotenpunkte der ausgeführten Aufgabe, darin: Kodifizierung der Verfahren und Definition der Bedingungen (Determinanten), Mapping von Parametern eines Models und Aufbau der Spezifikation von funktionellen Systemanforderungen auf der Grundlage des erstellten Modells dargestellt. Im Artikel wurden Ergebnisse der Bedeutung und der Angemessenheit der Verfahren dargestellt, die Gegenstand der Implementierung des IT-Systems sind.

Schlüsselwörter: IT-Projekt, Sicherheit der Geschäftsprozesse, ein das Management förderndes IT-System, Umsetzung der IT-Prozesse

Piotr Komsta

Концепция динамического моделирования процессов имплементации интегрированных систем и проблема безопасности бизнес-процессов при реализации ИТ-проектов

Резюме

Статья базируется на опыте автора в области применения концепции динамического моделирования процессов имплементации интегрированных систем в процессе создания спецификаций функциональных требований к информационной системе. В статье рассмотрены вопросы безопасности бизнес-процессов в контексте реализации ИТ-проекта, суть концепции динамического моделирования и узловых точек реализованного задания, в том числе: упорядочивание процедур и определение условий, мапирование параметров модели и создание спецификации функциональных требований к ИС на основе созданной модели. Были также представлены результаты анализа значимости и адекватности процедур, которые являются предметом имплементации информационной системы.

Ключевые слова: ИТ-проект, безопасность бизнес-процессов, информационная система, поддерживающая управление, внедрение информационных систем

Z kart historii
From the History
Aus der Geschichte
Страницы истории

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-009

Janusz Wojtycza

dr hab., prof. KA, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0002-5872-8403

Krakowska Chorągiew Męska ZHP. Powstanie i początki działalności (1920–1921). Kalendarium wydarzeń

Wprowadzenie

Związek Harcerstwa Polskiego (ZHP), wywodzący się ze skautingu, był zawsze mocno związany z wojskiem i przysposobieniem wojskowym. W 2020 r. przypada setna rocznica powołania do życia krakowskich chorągwi męskiej i żeńskiej. Chorągwie powstały w wyniku ostatecznego połączenia w jednolity ZHP dawnych dzielnicowych organizacji harcerskich, co miało miejsce na I Walnym Zjeździe w Warszawie w dniach 31 grudnia 1920 – 2 stycznia 1921 r.[1].

Historia harcerstwa krakowskiego – jednego ze środowisk przodujących w całej historii organizacji – nie doczekała się jak dotychczas zadowalającej syntezy naukowej. Poszczególne okresy do roku 1950 zostały już w pewnej mierze opisane[2], wydano także materiały źródłowe[3]. Późniejszy okres został opracowany w znacznej części na poziomie hufców miasta Krakowa, wydano także wspomnienia

1 W. Błażejewski, *Z dziejów harcerstwa polskiego (1910–1939)*, Warszawa 1985, s. 158.

2 W. Hausner, *Krakowski skauting 1910–1914*, Kraków 1994; J. Wojtycza, *Skauting polski w Galicji i na Śląsku Cieszyńskim w latach 1910–1919*, Kraków 2000; P. Miłobędzki, *Harcerze w okupowanym Krakowie*, Kraków 2005; *Konspiracja harcerska w Krakowie 1939–1945*, red. J. Wojtycza, Kraków 2019; B. Rzońca, *Krakowska Chorągiew Harcerzy w latach 1945–1950*, Kraków 2015.

3 *Rozkazy i okólniki Krakowskiej Chorągwi Męskiej/Harcerzy z lat 1920–1939*, zebr. i opr. J. Wojtycza, Kraków 2017 [płyta CD]; *Rozkazy Krakowskiej Chorągwi Harcerzy/Chorągwi ZHP w Krakowie z lat 1945–1950*, zebr. i opr. J. Wojtycza, Kraków 2018 [płyta CD].

komendantów chorągwi i materiały źródłowe[4]. Okres międzywojenny przebadano jedynie w odniesieniu do harcerstwa żeńskiego[5]. Dokonała tego na początku lat 80. ubiegłego wieku dr Maria Irena Mileska[6], a jej obszerne opracowanie zostało wydane drukiem w latach 2003–2004[7]. Warto wspomnieć, że podobne opracowanie w odniesieniu do chorągwi lwowskich przygotowała dr Irena Kozimala[8]. Szereg ważnych informacji dotyczących działalności krakowskiego harcerstwa znajdujemy w ogólnych opracowaniach i edycjach źródeł do dziejów harcerstwa w Polsce, lecz nie są one w żadnym stopniu wystarczające[9].

Prezentowany w niniejszym artykule opis powstania lokalnych struktur ogólnopolskiego ZHP jest wynikiem podjętych przez autora badań nad męskim harcerstwem krakowskim okresu międzywojennego. Podstawą badań są źródła archiwalne znajdujące się w Archiwum Akt Nowych w Warszawie w zespole „Archiwum Związku Harcerstwa Polskiego", obejmującym lata 1913–1939, oraz zachowane źródła drukowane, jak sprawozdania Zarządu Oddziału i komendy chorągwi, rozkazy komendy chorągwi[10] oraz w mniejszym stopniu sprawozdania Naczelnej Rady Harcerskiej i publikacje na łamach prasy harcerskiej.

Artykuł przedstawia powstanie Krakowskiej Chorągwi Męskiej ZHP i jej działalność do końca 1921 r. Jest pierwszym opracowaniem tego tematu z wykorzystaniem dotychczas niepublikowanych źródeł archiwalnych. Opis nie uwzględnia w szerszym zakresie tła oraz uwarunkowań funkcjonowania chorągwi – ogranicza się do jej rozwoju organizacyjnego. Zestawienie najważniejszych wydarzeń opatrzono licznymi cytatami, w których zachowano oryginalną pisownię i interpunkcję.

4 K. Wojtycza, *Hufiec Kraków Kleparz-Łobzów w latach 1957–1972*, Kraków 2007; idem, *Hufiec Kraków-Krowodrza w latach 1973–1989*, Kraków 2014; J. Wojtycza, *Hufiec Kraków-Nowa Huta w latach 1957–1989*, Kraków 2017; K. Wojtycza, *Hufiec Kraków-Śródmieście w latach 1973–1989*, Kraków 2018; idem, *Hufiec Kraków-Zwierzyniec w latach 1957–1972*, Kraków 2011; *Komendanci Chorągwi Krakowskiej ZHP z lat 1956–1996 o swojej pracy*, red. J. Wojtycza, K. Wojtycza, Kraków 1999; *Rozkazy Krakowskiej Chorągwi ZHP z lat 1957–1975*, zebr. i opr. J. Wojtycza, Kraków 2019 [płyta CD].

5 Działalności harcerstwa męskiego w tym okresie dotyczy jedynie praca P. Grochowskiego *Hufiec Harcerzy Kraków-Podgórze w latach 1922–1939*, Kraków 2004.

6 Maria Irena Mileska z d. Książek, pseud. Jaga (1908–1988), geograf, dr nauk przyrodniczych, por. AK, harcmistrzyni, komendantka Krakowskiej Chorągwi Harcerek (1934–1935), kierowniczka Działu Łączności Pogotowia Harcerek (1941–1944), uczestniczka powstania warszawskiego, z rozkazu AK komendantka stalagu VI C Oberlangen.

7 M.I. Mileska, *Materiały do historii krakowskiego harcerstwa żeńskiego w latach 1911–1939*, t. 1, wstęp, opr. i red. J. Wojtycza, Kraków 2003; eadem, *Materiały do historii krakowskiego harcerstwa żeńskiego w latach 1911–1939*, t. 2, opr., uzup. i red. J. Wojtycza, Kraków 2004.

8 I. Kozimala, *Lwowska Chorągiew Harcerek ZHP w latach 1911–1939*, Przemyśl 2003; eadem, *Lwowska Chorągiew Harcerzy w latach 1921–1939*, Przemyśl 2007.

9 Z pozycji wydanych w ostatnich latach warto wskazać: W. Hausner, M. Wierzbicki, *Sto lat harcerstwa*, Warszawa 2015; G. Nowik, *Polskie związki skautowe i harcerskie 1909–1922*, Warszawa 2019; *Wybór źródeł do dziejów ZHP*, t. 1, *Utworzenie ogólnopolskiego Związku Harcerstwa Polskiego i czas próby ruchu harcerskiego (1918–1944)*, wyb. i opr. K. Marszałek, Kraków 2014.

10 Autor w trakcie wieloletnich badań odszukał 80% rozkazów komendy Krakowskiej Chorągwi Męskiej/Harcerzy z lat 1920–1939. Zebrane sprawozdania odnoszące się do tegoż okresu liczą łącznie 577 stron (zob. przypis 3).

Powstanie chorągwi i pierwszy rok działalności

W związku odkomenderowaniem dotychczasowego komendanta Okręgu Krakowskiego ppłk. Bronisława Piątkiewicza[11], skierowanego na czele ochotniczej kompanii[12] przez Dowództwo Okręgu Generalnego do służby granicznej na granicy Górnego Śląska, i złożeniem przez niego rezygnacji z funkcji, z dniem 30 września 1920 r. funkcję tę objął przodownik Tadeusz Biernakiewicz[13].

W listopadzie meldował on, że praca komendy dopiero się rozpoczęła i natrafiała na duże trudności. Była prowadzona rejestracja drużyn. Na terenie Krakowa działało jedno koło starszych harcerzy i harcerek (akademików). Koła Przyjaciół Harcerstwa nie istniały, jedynie w Rzeszowie funkcjonował Patronat Harcerski. Komendant przedstawił proponowany skład komendy oraz prosił o pomoc w pozyskaniu od władz miasta lub władz wojskowych lokali dla drużyn[14].

Uchwałą V Zjazdu Naczelnej Rady Harcerskiej, obradującego w dniach 30 października – 2 listopada 1920 r., w miejsce nazwy „komenda miejscowa" wprowadzono „nazwę komenda hufca". Podharcmistrzami mianowani zostali Tadeusz Biernakiewicz[15], Henryk Kapiszewski[16], Stefan Kuta[17] i Władysław Spoliński[18].

Komenda Krakowskiej Chorągwi Męskiej powstała 1 grudnia 1920 r. z przekształcenia Skautowej Komendy Okręgowej. W dniu tym komendant chorągwi podharcmistrz Tadeusz Biernakiewicz zwrócił się do harcerzy z następującym apelem:

> Obejmując komendę zwracam się do wszystkich drużyn i do wszystkich instruktorów z gorącym wezwaniem do wytężonej pracy. Po spełnionym obowiązku, który powołał nas do obrony zagrożonej Rzeczypospolitej i po powrocie do warsztatu codziennej pracy, czas już na twórcze i celowe budowanie harcerstwa, zarówno jego wewnętrznej treści, jak i organizacji. Przed nami praca wielka i zaszczytna. Dużo jest złego, niepotrzebnego, szkodliwego, dużo słabości, nieudolności i nieumiejętności.

11 Bronisław Piątkiewicz (1878–1966), prof. fotogrametrii, ppłk, skautowy komendant miejscowy w Krakowie (1914–1917), komendant drużyn skautowych I i II Okręgu „Sokoła" (1916–1920).

12 Jednostka ta, sformowana w koszarach przy ul. Rajskiej, nosiła nazwę I kompanii Krakowskiego Harcerskiego Batalionu 201/V. Fotografia z pieczęcią w posiadaniu autora. Zob. B. Leonhard, *Kalendarium z dziejów harcerstwa krakowskiego 1910–1950*, Kraków 2001, s. 58.

13 Archiwum Akt Nowych w Warszawie, zespół „Archiwum Związku Harcerstwa Polskiego [1913–1939]" (dalej: AAN, AZHP), sygn. 1272, k. 35, Pismo B. Piątkiewicza z 2 IX 1920 r. z prośbą o zwolnienie z obowiązków; k. 36, pismo z 30 IX 1920 r. – tymczasowe powierzenie funkcji T. Biernakiewiczowi.

14 AAN, AZHP, sygn. 1272, k. 60–61, Pismo Komendy Męskiej Chorągwi Krakowskiej L. 30/20 z 26 XI 1920 r. do Głównej Kwatery Męskiej ZHP.

15 Tadeusz Stefan Biernakiewicz (1898–1965), mgr wych. fiz., pracownik Studium WF UJ i CIWF, harcmistrz, komendant Krakowskiej Chorągwi Męskiej (1920–1921), członek Naczelnej Rady Harcerskiej (1921–1923).

16 Henryk Kapiszewski (1899–1964), prawnik, dyplomata, historyk, harcmistrz, komisarz międzynar. Gł. Kwatery Harcerzy (1933–1935), kierownik Wydz. Zagr. Naczelnictwa ZHP (1935–1936), komisarz międzynar. Naczelnego Komitetu Wykonawczego ZHP w Paryżu (1939–1940), kierownik Działu Zagr. Komitetu Naczelnego ZHP w Londynie (1943–1944); ojciec prof. Andrzeja Kapiszewskiego (1948–2007).

17 Stefan Kuta, od 1922 r. Kaliński (1892–1946), oficer WP, harcmistrz, komendant Krakowskiej Chorągwi Męskiej (1921–1922), malarz pejzażysta.

18 AAN, AZHP, sygn. 1272, k. 55, Rozkaz miesięczny Komendy Męskiej Chorągwi Krakowskiej ZHP L. 2 z 2 I 1921 r.; k. 66, Rozkaz miesięczny Komendy Chorągwi L. 1 z 1 XII 1920 r.

Tylko przy wspólnym, zgodnym wysiłku zdołamy to wszystko usunąć. Trzeba nam więc nabrać dobrej woli i ufności we własne siły, a wysiłki uwieńczone zostaną pomyślnym skutkiem. Chwila ta jest, według nas, odpowiednią, a sprawa pilną i naglącą. W Polsce ścichła wojenna wrzawa. Od granic zewnętrznych nam trzeba wzrok ku sobie skierować i skrzętnie budować dom, którego wznoszenia odbiegliśmy dla obrony przed złym sąsiadem. Imajmy się więc wielkiego dzieła, do którego powołany jest każdy z nas, czy komendant, czy drużynowy, czy najmłodszy z młodzików, dzieła odrodzenia wewnętrznego Polski, którą we własnych duszach nosimy. Czuwajmy![19].

Rozkaz miesięczny L. 1 z dnia 1 grudnia 1920 r. określił granice chorągwi: „do linii rzeki Wisłoka i górnego Sanu na wschód, do granicy Śląska ciesz. na zachód w granicach zach. Małopolski”[20].

Komenda chorągwi ukonstytuowała się w następującym składzie[21]: komendant chorągwi – phm.[22] Tadeusz Biernakiewicz, przyboczny (sekretarz) – phm. Henryk Kapiszewski, referent organizacyjny – phm. Władysław Spoliński, referent skarbowy – Kazimierz Parafiński, instruktor objazdowy – Zbigniew Trylski[23].

Uchwałą Naczelnictwa ZHP z dnia 9 grudnia 1920 r. stopień przodownika otrzymali[24] Józef Bielec[25], Józef Grzesiak[26], Tadeusz Kossowski, Kazimierz Parafiński i Stanisław Wąsowicz[27].

Na dzień 2 stycznia 1921 r. w skład Krakowskiej Chorągwi Męskiej wchodziły następujące hufce: Kraków, obejmujący drużyny z Krakowa, Rakowic, Podgórza i Wieliczki; Wadowice, do którego należały drużyny z Wadowic, Kleczy Górnej, Andrychowa i Zatora; Tarnów, Rzeszów i Nowy Sącz. Drużyny z pozostałych miejscowości podlegały bezpośrednio komendzie chorągwi[28].

W styczniu 1921 r. ukazał się okólnik komend krakowskich chorągwi męskiej i żeńskiej, wzywający w związku ze zbliżającym się plebiscytem do zbiórki pieniędzy i książek dla harcerstwa górnośląskiego. Informował też, że drużyny krakowskie zobowiązały się do przekazania na ten cel 10 marek od osoby[29].

[19] AAN, AZHP, sygn. 1272, k. 65, Rozkaz miesięczny Komendy Chorągwi L. 1 z 1 XII 1920 r.

[20] *Ibidem*.

[21] *Ibidem*, k. 66.

[22] phm. – podharcmistrz.

[23] Zbigniew Trylski (1899–1972), inż. rolnik, nauczyciel, harcmistrz, Naczelnik Harcerzy (1937–1939), wiceprzewodniczący ZHP poza granicami Kraju (1949–1950).

[24] AAN, AZHP, sygn. 1272, k. 79.

[25] Józef Bielec (1899–1940), dr praw, harcmistrz, komendant Krakowskiej Chorągwi Męskiej (1923–1924), komendant Śląskiej Chorągwi Harcerzy (1935–1939); zginął w Bołogoje k. Charkowa.

[26] Józef Andrzej Grzesiak, pseud. Czarny, Kmita, Mar (1900–1975), urzędnik, kpt. AK, harcmistrz, komendant Wileńskiej Chorągwi Męskiej/Harcerzy (1926–1933, 1935–1936), komendant Wileńskiej Chorągwi Szarych Szeregów „Ul Brama” (1941–1944), więziony w Workucie (1945–1955), kier. Wydz. Obozów Gł. Kwatery Harcerstwa (1957–1958), komendant Gdańskiej Chorągwi Harcerstwa (1957–1958).

[27] Stanisław Michał Wąsowicz, pseud. Sztoś (1901–1941), prawnik, sędzia, harcmistrz, hufcowy Hufca Harcerzy w Nowym Sączu (1931–1937), hufcowy Szarych Szeregów w Nowym Sączu (1939–1941), zginął rozstrzelany w obozie koncentracyjnym Auschwitz.

[28] AAN, AZHP, sygn. 1272, k. 55, Rozkaz miesięczny Komendy Męskiej Chorągwi Krakowskiej ZHP L. 2 z 2 I 1921 r.

[29] AAN, AZHP, sygn. 1272, k. 57, Okólnik Komend Chorągwi Krakowskich ZHP L. 2 z 15 I 1921 r.

Tabela 1. Wykaz drużyn przyjętych do Krakowskiej Chorągwi Męskiej 1 grudnia 1920 r.

Lp.	Miejscowość	Numer	Patron
1.	Andrychów	I	T. Kościuszko
2.	Chrzanów	I	brak
3.	Jasło	I	J. Bem
4.	Klecza Górna	I	S. Czarniecki
5.	Kraków	I	T. Kościuszko
6.	Kraków	II	H. Dąbrowski
7.	Kraków	III	K. Pułaski
8.	Kraków	IV	J. Grodyński*
9.	Kraków	VI	R. Traugutt
10.	Kraków	VII	T. Rejtan
11.	Kraków	IX	D. Czachowski
12.	Kraków	XIII	J. Dwernicki
13.	Mielec	I	T. Kościuszko
14.	Mielec	II	J. Kiliński
15.	Myślenice	I	T. Kościuszko
16.	Nowy Sącz	I	S. Czarniecki
17.	Nowy Sącz	II	R. Traugutt
18.	Nowy Sącz	IV	Zawisza Czarny
19.	Nowy Targ	I	Kazimierz Pułaski
20.	Podgórze (Kraków)	I	brak
21.	Prądnik k. Krakowa	I	W. Warneńczyk
22.	Rakowice k. Krakowa	brak	brak
23.	Rzeszów	I	J. Piłsudski
24.	Rzeszów	II	T. Kościuszko
25.	Rzeszów	III	S. Czarniecki
26.	Rudnik n. Sanem	I	T. Kościuszko
27.	Tarnów	I	Zawiszy Czarnego
28.	Tarnów	II	S. Mohort
29.	Tarnów	III	M. Wołodyjowski
30.	Tarnów	IV	brak
31.	Wadowice	I	S. Żółkiewski
32.	Wieliczka	I	T. Kościuszko
33.	Wieliczka	II	Zawisza Czarny
34.	Zakopane	I	J. Poniatowski
35.	Zator	I	T. Kościuszko
36.	Żywiec	I	K. Pułaski

* Jerzy Grodyński (1883–1918), inż. architekt, skautowy komendant miejscowy w Krakowie (1917–1918), zginął w czasie walk o Lwów.

Źródło: Archiwum Akt Nowych w Warszawie, zespół „Archiwum Związku Harcerstwa Polskiego [1913–1939]”, sygn. 1272, k. 65–66, Rozkaz miesięczny Komendy Chorągwi L. 1 z 1 XII 1920 r.

W dniach 12–14 lutego 1921 r. przebywał w Krakowie wiceprzewodniczący ZHP dr Tadeusz Strumiłło[30], który tak ocenił pracę komendy Krakowskiej Chorągwi Męskiej i hufca krakowskiego:

> K[o]m[en]da chor. bardzo młoda, pracuje bodaj dość sprawnie, kancelaria w porządku (prowadzi Kapiszewski); kłopoty z lokalem (gdy coś wynaleźli niezłego, wojsko im zarekwirowało, gnieżdżą się więc w ciemnej sali parterowej «Samopomocy» od podwórza, gdzie jest ciasno, a wszystko ma się zmieścić); przygotowania do puszczenia w ruch sklepu… […] Stosunek obu k[o]m[en]d ch[orągwi] dobry, razem tworzą grono dość zżyte, swobodne i sympatyczne.
> Drużyny w Krakowie – odradzają się stopniowo – nie tyle liczebnie, ile co do życia się i zabierania do porządnej pracy. Na zbiórce szarż miałem ok. 50 chłopców z 14 drużyn. […]
> Prezentują się chłopcy dość wątle, ale sympatycznie i dość zuchowato; kilka drużyn dobrze wyekwipowanych i z laskami (zwł. Rakowicka).
> Prowincją zajmuje się w K[o]m[en]dzie m[ęskiej] jako jej wizytator dh Trylski. Dane pierwsze zebrano drogą ogłoszeń i wezwań w pismach, bo po dawnej K[o]m[en]dzie b. słabe wykazy pozostały.
> Hufiec Krakowski obejmuje prócz 11 drużyn Krakowskich – Rakowicką i 2 wielickie, które między sobą tak ostro walczą, że z nich hufca zrobić nie można. Prawie wszystkie dr[użyn]y hufca Krak[owskiego] mają już na czele akademików (wybranych w Kole St[arszego]. harc.), jedna jest przy Sokole Podgórskim (b. młoda i jeszcze niekarna – 12-ta), jedna ma czynnego, porządnego opiekuna prof. Gostkowskiego (9-ta – też Podgórska) i osobne Koło P[rzyjaciół] H[arcerstwa], jedna («czarna 13-tka») ma na czele montera (Soleckiego), porządnego chłopa, jedna jest mieszana «przedmiejska»: (Prądnicka – 11-ta), jedną kieruje profesor jako drużynowy (Rakowicką – prof. Hirnle – dawniej w Kołomyi). Rakowicka dr[użyn]a zasługuje na uwagę jeszcze i dlatego, że obejmuje 70% internatu XX. Pijarów, jest zżyta, dobrze wychowawczo postawiona i sporo technicznie wyrobiona.
> Dr[użyn]a 10-ta ze Szk. Przemysłowej – pod opieką prof. Affanasowicza[31] – ma na razie 16 ludzi i szykuje się do silnej kampanii w roku następnym. […]
> Środowisk więc w Chorągwi razem 24. Drużyn około 45[32].

13 lutego 1921 r. w sali Kopernika Collegium Novum UJ z udziałem ok. 300 osób odbył się „wiec rodzicielsko-nauczycielski", na którym do Koła Przyjaciół Harcerstwa wstąpiło ok. 100 obecnych, wybrano Komitet Organizacyjny pod przewodnictwem prof. Gostkowskiego oraz odbył się odczyt dr. Tadeusza Strumiłły[33].

14 lutego odbył się w Parku Jordana przegląd krakowskich drużyn męskich i żeńskich przez Przewodniczącego ZHP gen. Józefa Hallera[34]. Mimo śnieżnej pogody

[30] Tadeusz Strumiłło, pseud. Dąb (1884–1958), dr filozofii, pedagog, harcmistrz Rzeczypospolitej, współtwórca harcerstwa, przewodniczący Nacz. Rady Harcerskiej (1919–1920), wiceprzewodniczący ZHP (1920–1923), Przewodniczący ZHP (1923–1925).

[31] Michał Affanasowicz (1887–1949), prof., inż. mechanik, harcmistrz, w 1914 r. członek Związkowego Naczelnictwa Skautowego, komendant Krakowskiej Chorągwi Męskiej (1923).

[32] AAN, AZHP, sygn. 1272, k. 58–60, Sprawozdanie Tadeusz Strumiłły z wyjazdu do Krakowa, 23 II 1921 r.

[33] AAN, AZHP, sygn. 1272, k. 62, Sprawozdanie Tadeusz Strumiłły z wyjazdu do Krakowa, 23 II 1921 r.

[34] Józef Haller (Haller de Hallenburg) (1873–1960), gen. broni, polityk, Przewodniczący ZHP (1920–1923), przewodniczący Zarządu Oddziału Wielkopolskiego ZHP (1927–1931).

stawiło się ok. 300 harcerzy, którzy po raporcie i przeglądzie dali pokaz umiejętności z ratownictwa i sygnalizacji. Następnie gen. Haller odebrał przyrzeczenie od ok. 10 druhen i 30 druhów[35].

Jeszcze w tym samym miesiącu ukonstytuował się Zarząd Oddziału pod przewodnictwem prof. Stanisława Ciechanowskiego[36], który od marca tegoż roku pracował w czterech sekcjach: prawniczej, lekarskiej, skarbowej i prasowej. Na uwagę zasługuje działalność sekcji lekarskiej, która sprawowała opiekę lekarską nad drużynami, gdyż wobec często podejmowanych przez drużyny wycieczek i braku skutecznych lekarstw bardzo ważna była działalność profilaktyczna. Drugim ważnym kierunkiem działalności Zarządu Oddziału było tworzenie warunków materialnych dla funkcjonowania harcerstwa; dużym sukcesem było uzyskanie terenu pod stanicę harcerską w Piwnicznej[37].

W marcu ukazał się okólnik obu komend chorągwi, zawierający m.in. apel o wpłaty na budowę stanicy harcerskiej w Piwnicznej i o pomoc w formie świadczenia pracy w ramach obozu roboczego harcerzy w wieku powyżej 16 lat, a ponadto – informacje o reorganizacji Komisji Dostaw Harcerskich w formie spółdzielni oraz zapowiedź organizacji Harcerskiej Kasy Oszczędności.

W okólniku ukazał się również list obu komend chorągwi do Inspektoratu Harcerskiego Okręgu Górnośląskiego w Bytomiu:

> Kochani Bracia!
> Z najstarszego grodu naszej Rzeczypospolitej, z serca Polski, które bije dźwiękiem wawelskiego dzwonu – Krakowa, odzywamy się do Was Bracia górnośląscy harcerze. Zasyłamy Wam najserdeczniejsze słowa braterskich pozdrowień i otuchy w Waszej walce o najświętsze prawa do narodowego bytu i rozwoju. Brakowało Was dotąd w naszym Domu, wielkiej, niepodzielnej Rzeczypospolitej, brakowało Was dotąd harcerze najmłodsi w naszym ogólnopolskim Związku Harcerstwa Polskiego, w który wnieść macie Waszą miłość i niczem niezachwianą wierność Ojczyźnie i Wasze tęgie dłonie do pracy nad wznoszeniem wielkiego gmachu Odrodzonej, Nowej Młodej Polski.
> Aby Wam choć trochę w Waszej walce pomóc, chorągiew krakowska ZHP, która obejmuje drużyny harcerskie na obszarze województwa krakowskiego, złożyła dla Was kilkaset książek i broszur polskich, które oby były wyrazem naszej łączności i zwiastunem dobrej nowiny braterstwa harcerskiego całej ziemi polskiej – oraz kilkanaście tysięcy marek polskich, które oddajemy do dyspozycji Inspektoratu okręgowego Górnego Śląska w Bytomiu.
> Imieniem drużyn żeńskich i męskich chorągwi krakowskiej – Komendy żeńskiej i męskiej Chorągwi Krakowskich ZHP w przeddzień niechybnego Sprawy Waszej i naszej zwycięstwa, którego Bóg najwyższy niech użyczy, przesyłamy Wam Bracia i Siostry gromkie słowa pozdrowień i zachęty do wytrwania w walce.
> Jednością silni Wy i My – Czuwajmy![38]

[35] AAN, AZHP, sygn. 1272, k. 59, Sprawozdanie Tadeusz Strumiłły z wyjazdu do Krakowa, 23 II 1921 r.

[36] Stanisław Witalis Ciechanowski (1869–1945), prof. dr hab., lek. anatomopatolog, przewodniczący Zarz. Oddziału ZHP w Krakowie (1921–1922), członek Nacz. Rady Harcerskiej (1921–1925).

[37] *II Sprawozdanie Naczelnej Rady Harcerskiej (1 I – 1 IX 1921)*, Warszawa 1921, s. 26–27. Stanica harcerska na Szerokiej Polanie w Kosarzyskach k. Piwnicznej, uroczyście otwarta w 1927 r., funkcjonuje do dziś.

[38] AAN, AZHP, sygn. 1272, k. 88–89, Okólnik Komend Chorągwi Krakowskich L. 3 z 15 III 1921 r.

W dniach 22–25 marca 1921 r. odbył się zjazd instruktorów chorągwi i krótki kurs metodyczny, obejmujący m.in. w części pierwszej mszę świętą i zwiedzanie Wawelu, sprawozdania środowisk i dyskusję, a części drugiej – wykłady i wycieczkę z ćwiczeniami[39].

Naczelnictwo ZHP 14 kwietnia 1921 r. zatwierdziło nowy skład komendy Krakowskiej Chorągwi Męskiej: komendant – phm. Tadeusz Biernakiewicz, przyboczny – phm. Henryk Kapiszewski, referent organizacyjny – Jan Surzycki, referent gospodarczy – phm. Władysław Spoliński, instruktor objazdowy – Zbigniew Trylski, referent skarbowy – Józef Bielec, urlopowany na okres egzaminów – Kazimierz Parafiański[40].

III powstanie śląskie zaktywizowało społeczeństwo Krakowa. Młodzież licznie zgłaszała się do punktów werbunkowych Towarzystwa Obrony Kresów Zachodnich i Związku Strzeleckiego. Zorganizowane grupy, liczące po 60, 80, a nawet 100 ochotników, były wysyłane na teren Górnego Śląska. Obok nich tworzyły się mniejsze grupy złożone z harcerzy, które wyjeżdżały samorzutnie. Wyjeżdżano także indywidualnie. Przykładem może tu być członek komendy chorągwi, b. harcerz i drużynowy III Drużyny Krakowskiej ppor. art. Jan Surzycki[41], który „zdezerterował" wraz z działonem i działkiem kal. 37 mm; zginął w ataku na Stare Koźle[42]. Wśród uczestniczących w powstaniu ok. 700 harcerzy najwięcej było osób z Krakowa[43].

19 czerwca 1921 r. w sali Kopernika Collegium Novum UJ odbyło się pierwsze spotkanie Koła Przyjaciół Harcerstwa Hufca Męskiego w Krakowie, którego przewodniczącym był rektor UJ prof. Stanisław Estreicher, a sekretarzem – prof. I Gimnazjum Feliks Fidziński[44].

W pierwszych dniach lipca odbył się we Lwowie zlot z okazji 10-lecia harcerstwa. Wśród 5000 uczestników liczną grupę stanowili harcerze krakowscy, dla których przygotowano specjalny pociąg i zapewniono zniżki kolejowe[45].

W czasie zlotu wydawane było pisemko „Wici Zlotowe", redagowane przez phm. Adama Ciołkosza[46], który rozprowadzał tam także broszurę z wydawanej

[39] AAN, AZHP, sygn. 1272, k. 90, Okólnik Komendy Chorągwi Męskiej L. 3 z 15 III 1921 r.

[40] AAN, AZHP, sygn. 1272, k. 81, Pismo Komendy Męskiej Chorągwi Krakowskiej l. dz. 203/21 z 16 III 1921 r. o zatwierdzenie składu komendy chorągwi.

[41] Jan Surzycki (1898–1921), student UJ, ppor. art., podharcmistrz, członek i referent organizacyjny komendy Krakowskiej Chorągwi Męskiej, uczestnik walk o Przemyśl i Lwów, kawaler orderu Virtuti Militari.

[42] A. Szeliga-Zahorska, *Krakowscy harcerze w powstaniach śląskich*, [w:] *Powstanie harcerstwa i jego udział w walkach o niepodległość i kształt granic odrodzonej Rzeczpospolitej. Materiały z konferencji naukowej odbytej w sali obrad Rady Miasta Krakowa w dniach 18–19 sierpnia 2010 roku*, red. J. Wojtycza, Kraków 2010, s. 210–212.

[43] Wg zestawień Głównej Kwatery Męskiej, w czasie walk o niepodległość i kształt granic Rzeczypospolitej sześciu harcerzy drużyn krakowskich zostało odznaczonych Krzyżem Srebrnym Virtuti Militari, dziewięciu – Krzyżem Walecznych, dziesięciu – innymi odznaczeniami, a 29 poległo. AAN, AZHP, sygn. 1401, k. 124, 127.

[44] AAN, AZHP, sygn. 1272, k. 128–129, Odezwa Zarządu Koła Przyjaciół Harcerstwa w Krakowie.

[45] AAN, AZHP, sygn. 1272, k. 136, Okólnik komendy Męskiej Chorągwi Krakowskiej L. 5 z 15 VI 1921 r.; zob. W. Błażejewski, *op. cit.*, s. 161.

[46] Adam Witold Maria Ciołkosz, pseud. Kremerowski (1901–1978), prawnik, publicysta, podharcmistrz, hufcowy i komendant Harcerskiej Komendy Dzielnicowej w Tarnowie (1917–1918), komendant Naczelnej Komendy Organizacji Harcerskiej na Warmię i Mazury (1920), przywódca Wolnego Harcerstwa (1921–1924).

w Krakowie serii „Listy do starszych harcerzy" pt. *Potrzeba przebudowy*, zawierającą opis koncepcji pracy harcerskiej po odzyskaniu przez Polskę niepodległości oraz apel o decentralizację ZHP i objęcie jego zasięgiem, na wzór angielski, „mas młodzieży rzemieślniczej i robotniczej, a wreszcie nędzoty miejskiej, dzieci ulicy, suteryn i poddaszy"[47]. Ciołkosz w kwietniu 1921 r. został zwolniony ze składu Głównej Kwatery Męskiej i jeszcze w tym samym roku odszedł na własną prośbę z ZHP[48].

W czasie wakacji 1921 r. odbył się kurs instruktorski w Piwnicznej oraz nieliczne obozy. W całej Polsce zorganizowano ogółem tylko 44 wakacyjne obozy harcerzy[49]. Wśród przyczyn tak niewielkiej akcji obozowej Zarząd Oddziału wskazał spóźnienie przekazania przyznanych subwencji, niewielką liczbę zgłoszeń, wynikającą z niezamożności rodziców uczestników, oraz zmiany personalne w komendzie hufca[50].

16 października 1921 r. odbył się w Krakowie Zjazd Oddziału ZHP, który wybrał na przewodniczącego prof. UJ Stefana Surzyckiego, a na wiceprzewodniczącego – dowódcę okręgu gen. Aleksandra Osińskiego[51]. W „Sprawozdaniu ze Zjazdu Oddziału ZHP w Krakowie" phm. Stanisław Sedlaczek[52] napisał:

> Z sprawozdania ustępującego Zarządu widać, że wykonano dużą pracę organizacyjną i pozyskano szereg poważnych osób do współpracy, zarówno w Zarządzie, jak w Kołach Przyjaciół, których kilka zorganizowano. Na uwagę zasługuje fakt pozyskania lekarzy dla hufców i drużyn w kilku miejscowościach i dalsza akcja w tym kierunku prowadzona przez sekcję lekarską. […]
> Pomoc miał Zarząd ze strony: Gen. Osińskiego (kurs w Limanowej i Pieskowej Skale), Towarzystwa Strzeleckiego (kurkowego – lokal, boisko), YMCA (kurs pływacki), Gminy Piwniczna (bezpłatnie ustaliła miejsca na obóz letni i ofiarowała 1 morgę w Kosarzyskach na stanicę), od Magistratu i Min. Zdrowia (kolonie), kap. Pfeiffera[53].

Tego samego dnia na zjeździe instruktorów referat programowy wygłosił Adam Ciołkosz, niebędący już instruktorem ZHP. Na komendanta chorągwi został wybrany phm. Stefan Kuta. Obok niego na funkcję komendanta kandydowali także phm. Henryk Kapiszewski i phm. Zbigniew Trylski[54]. Komenda Chorągwi ukonstytuowała

[47] W. Błażejewski, *op. cit.*, s. 162; B. Leonhard, *op. cit.*, s. 62.

[48] Wątku tego nie rozwijamy, gdyż epizod Wolnego Harcerstwa jest szczegółowo opisany w historiografii harcerskiej, a przy tym nie odnosi się wyłącznie do harcerstwa krakowskiego.

[49] *Materiały do chronologii historii i tradycji ZHP*, cz. 3, „Harcerstwo" 1982, nr 3, s. 26 (18).

[50] *II Sprawozdanie Naczelnej Rady Harcerskiej…*, s. 28.

[51] Aleksander Osiński (1870–1956), generał-major armii Imperium Rosyjskiego, gen. dyw. WP, kier. Ministerstwa Spraw Wojskowych (1923), senator RP (1935–1939), wiceprzewodniczący ZHP (1923–1926).

[52] Stanisław Marian Sedlaczek, pseud. Marian Lwowicz, Sas (1892–1941), pedagog, harcmistrz Rzeczypospolitej, Naczelnik Harcerstwa na Rusi i w Rosji (1915–1919), Naczelnik Głównej Kwatery Męskiej (1919–1921), wiceprzewodniczący ZHP (1921–1926), Naczelnik Harcerzy (1926–1931), Naczelnik Harcerstwa Polskiego (1939–1941), zginął w obozie koncentracyjnym Auschwitz.

[53] AAN, AZHP, sygn. 1272, k. 169, S. Sedlaczek, Sprawozdanie ze zjazdu Oddziału ZHP w Krakowie, 16 października 1921, Warszawa 18 X 1921 r.

[54] AAN, AZHP, sygn. 1272, k. 171, A. Heinrich, Raport z dojazdu do Krakowa na zjazd instruktorów Chorągwi w dniu 16 października 1921 r., 18 X 1921 r.

się w składzie: phm. Stefan Kuta – komendant chorągwi, phm. Henryk Kapiszewski – przyboczny komendanta chorągwi, pd.[55] Kazimierz Parafiński – referent skarbowy, Jerzy Barun – referent prasowy, phm. Zbigniew Trylski – instruktor objazdowy[56].

W rozkazie komendy chorągwi phm. Tadeusz Biernakiewicz, żegnając się z podwładnymi, napisał:

> Nie liczcie w pracy waszej na żadną pobudkę z góry, lecz pracujcie tak, jakby jej zupełnie nie było, wydobywając ze siebie całą pomysłowość, inwencję i energię, na jaką was stać! Budźcie w waszych zastępach, drużynach i w każdym poszczególnym harcerzu zainteresowanie się życiem i pracami swego zastępu, drużyny, chęć osiągania coraz większej sumy sprawności fizycznych i moralnych, twórzcie życie i ruch, pamiętając że senność, nuda i nieruchliwość to śmierć waszej pracy! Nie tracąc nigdy z oczu naszych wielkich celów, nie zaniedbujcie żadnego z środków, którymi tak bogato nasz system rozporządza i taktujcie każdy z nich, jakby od niego wszystko zależało! Nie zrażajcie się tym, że wasi chłopcy nie zawsze i nie dość dokładnie odróżniają rzeczy wielkie od małych, wiedzcie bowiem, że jeśli u instruktora jest świadomość celów, znajdzie się ona i u jego harcerzy! Strzeżcie się tylko z jednej strony zejścia na bezduszną drogą ideologizowania, z drugiej zmechanizowania i zamknięcia pracy w ciasne regułki organizacyjności, która jest tylko środkiem ułatwiającym osiągnięcie naszych celów! Starajcie się różniczkować to życie, nigdy zaś go nie przytłumiać formami!
> Nie wprowadzajcie też w wasze życie wielu form wojskowych, które rychlej niż cokolwiek innego doprowadzają do spaczenia harcerstwa i wyrodzenia się w nienaturalne zwyczaje, choćby nawet początkowo miały wielkie u chłopców powodzenie! System zawodów i współzawodnictwa, reprezentowany tak silnie w sportach, które oby jak najszerzej ogarnęły nasze drużyny, winien być jednym z głównych waszych środków pracy. Pociąga to za sobą ćwiczenie się małymi grupami, a więc zwrócenie bacznej uwagi na życie i pracę zastępów, które tak dotąd po macoszemu traktowano! Streszczając dodam jeszcze, że naczelną zasadą winno być jak najbardziej swoiste traktowanie pracy i nie krępowanie się żadnym schematem ni formułą zgodnie tylko z ogólnymi podstawami systemu, własnym sumieniem i poczuciem karności organizacyjnej. […]
> [Ż]yczę z najgłębszego serca, by praca wasza przyniosła te wyniki, jakich słusznie zarówno my sami, jak i cała Polska po harcerstwie oczekuje! Szczęść Wam Boże! Czuwajcie![57].

W dniach 30 października – 1 listopada 1921 r. w auli Uniwersytetu Jagiellońskiego obradował VIII Zjazd Naczelnej Rady Harcerskiej. Z tej okazji w parku Jordana odbył się przegląd z udziałem 282 harcerzy i 142 harcerek. Przewodniczący ZHP gen. Haller udekorował odznaką „Za Zasługę" organizatora i byłego przewodniczącego, a w tym czasie członka Zarządu Oddziału ZHP w Krakowie prof. Stanisława Ciechanowskiego[58].

[55] pd. – przodownik, wówczas najniższy stopień instruktorski w ZHP.

[56] AAN, AZHP, sygn. 1272, k. 186, Rozkaz miesięczny komendy Męskiej Chorągwi Krakowskiej L. 12 z XI 1921 r.

[57] AAN, AZHP, sygn. 1272, k. 160–161, Rozkaz Komendy Męskiej Chorągwi Krakowskiej L. 11 z X 1921 r.

[58] C. Brzoza, *Kraków między wojnami. Kalendarium 28 X 1918 – 6 IX 1939*, Kraków 1998, s. 78; B. Leonhard, *op. cit.*, s. 64..

2 listopada 1921 r. w Krakowie odbyła się odprawa komendantów i komendantek chorągwi. Z Krakowa wzięli w niej udział jako goście prof. S. Surzycki, phm. dr T. Strumiłło, phm. T. Biernakiewicz, phm. Z. Trylski i J. Horodelski. W „Protokole odprawy komendantów środowisk pracy harcerskiej" w sprawozdaniu komendy Krakowskiej Chorągwi Męskiej czytamy:

> Dotychczasowa Komenda działała chaotycznie. Był Kurs Metodyczny; jeden w czasie Wielkiejnocy, drugi w lecie. Na obu wyniki pracy b. dobre. We wszystkich drużynach zrobiono inspekcję. Obecnie praca idzie dość dobrze; są warsztaty. Po wakacjach już był jeden popis i wystawa prac. W projekcie jest szereg popisów. Odbył się zjazd Chorągwi, na którym dokonano wyboru nowego komendanta. Stosunek do władz wojsk. b. dobry. – Wiele pomagają. Wojsko dało lokal na komendę, bursy i na izby drużyn. Koło Star[szego]. Harc. istnieje i działa bardzo sprawnie. Są dwie drużyny wiejskie oraz jedna „Zuchów" – z[astę]py zuchów są jednocześnie i przy drużynach. Istnieją dwie bursy (męska i żeńska) w lokalu ofiarowanym przez wojsko. – Piwniczna daje dwa morgi ziemi, N. Sącz – 2 morgi. Tworzy się warsztaty oraz organizuje Koła Przyjaciół. Na przyszłym zlocie Chorągwi rozegrane będą zawody o pierwsze miejsce (dla drużyny) w Chorągwi. Drużyn jest 57, ludzi do 3000[59].

Z tą informacją koresponduje ocena Naczelnika Głównej Kwatery Męskiej phm. Henryka Glassa: „W Krakowie też widać postęp w pracy; uderza tu nadzwyczaj wydatna pomoc społeczeństwa; pomyślnym objawem jest powstanie Oddziału. Co się tyczy «kursu instr.» to bezwzględnie stał on na wysokości zadania, ale szkoda, że nie zwrócono się do Gł. Kw. o przeprowadzenie próby"[60].

9 listopada 1921 r. Naczelnictwo ZHP mianowało komendantem Krakowskiej Chorągwi phm. Stefana Kutę, a jego zastępcą – phm. Zbigniewa Trylskiego[61]. Komenda Chorągwi z dniem 16 listopada 1921 r. podzieliła dotychczasowy Hufiec Krakowski na Hufiec Krakowski (drużyny I–VIII, X, XI, XIII i XVII), Hufiec Podgórsko-Wielicki (drużyny IX, XII, XV i XVI) oraz Hufiec Rakowicki (drużyny XIV i XVIII)[62].

W grudniu tego roku komendant chorągwi poinformował, że został wykonany sztandar chorągwi[63]. Sztandar ten został uroczyście poświęcony i wręczony na Rynku Głównym 28 maja 1922 r. w czasie apelu rozpoczęcia „Tygodnia Harcerskiego"[64].

Podsumowanie

W artykule przedstawiono rozwój organizacyjny Krakowskiej Chorągwi Męskiej w świetle dokumentów wytworzonych przez Zarządu Oddziału, władze harcerskie

[59] AAN, AZHP, sygn. 666, k. 96, O. Grzymałowski, Protokół odprawy komendantów środowisk pracy harcerskiej na terenie ZHP, Kraków 2 XI 1921 r.

[60] AAN, AZHP, sygn. 666, k. 77.

[61] Rozkaz Naczelnictwa ZHP L. 4 z 12 I 1922 r., „Rozkazy, okólniki, instrukcje [N ZHP]" nr 12 z 21 I 1922 r., s. 4.

[62] AAN, AZHP, sygn. 1272, k. 211, Rozkaz Komendy Męskiej Chorągwi Krakowskiej L. 14 z XII 1922 r.

[63] AAN, AZHP, sygn. 1272, k. 209, Okólnik Komendy Męskiej Chorągwi Krakowskiej L. 6 z 1 XII 1921 r.

[64] C. Brzoza, *op. cit.*, s. 88. Sztandar znajduje się w Kolekcji Harcerskiej Muzeum Krakowa, która powstała w 1991 r.

chorągwi oraz centralne. Chorągiew powstała w wyniku połączenia w jednolity Związek Harcerstwa Polskiego dawnych dzielnicowych organizacji harcerskich, co miało miejsce w czasie I Walnego Zjazdu w Warszawie w dniach 31 grudnia 1920 – 2 stycznia 1921 r. Równolegle organizował się Zarząd Oddziału Krakowskiego ZHP. Praca chorągwi szybko okrzepła. W 1921 r. w samym Krakowie działało już 18 drużyn podzielonych na trzy hufce. Środowisko było dobrze oceniane przez władze i wspierane przez lokalne społeczeństwo. Chorągwią sprawnie kierował – pomimo częstych zmian personalnych – dobrze przygotowany i ideowo zaangażowany zespół. Jej działalność organizowali m.in. późniejsi wybitni działacze harcerscy, pełniący funkcje w naczelnych władzach ZHP. Niektórzy z nich w okresie okupacji ofiarą swojego życia zaświadczyli o wierności harcerskim ideałom. Autor planuje kontynuowanie podjętych badań dla opracowania dziejów krakowskiego harcerstwa w okresie międzywojennym.

Bibliografia

Opracowania

Błażejewski W., *Z dziejów harcerstwa polskiego (1910–1939)*, Warszawa 1985.

Grochowski P., *Hufiec Harcerzy Kraków-Podgórze w latach 1922–1939*, Kraków 2004.

Hausner W., *Krakowski skauting 1910–1914*, Kraków 1994.

Hausner W., Wierzbicki M., *Sto lat harcerstwa*, Warszawa 2015.

Komendanci Chorągwi Krakowskiej ZHP z lat 1956–1996 o swojej pracy, red. J. Wojtycza, K. Wojtycza, Kraków 1999.

Konspiracja harcerska w Krakowie 1939–1945, red. J. Wojtycza, Kraków 2019.

Kozimala I., *Lwowska Chorągiew Harcerek ZHP w latach 1911–1939*, Przemyśl 2003.

Kozimala I., *Lwowska Chorągiew Harcerzy w latach 1921–1939*, Przemyśl 2007.

Leonhard B., *Kalendarium z dziejów harcerstwa krakowskiego 1910–1950*, Kraków 2001.

Mileska M.I., *Materiały do historii krakowskiego harcerstwa żeńskiego w latach 1911–1939*, t. 1, wstęp, opr. i red. J. Wojtycza, Kraków 2003.

Mileska M.I., *Materiały do historii krakowskiego harcerstwa żeńskiego w latach 1911–1939*, t. 2, opr., uzup. i red. J. Wojtycza, Kraków 2004.

Miłobędzki P., *Harcerze w okupowanym Krakowie*, Kraków 2005.

Nowik G., *Polskie związki skautowe i harcerskie 1909–1922*, Warszawa 2019.

Powstanie harcerstwa i jego udział w walkach o niepodległość i kształt granic odrodzonej Rzeczpospolitej. Materiały z konferencji naukowej odbytej w sali obrad Rady Miasta Krakowa w dniach 18–19 sierpnia 2010 roku, red. J. Wojtycza, Kraków 2010.

Rozkazy i okólniki Krakowskiej Chorągwi Męskiej/Harcerzy z lat 1920–1939, zebr. i opr. J. Wojtycza, Kraków 2017 [płyta CD].

Rozkazy Krakowskiej Chorągwi Harcerzy/Chorągwi ZHP w Krakowie z lat 1945–1950, zebr. i opr. J. Wojtycza, Kraków 2018 [płyta CD].

Rozkazy Krakowskiej Chorągwi ZHP z lat 1957–1975, zebr. i opr. J. Wojtycza, Kraków 2019 [płyta CD].

Rzońca B., *Krakowska Chorągiew Harcerzy w latach 1945–1950*, Kraków 2015.

Wojtycza J., *Hufiec Kraków-Nowa Huta w latach 1957–1989*, Kraków 2017.

Wojtycza J., *Skauting polski w Galicji i na Śląsku Cieszyńskim w latach 1910–1919*, Kraków 2000.

Wojtycza K., *Hufiec Kraków Kleparz-Łobzów w latach 1957–1972*, Kraków 2007.

Wojtycza K., *Hufiec Kraków-Krowodrza w latach 1973–1989*, Kraków 2014.

Wojtycza K., *Hufiec Kraków-Śródmieście w latach 1973–1989*, Kraków 2018.

Wojtycza K., *Hufiec Kraków-Zwierzyniec w latach 1957–1972*, Kraków 2011.

Wybór źródeł do dziejów ZHP, t. 1: *Utworzenie ogólnopolskiego Związku Harcerstwa Polskiego i czas próby ruchu harcerskiego (1918–1944)*, wyb. i opr. K. Marszałek, Kraków 2014.

Źródła archiwalne

Archiwum Akt Nowych w Warszawie, zespół „Archiwum Związku Harcerstwa Polskiego [1913–1939]", sygn. 666, 1272, 1401.

Krakowska Chorągiew Męska ZHP. Powstanie i początki działalności (1920–1921). Kalendarium wydarzeń

Streszczenie

Artykuł przedstawia początki działalności Krakowskiej Chorągwi Męskiej ZHP. Opisuje rozwój organizacyjny chorągwi w świetle dokumentów ówczesnych lokalnych oraz centralnych władz harcerskich (1920–1921). W opracowaniu wykorzystano niepublikowane źródła archiwalne, znajdujące się w Archiwum Akt Nowych w Warszawie (zespół „Archiwum Związku Harcerstwa Polskiego [1913–1939]") oraz zachowane źródła drukowane (sprawozdania Zarządu Oddziału i komendy chorągwi, rozkazy komendy chorągwi, sprawozdania Naczelnej Rady Harcerskiej i publikacje na łamach prasy harcerskiej). Powstanie chorągwi było związane z ostatecznym połączeniem w jednolity ZHP dawnych dzielnicowych organizacji harcerskich na I Walnym Zjeździe ZHP w Warszawie (31 grudnia 1920 – 2 stycznia 1921). Równolegle organizował się Zarząd Oddziału Krakowskiego ZHP. W 1921 r. w Krakowie działało już 18 drużyn podzielonych na trzy hufce. Środowisko było dobrze oceniane przez władze i wspierane przez lokalną społeczność. Jego pracę organizowali późniejsi wybitni działacze harcerscy; niektórzy z nich w czasie okupacji ofiarą swojego życia zaświadczyli o wierności harcerskim ideałom.

Słowa kluczowe: Związek Harcerstwa Polskiego (ZHP), I Walny Zjazd ZHP, harcerstwo polskie w II RP, Krakowska Chorągiew Męska ZHP, Archiwum Związku Harcerstwa Polskiego z lat 1913–1939

Krakow Region Boys' Division of the Polish Scouting and Guiding Association: Timeline of the Origins and Early Days (1920–1921)

Abstract

This paper looks at the origins and early days of the Cracow Region Boys' Division of the Polish Scouting and Guiding Association, commonly referred to in Polish as ZHP, its abbreviated form. It describes the organisational growth of the Region against the backdrop of a variety of documents pertaining to the contemporaneous local and central scouting and guiding authorities (1920–1921). The paper has been written on the basis of unpublished archive sources retrieved from the Archives of Modern Records in Warsaw – the collection of the „Polish Scouting and Guiding Association Archive [1913–1939]",

as well as the existing paperback sources – such as the reports of the Branch and Region headquarters, the orders given by the region headquarters, the reports of the Supreme Scouting and Guiding Council, and the publications found in the scouting and guiding press. The formation of the Region was connected to the ultimate merger of the former district scouting and guiding organisations into a uniform ZHP at the First General ZHP Meeting, held in Warsaw from 31 December 1920 to 2 January 1921. At the same time, the Board of the Krakow Branch of ZHP was gradually taking shape. In 1921, in Krakow there were as many as 18 teams subdivided into three troops. The whole community was well thought of by the authorities and received extensive support from the locals. At a later stage, its work was organised by eminent scouting and guiding activists. During the wartime occupation, some of them paid with their lives to prove their unreserved loyalty to the ideals of scouting.

Key words: Polish Scouting and Guiding Association (ZHP), First General Meeting of ZHP, Polish scouting and guiding in the Second Polish Republic, Krakow Region Boys' Division of ZHP, Archive of the Polish Scouting and Guiding Association from the years 1913–1939

Das männliche Fähnlein des Polnischen Pfadfinderverbands in Kraków. Entstehung und Anfang der Tätigkeit (1920–1921). Wichtigste Ereignisse Zusammenfassung

Der Artikel stellt den Anfang der Tätigkeit des männlichen Fähnleins des Polnischen Pfadfinderverbands in Kraków dar. Er beschreibt die organisatorische Entwicklung der Fähnlein vor dem Hintergrund der damaligen lokalen und zentralen Behörden der Pfadfinder (1920–1921). In dieser Arbeit wurden unveröffentlichte archivalische Überlieferungen benutzt, die sich im Archiv für Neuakten in Warschau befinden (Gruppe „Archiv für den Polnischen Pfadfinderverband [1913–1939]") und die erhalten gebliebenen gedruckten Texte verschiedener Art (Berichte des Vorstands der Abteilung und Befehle des Fähnleins, Befehle des Fähnleinkommandos, Berichte des höchsten Pfadfinder-Rates und Veröffentlichungen in der Pfadfinder-Presse) genutzt. Die Entstehung des Fähnleins war mit der endgültigen Vereinigung in einen einheitlichen Pfadfinderverband alter Viertelpfadfinderorganisationen im I. Haupttreffen des Polnischen Pfadfinderverbands in Warszawa (vom 31.XII.1920 bis zum 2.I.1921) verbunden. Gleichzeitig hat sich der Vorstand der Krakauer Abteilung des Polnischen Pfadfinderverbands organisiert. Im Jahre 1921 waren in Kraków schon 18, in 3 Einheiten geteilte Pfadfindergruppen tätig. Das Milieu wurde durch die Behörde positiv bewertet und durch die lokale Gemeinschaft unterstützt. Die Arbeit wurde von den späteren angesehenen Pfadfinderaktivisten organisiert, manche von ihnen haben ihr Leben geopfert um seinen Pfadfinderidealen stets treu zu bleiben.

Schlüsselwörter: Der Polnische Pfadfinderverband (ZHP), I. Haupttreffen des Polnischen Pfadfinderverbands, polnische Pfadfinderbewegung in der Zweiten Republik Polen, das männliche Fähnlein des Polnischen Pfadfinderverbands in Kraków, Archiv für den Polnischen Pfadfinderverband aus den Jahren 1913–1939

Краковская мужская хоругвь Союза польских харцеров. Создание и начало деятельности (1920–1921). Календарь событий Резюме

В статье рассказывается о началах деятельности Краковской мужской хоругви Союза польских харцеров (скаутов). Представлено организационное развитие хоругви (подразделения) в свете документов местных и центральных скаутских властей (1920–1921). В исследовании были использованы неопубликованные архивные источники, находящиеся в Архиве новых актов в Варшаве (фонд «Архив Союза польских харцеров [1913–1939 гг.]») и сохранившиеся печатные источники (отчеты Управления отдела и комендатуры хоругви, приказы комендатуры хоругви, доклады Верховного совета харцеров и публикации на страницах скаутских газет). Создание хоругвей было связано с объединением в единый СПХ разных скаутских организаций на Первом общем съезде СПХ в Варшаве (31 декабря 1920 г. – 2 января 1921 г.). В то же время было создано управление краковского отдела СПХ. В 1921 г. в Кракове действовало уже 18 дружин, разделенных на три хуфца (отряды). Организацию хорошо оценивали власти и она имела поддержку местных жителей. Работой организации руководили видные скаутские активисты; некоторые из них, во время нацисткой оккупации, отдали жизнь за верность скаутским идеалам.

Ключевые слова: Союз польских харцеров (СПХ), Первый общий съезд СПХ, польские скауты во Второй Речи Посполитой, Краковская мужская хоругвь СПХ, архив Союза польских харцеров 1913–1939 гг.

Varia

Varia

Varia

Вариа

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-010

Andrzej Krzak

dr hab., prof. UJD, Uniwersytet Humanistyczno-Przyrodniczy im. Jana Długosza w Częstochowie
ORCID: 0000-0002-6886-5057

Rosyjskie rozwinięcia teorii „małej wojny". Wymiar historyczny i współczesny

Wprowadzenie

Konflikty na Ukrainie, w regionie Bliskiego i Środkowego Wschodu oraz w Afryce Północnej (zwłaszcza w kontekście wojny z tzw. Państwem Islamskim) wywołały debatę odnoszącą się do zmian, jakie nastąpiły wokół współczesnej sztuki wojennej. Zaproponowane nowe spojrzenia na warunki i formy prowadzenia działań militarnych spowodowały, iż od przynajmniej dwóch dekad dominuje pogląd, że doszło do fundamentalnych zmian w dziedzinie myśli wojskowej oraz strategii i taktyki prowadzenia wojen. Skutkiem tej debaty jest pojawienie się wielu nowych pojęć i koncepcji, czego przykładem jest m.in. próba wyjaśnienia przebiegu działań militarnych w ramach konfliktu we wschodniej Ukrainie i na Krymie. Poszukiwanie nowego kanonu sztuki wojennej doprowadziło wojskowych, polemologów oraz ekspertów do zdefiniowania zjawiska nowych wojen jako konfliktów określanych mianem „wojen hybrydowych". Bezsporny pozostaje fakt, że współcześnie – w warunkach rewolucyjnego postępu naukowo-technicznego oraz dominacji mediów i rozwoju środków komunikacji – konieczne stało się dokonanie analizy zjawiska wojny na tle tych nowych uwarunkowań. Ale czy w działaniach Rosji (chociażby na Ukrainie) można dostrzec, że stosuje ona nowe, do tej pory nieznane formy prowadzenia wojen lub opracowała nowe rozwiązania taktyczne w działaniach bojowych? Czy też może są to doskonale nam znane sposoby, jedynie dostosowane do wymogów współczesnego pola walki i realiów wojny XXI w., zwłaszcza w odniesieniu do rewolucji w sprawach wojskowych, jaka miała miejsce w ciągu kilku ostatnich dekad? Pytania te posłużą analizie rosyjskich poglądów odnoszących się do prowadzenia działań militarnych w XXI w. w kontekście tzw. rosyjskiej małej wojny

– i ewolucji tego pojęcia w zderzeniu z teoriami wojen hybrydowych proponowanych przez zachodnich ekspertów. Po analizie dostępnych źródeł oraz literatury przedmiotu w oparciu o metody właściwe dla nauk politycznych, nauk o bezpieczeństwie, a także historii (wyróżnić należy przede wszystkim metodę analizy systemowej, historycznej, a także w odniesieniu do doświadczeń historycznych – analizy i syntezy) sformułowano następującą hipotezę roboczą: Rosja od ponad dwóch dekad prowadzi aktywną politykę zagraniczną nie tylko w ujęciu regionalnym, lecz przede wszystkim globalnym, która obejmuje wszystkie istotne dziedziny funkcjonowania państwa. Wojskowi i politycy przywiązują dużą wagę do poznania najnowszych trendów i zmian w światowej teorii politycznej, lecz przede wszystkim – w sztuce wojennej. Przy czym rosyjski pogląd na sztukę wojenną oraz formy i sposoby prowadzenia działań militarnych jest zawsze podporządkowany doświadczeniom i rozwiązaniom, jakie Rosja stosowała w przeszłości. Nie powinno zatem być zaskoczeniem, iż podejmowane wobec Ukrainy działania nie stanowią nowych rozwiązań doktrynalnych, lecz są modyfikacją znanych form – dostosowanych do współczesnych warunków politycznych i technologicznych.

Wojny hybrydowe – koncepcja i mit

Po zimnej wojnie analitycy w wielu krajach nie mogli dokładnie zdefiniować pojawiających się zagrożeń, które nie pasowały do ówczesnych koncepcji i nie dawały się jednoznacznie sklasyfikować[1]. Amerykańscy wojskowi w poszukiwaniu nowych kanonów mówili „o hybrydowych zagrożeniach lub wojnach [także konfliktach lub działaniach]”[2], które miałyby w końcu rozwikłać dylemat wszystkich administracji USA po zakończeniu zimnej wojny, czyli znaleźć odpowiedź na pytanie: dlaczego Stany Zjednoczone, będąc potęgą (hegemonem), nie potrafią rozstrzygnąć na swoją korzyść konfrontacji militarnej[3] ze znacznie słabszymi przeciwnikami[4].

Z kolei Rosjanie, analizując poczynania Stanów Zjednoczonych, zdawali sobie sprawę z rewolucyjnych zmian, jakie przyniósł kres zimnej wojny w przestrzeni geopolitycznej i geostrategicznej, oraz z tego, że Federacja Rosyjska (powstała po rozpadzie ZSRR) utraciła pozycję drugiego supermocarstwa i tylko jej arsenał jądrowy zmuszał Stany Zjednoczone do traktowania Rosji jako partnera. Rozwój technologii, możliwość wykorzystania nowych przestrzeni, łączenie starych metod prowadzenia walki z nowoczesnymi systemami uzbrojenia i odwrotnie, a przede wszystkim

[1] Е.Н. Грачиков, *Гибридные войны: опыт Израиля*, „Вестник Московского университета” 2015, № 4, s. 267.

[2] Zob. F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007; idem, *Hybrid Warfare Challenges*, „Joint Force Quarterly” 2009, nr 52, s. 34–39; idem, *Hybrid vs. Compound War. The Janus Choice: Defining Today's Multifaceted Conflict*, „Armed Forces Journal” 2009, October 1, http://www.armedforces journal.com/hybrid-vs-compound-war [dostęp: 01.04.2015].

[3] R. Kopeć, *Rewolucja w sprawach wojskowych – uniwersalne remedium czy wielka iluzja?*, [w:] *Przeszłość – teraźniejszość – przyszłość. Problemy badawcze młodych politologów*, red. D. Mikucka-Wójtowicz, Kraków 2010, s. 202–204.

[4] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, red. W. Sokała i B. Zapała, Warszawa 2011, s. 10.

pojawienie się aktorów pozapaństwowych, stały się wg współczesnych teoretyków wojskowości wyznacznikiem nowych wojen – wojen XXI wieku. Szczególnie wnikliwie analizowano przebieg dwóch wojen w Zatoce Perskiej oraz agresji NATO na Jugosławię. Eksperci oraz naukowcy rosyjscy doskonale zdawali sobie sprawę z faktu, iż wojny z udziałem wielkich masowych armii to przeszłość, zwłaszcza że rewolucja technologiczna, rozwój systemów precyzyjnego rażenia i przeniesienie pola walki w nowe wymiary (w kosmos oraz cyberprzestrzeń) kompletnie zmieniły postrzeganie zjawiska wojny. Rosjanie uważali, iż ludzkość będzie miała do czynienia z konfliktami i wojnami asymetrycznymi[5], a o hybrydowości konfliktów pisano raczej w odniesieniu do amerykańskiej szkoły myśli wojskowej. Współcześnie granica między regularną i „nieregularną” wojną niewątpliwie uległa zatarciu. Zaniepokojenie przywódców politycznych Federacji Rosyjskiej budziło coraz większe zaangażowanie polityczne i militarne USA – zwłaszcza w strefach, które władze rosyjskie traktują jako swój obszar wpływów. Jednocześnie Rosja rozpoczęła żmudną drogę powrotu do współdecydowania o losach świata i zmiany panującego porządku światowego na bipolarny.

Już wojna w Czeczenii i niestabilna sytuacja w środkowoazjatyckich i kaukaskich limitrofach dowiodły jednak, że Rosja, podobnie jak USA, jest nieprzygotowana do prowadzenia efektywnych działań militarnych w zmienionych warunkach bojowych. Zwłaszcza początkowa faza I wojny czeczeńskiej pokazała, iż przewyższająca technologicznie przeciwnika, regularna armia nie była w stanie rozprawić się z jednostkami nieregularnymi i rebelianckimi. Katastrofa operacji wojsk rosyjskich wpłynęła niekorzystnie nie tylko na sytuację wewnętrzną państwa, lecz również na jego pozycję międzynarodową. Rosjanie długo nie wyciągali żadnych wniosków z klęski. Refleksja przyszła jednak wraz z odsunięciem ludzi Borysa Jelcyna i nowymi porządkami zaprowadzonymi przez Władimira Putina. Niewątpliwie reforma sił zbrojnych zainicjowana za jego prezydentury jest kluczowym elementem obserwowanej od dawna zmiany jakościowej armii rosyjskiej. Przy czym nie należy przeceniać rosyjskich możliwości – zwłaszcza dotyczących organizacji i zarządzania. We wdrażaniu rewolucyjnych planów modernizacyjnych Rosję ograniczają również finanse.

Z kolei eksperci zachodni, analizując konflikt czeczeński, utwierdzili się w przekonaniu, iż wojny przyszłości będą toczone według nowych i zgoła nieprzewidywalnych form i sposobów walki, często łączących taktykę konfliktów regularnych i metody konfliktów nieregularnych, a aktorami będą nie tylko państwa, lecz również (lub przede wszystkim) podmioty pozapaństwowe[6]. W ten sposób wprowadzono do powszechnego dyskursu nowe koncepcje: wojen asymetrycznych i wojen hybrydowych. Przy czym obu ideom przypisano „mityczne” znaczenie, na nowo próbując

[5] Zob. М.А. Гареев, *Война и современное международное противоборство*, „Независимое военное обозрение” 1998, № 1; В.Д. Рябчук, Ю.С. Солнышков, *Военное науковедение и методология решения проблем управления. Военно-теоретический труд*, Москва 1998; В.В. Серебрянников, *Войны России: социально-политический анализ*, Москва, 1999; В.И. Слипченко, *Бесконтактные войны*, Москва 2001.

[6] Pojęcia „działania hybrydowe” oraz „wojna hybrydowa” pojawiły się w 2002 r. w monografii amerykańskiego mjr. Williama J. Nemetha poświęconej wojnie czeczeńskiej: W.J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey, CA 2002, s. 40–42; zob. S. Rusnáková, *Russian New Art of Hybrid Warfare in Ukraine*, „Slovak Journal of Political Sciences” 2017, vol. 17, nr 3–4, s. 346.

wytłumaczyć znane kanony sztuki wojennej, obecnej w dziejach ludzkości co najmniej od czasów starożytnych. Ten swoisty mit wojen (działań) hybrydowych, mający wyjaśniać wydarzenia związane z rzekomo nowymi formami współczesnego wojowania, został natychmiast wykorzystany w związku z konfliktem na Ukrainie.

Według amerykańskiego teoretyka wojskowości Franka G. Hoffmana wojna hybrydowa cechuje się „zbieżnością [...] fizyczną i psychologiczną, kinetyczną i niekinetyczną, bojowników i cywilów [...] sił zbrojnych i społeczności, państw i aktorów niepaństwowych, a także zdolności bojowych, w które są wyposażone”[7]. Inni anglosascy teoretycy bardzo podobnie definiowali zjawisko hybrydowości wojen[8], podkreślając niezwykłość tej koncepcji i w dość dowolny sposób traktując przykłady działań o charakterze hybrydowym w przeszłości. Np. Daniel T. Lasica postrzega hybrydowość jako logiczną kompilację strategii i taktyki, polegającą na wymieszaniu różnych form działań zbrojnych[9], co niestety świadczy o kompletnym niezrozumieniu podstaw sztuki wojennej i jej zasad.

Z kolei Robert G. Walker traktuje hybrydowość jako wynik zbieżności zasad i form łączących wojnę konwencjonalną z operacjami specjalnymi[10]. Podobnie ujmuje hybrydowość John J. Mccuen, który uważa, iż wojna hybrydowa to kombinacja wojny symetrycznej i asymetrycznej (czyli formy konwencjonalnej i nieregularnej)[11].

Wydaje się zatem, że w ocenie anglosaskich ekspertów zjawisko to – chociaż nie nowe – będzie stanowić spore wyzwanie zarówno dla USA, jak i innych państw, zwłaszcza tzw. starych demokracji. Zagrożenia hybrydowe i asymetryczne wskazują, że podmioty niepaństwowe coraz częściej uzyskują dostęp do systemów broni, które do niedawna były wyłączną domeną państw. Z drugiej strony państwa są i będą zmuszone coraz częściej sięgać po niekonwencjonalne strategie (taktykę, formy i metody), mające na celu zwalczanie nieformalnych grup lub organizacji, jak również ograniczanie wpływu mocarstw lub innych silniejszych podmiotów stosunków międzynarodowych[12]. Przy czym wprowadzenie do obiegu naukowego i dyskursu eksperckiego nowych pojęć, np. wojen niepaństwowych, nietrynitarnych, buntowniczych[13], a także negowanie clausewitzowskiej teorii sztuki wojennej

[7] A. Gruszczak, *op. cit.*, s. 13.

[8] Ł. Skoneczny *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego” 2015, wydanie specjalne: *Wojna hybrydowa*, s. 40.

[9] D.T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, Fort Leavenworth 2009, s. 11.

[10] Walkera należy uznać za prekursora współczesnych badań nad zjawiskiem hybrydowości pola walki. Opisując ekspedycyjną zdolność Korpusu Piechoty Morskiej, określił go jako „hybrydową siłę w trakcie wojny hybrydowej”. Według Walkera „wojna hybrydowa jest zjawiskiem leżącym między wojną specjalną i konwencjonalną”, zob. F.B. Steder, *Introduction: The Theory, History, and Current State of Hybrid Warfare*, „Combating Terrorism Exchange (CTX)” 2016, vol. 6, nr 4, s. 8.

[11] Zob. A. Gruszczak, *op. cit.*, s. 13.

[12] F.G. Hoffman, *Hybrid Warfare…*, s. 39.

[13] Pojęcie „wojny buntownicze” nawiązuje do koncepcji rosyjskiego białogwardyjskiego pułkownika, emigracyjnego publicysty i teoretyka wojskowości Jewgienija Messnera. Zauważył on (swoje hipotezy opierał na koncepcji Samuela P. Huntingtona), że od lat 60. ubiegłego wieku następują jakościowe i ilościowe zmiany w obszarze wojen i konfliktów. Według jego teorii powstania, rewolucje i wyzwalanie się państw kolonialnych doprowadziły do ewolucji działań nieregularnych, które wraz z takimi czynnikami jak manipulacja społeczna, perswazja, działania psychologiczne i dezinformacja oraz dywersja będą miały coraz większe znaczenie w narastającym konflikcie. Niektórzy z polskich naukowców (Leszek Sykulski, Kazimierz Kraj) mocno akcentują znaczenie koncepcji Messnera, stawiając ją w roli paradygmatu przyszłych, postzimnowojennych konfliktów, nie bacząc, iż w jego wywodach nie ma nic nowego, jeśli chodzi o teorię wojen i wojskowości, zob. np. K. Kraj, *Wojny asymetryczne czy* miatieżewojna *Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku*, „Bezpieczeństwo. Teoria i Praktyka” 2012, nr 3, s. 33–39; L. Sykulski, *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera*, „Przegląd Geopolityczny” 2015, t. 11, s. 103–112; *Хочешь мира, Победи мятежевойну! Творческое наследие Е.Э. Месснера*, Под общей редакцией В.И. Марченкова, Москва 2005, http://militera.lib.ru/science/0/pdf/messner_ea01.pdf [dostęp: 12.01.2019]; *Мятежевойна*, „Независимое военное обозрение”, 5.11.1999, http://nvo.ng.ru/ history/1999-11-05/7_rebelwar.html [dostęp 12.01.2019]; И.В. Домнин, А.Е. Савинкин, *Асимметричное воевание*, „Отечественные записки” 2005, № 5, http://magazines.russ.ru/oz/2005/5/2005_5_5.html [dostęp: 12.01.2019].

powoduje zamęt definicyjny i tym samym szkodzi współczesnym badaniom polemologicznym, czyli nad zjawiskiem wojny i pokoju[14].

Niewątpliwie w odniesieniu do współczesnych konfliktów militarnych (wojen) hybrydyzację pola walki należy rozumieć jako współistnienie starych i nowych metod (form) prowadzenia działań bojowych, czyli klasycznych, konwencjonalnych sposobów wspartych systemami nowych technologii, gdzie radiotelefon jest równie przydatny jak urządzenia GPS. Zatem obok siebie funkcjonują prymitywne narzędzia walki oraz najnowocześniejsze systemy uzbrojenia i wyposażenia. Zauważalna jest również swoista symbioza pomiędzy klasycznymi formami działań taktycznych i operacjami specjalnymi, które mogą być dodatkowo wsparte niekonwencjonalnymi metodami działań bojowych.

Z pozoru wydaje się, że wojny hybrydowe są rozwinięciem idei wojen asymetrycznych. Jeśli jednak weźmiemy pod uwagę fakt, iż wojny hybrydowe wg zachodnich koncepcji stanowią konglomerat różnych działań łączących w sobie walkę konwencjonalną oraz nieregularne jej formy z wykorzystaniem najnowszych technologii (zwłaszcza informatycznych i sieciocentrycznych), to z pewnością *novum* tych wojen będzie się odnosiło do rosnącej aktywności potencjalnych aktorów konfliktu w cyberprzestrzeni.

Czy w tym kontekście można zatem mówić, iż Rosja w czasie konfliktu ukraińskiego faktycznie zastosowała jakieś nowe metody prowadzenia wojny[15]?

We wstępie do edycji czasopisma „The Military Balance” (wydawanego przez Międzynarodowy Instytut Badań Strategicznych) z 2015 r., rosyjska wojna hybrydowa została opisana jako

> działania obejmujące wykorzystanie narzędzi wojskowych i niewojskowych w zintegrowanej kampanii mającej na celu zaskoczenie, przejęcie inicjatywy i uzyskanie korzyści psychologicznych i fizycznych przy użyciu środków dyplomatycznych, informacyjnych, operacji cybernetycznych, a także tajnych i okazjonalnie jawnych działań wojskowych, wywiadowczych (agenturalnych), a ponadto nacisków o charakterze ekonomicznym[16].

[14] Ch. Bassford, *Na palcach wokół trójcy Clausewitza*, tłum. S. Górka, „Kwartalnik Bellona” 2017, nr 1, s. 93–98.

[15] K. Grabowska, *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, „Świat Idei i Polityki” 2015, t. 14, s. 270–273.

[16] *Editor's Introduction. Complex crises call for adaptable and durable capabilities*, „The Military Balance” 2015, s. 5, https://www.tandfonline.com/doi/pdf/10.1080/04597222.2015.996334 [dostęp:

Definicja ta jest zgodna z poglądami panującymi na Zachodzie, określającymi współczesne metody prowadzenia polityki przez Kreml. Jest ona też bliska poglądom wyrażanym przez dość liczną grupę ekspertów i polityków blisko związanych z Putinem i jego współpracownikami. Przykładem niech będzie jeden z autorów rosyjskiego postrzegania wojny, bliski doradca Putina – Władysław Surkow, który wg zachodnich źródeł wprowadził do obiegu naukowego i publicystycznego pojęcie „wojny nielinearnej" [*non-linear war*][17]. „W starych wojnach XIX i XX wieku walczyły dwie strony. Teraz wszyscy są przeciwko wszystkim"[18] – cytaty z eseju Surkowa stały się podstawą do głoszenia tezy, iż Rosjanin jest autorem nowej teorii prowadzenia działań wojennych. Jego wystąpienie, mające naturę publicystyczną, zostało skrzętnie wykorzystane zwłaszcza w kontekście udziału Rosji w konflikcie ukraińskim. Stanowić miało niepodważalny dowód na istnienie jakieś rosyjskiej nowej formy wojowania.

Wnikliwa analiza wydarzeń związanych z konfliktem ukraińskim, a także licznie pojawiające się oceny i raporty dotyczące udziału w nim Rosji spowodowały, iż zaczęto poszukiwać jakiegoś nowego *modus operandi* w działaniach przywódców politycznych i dowódców rosyjskich. Pierwszym znaczącym sygnałem miała być tzw.

12.01.2019]; zob. M. Galeotti, *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right*, b.m.w. 2016, s. 19; A. Gorzkowicz, *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1, s. 148. (Tłumaczenia zawartych w artykule cytatów: A. Krzak).

17 Zob. J.R. Haines, *Russia's Use of Disinformation in the Ukraine Conflict*, FPRI, E-Notes, February 17, 2015, s. 2, https://www.fpri.org/docs/haines_on_disinformation.pdf [dostęp: 12.01.2019]. Pierwszy raz termin ten pojawił się w eseju *Без неба*, opublikowanym przez Surkowa pod pseudonimem Natan Dubowickij na stronie Русский пионер 12 marca 2014 r.: „Писатель Натан Дубовицкий, известный своими романами «Околоноля», «Машинка и Велик» и повестью «Дядя Ваня», написал рассказ «Без неба». Рассказ о пятой мировой войне — первой нелинейной войне, где все воевали против всех. Интерпретаций может быть много — особенно сегодня, когда настроения в обществе уж точно нельзя назвать простыми и двухмерными. Андрей Колесников, главный редактор журнала «Русский пионер»". Do działań nielinearnych nawiązywał również gen. mjr Wasilij Rezniczenko pod koniec istnienia Związku Radzieckiego. Zasadnicza część używanych przez naukowców i ekspertów Zachodu definicji pochodzi z analizy artykułu rosyjskiego gen. Walerija Gierasimowa z 27 lutego 2013 r. Według Marka Galeottiego, Michaela Kofmana, Matthew Rojansky'ego czy Tada A. Schnaufera, artykuł ten ma opisywać fundamenty wojny nielinearnej. Pojęcie „nielinearności" przedstawia konflikt, w którym na obszarze działań wojennych nie ma wyraźnych linii frontu i teatrów działań militarnych. Wojna nielinearna opiera się zatem na subwersji, podziale społecznej i politycznej struktury, umożliwiającym agresorowi realizację założonych celów z wykorzystaniem środków pozamilitarnych, zob. T.A. Schnaufer, *Redefining Hybrid Warfare: Russia's Non-linear War against the West*, „Journal of Strategic Security" 2017, vol. 10, nr 1, s. 19–22, 24; B. Perry, *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations*, Small Wars Journal, https://smallwarsjournal.com/index.php/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera [dostęp: 12.01.2019]; M. Tarnawski, *Rosyjska koncepcja konfliktu nielinearnego*, [w:] *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, red. Ł. Jureńczyk, S. Sadowski, M. Jastrzębski, J. Waskan, Bydgoszcz 2016, s. 54.

18 „Vladislav Surkov's use of the term *non-linear war* exemplifies how Russian theorists characterize 21st century warfare. He wrote, «The old wars of the 19th and 20th centuries involved two sides. Now, it is all against all»", J.R. Haines, *op. cit.*, s. 2; zob. też J. Bērziņš, *Russian New Generation Warfare is not Hybrid Warfare*, [w:] *The War in Ukraine: Lessons for Europe*, red. A. Pabriks, A. Kudors, Rīga 2015, s. 42.

doktryna Gierasimowa, która za sprawą Marka Galeottiego niestety na trwale weszła do obiegu publicystycznego i naukowego. Ta wypaczona analiza wykładu (i artykułu) szefa sztabu Generalnego Rosji gen. płk. Walerija Gierasimowa[19] spowodowała, iż liczne grono ekspertów uważa, że Rosjanie mieli wprowadzić w życie nową doktrynę wojenną[20] i – co istotniejsze – przetestować ją w praktyce. Pogląd ten wciąż funkcjonuje, pomimo krytycznego stanowiska wielu ekspertów i naukowców[21], i najprawdopodobniej na stałe zagości w literaturze przedmiotu, skutecznie dezinformując odbiorców i wprowadzając chaos w badaniach naukowych.

Niewątpliwie w próbach zrozumienia rosyjskiego sposobu widzenia zjawiska wojny czy sztuki wojennej największym błędem zachodnich teoretyków jest jego rozpatrywanie w ramach zachodnioeuropejskich doświadczeń i metodologii badań w obszarze wojen, konfliktów i – w szerszym ujęciu – polemologii jako nauki o wojnie. „Hybrydowość" – oznaczająca mieszankę różnych elementów – w ujęciu teorii wojowania jest niezwykle pożądanym i chwytliwym pojęciem. Jednak ze względu na to, że jest to pewna koncepcja militarna i jednocześnie efekt amerykańskiej myśli wojskowej, jej podstawowe ramy metodologiczne w znacznym stopniu różnią się rosyjskich poglądów na teorię współczesnych konfliktów. Dlatego też jakakolwiek próba przypisywania rosyjskim poglądom amerykańskiego punktu widzenia współczesnych wojen jest niczym innym jak podstawowym, wręcz elementarnym

19 В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер", 27.02.2013, № 8, s. 2–4; idem, *Роль Генерального штаба в организации обороны страны в соответствии с новым Положением о Генеральном штабе, утверждённым Президентом Российской Федерации*, „Вестник Академии военных наук" 2014, № 1, s. 14–23; М.А. Гареев, *Итоги деятельности Академии военных наук за 2013 год и задачи академии на 2014 год*, „Вестник Академии военных наук" 2014, № 1, s. 7–14.

20 Galeotti zatytułował swój opublikowany wiosną 2013 r. na blogu artykuł *Gerasimov Doctrine*. Przedstawione w nim oceny i komentarze były powierzchowne i niepoparte żadnymi argumentami. Wielu naukowców, ekspertów i polityków twierdziło następnie, iż tzw. doktryna Gierasimowa jest „nowym typem wojny", „rozszerzoną teorią współczesnej wojny", a nawet „ideą wojny totalnej" *made in Russia*. Jednak nawet z pobieżnej analizy dostępnego materiału jasno wynika, iż nie ma takiej doktryny ani idei. Przyznał to sam Galeotti, który w 2014 r. tłumaczył, że chodziło mu tylko o „chwytliwy tytuł", a sama „doktryna" nie istnieje, M. Galeotti, *„The 'Gerasimov Doctrine' and Russian Non-linear Warfare"*, Moscow's Shadows, July 6, 2014 https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war [dostęp: 12.01.2019]; idem, *Służby wywiadowcze Rosji są w stanie (politycznej) wojny*, Przegląd NATO, 12/05/2017, https://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/PL/index.htm [dostęp: 12.01.2019]. Problem w tym, że dopóki udajemy, że istnieje, to faktycznie będzie nam ona przesłaniała prawdziwą naturę zagrożeń, jakie niesie polityka Rosji wobec Europy, zwłaszcza Środkowej. Podobną refleksję w 2018 r. wyraził zresztą Galeotti, który dodał: „Wierzę, że mam prawo to powiedzieć, ponieważ, ku mojemu wielkiemu zirytowaniu, wymyśliłem ten termin [„doktrynę Gierasimowa" – przyp. AK.], który od tego czasu zaczął żyć własnym niszczycielskim życiem…", idem, *I'm Sorry for Creating the 'Gerasimov Doctrine'*, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [dostęp: 12.01.2019]. Również Jolanta Darczewska w swoim artykule wspomina o „doktrynie Gierasimowa" w kontekście wojny hybrydowej, w rozwinięciu refleksji nad nowymi wojnami. Jest to kolejna błędna analiza, wypaczająca naturę wystąpienia Gierasimowa. Niestety, interesujący artykuł Darczewskiej zawiera dość liczne błędy i niezweryfikowane źródła, J. Darczewska, *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18, s. 42–43 *et passim*.

21 S. Rusnáková, *op. cit.*, s. 343–345.

błędem metodologicznym, zakładającym, iż rosyjskie rozwiązania praktyczne i teoretyczne muszą być spójne z poglądami prezentowanymi przez zachodnioeuropejskich badaczy i ekspertów – tak jakbyśmy mieli do czynienia z tym samym sposobem myślenia, kulturą i rozwojem teorii strategicznej, jak również identycznymi poglądami na formy prowadzenia działań wojennych we współczesnej Rosji oraz na Zachodzie, zwłaszcza w Stanach Zjednoczonych. Nic bardziej mylnego. Fakt, że Rosjanie poświęcają dużo czasu na wnikliwe studia i analizę opracowań amerykańskich i zachodnich teoretyków i ekspertów z zakresu szeroko rozumianego bezpieczeństwa i wojskowości jest przejawem naturalnej działalności środowisk akademickich i eksperckich w Rosji (podobnie było w okresie istnienia ZSRR). Służy to przede wszystkim poznaniu sposobu myślenia i kultury strategicznej przeciwnika, a zwłaszcza uzyskaniu wiedzy o jego słabych i mocnych stronach, a tym samym – budowaniu własnych rozwiązań doktrynalnych i (ewentualnej) przewagi w wymiarze taktycznym i strategicznym.

Ten punkt widzenia w rosyjskiej myśli strategicznej jest rozwijany i pielęgnowany od czasów carskich i nie należy się łudzić, iż Rosjanie kiedykolwiek zmienią swoje poglądy i postępowanie. Zachód, chcąc w jakiś logiczny sposób wytłumaczyć wydarzenia na Wschodzie (zwłaszcza rebelię i aneksję Krymu, a *de facto* rozpad państwa ukraińskiego), postanowił przedstawić je opinii społecznej jako zamierzone działania Kremla mające na celu rozbicie i przejęcie kontroli nad suwerennym państwem, z wykorzystaniem narzędzi właściwych dla nowego typu wojen. W odpowiedzi strona rosyjska zaprzeczała swojemu udziałowi w konflikcie[22] oraz oskarżyła, iż Zachód „to coś" (wojnę hybrydową) stosuje wobec Rosji[23]. Można byłoby stanowisko Rosji podsumować stwierdzeniem, iż najlepszą obroną jest atak oraz że takie postępowanie jest charakterystyczne dla Kremla. Jednak aby dokonać obiektywnej analizy wydarzeń na Ukrainie, należy wziąć pod uwagę historyczne doświadczenia, a działania Rosji postrzegać w dużo szerszym kontekście niż ten zaproponowany przez anglosaski punkt widzenia. Wydaje się, że Zachód zapomniał, iż przynajmniej od dekady rosyjscy eksperci, wojskowi i politycy snuli rozważania na temat przyszłych wojen. Uważali, podobnie jak Gierasimow, iż będą to konflikty z użyciem broni precyzyjnego rażenia, bezkontaktowe, ze znacznym udziałem

[22] Eksperci i autorzy rosyjscy opisywali zjawisko hybrydowości nowych wojen w kontekście rozważań konceptualnych pojawiających się w zachodnioeuropejskiej myśli wojskowej, zob. np. А. Бартош, *Гибридные войны в стратегии США и НАТО*, Центр анализа террористических угроз (ЦАТУ), 23.10.2014, http://catu.su/analytics/874-gibridnye-vojny-v-strategii-ssha-i-nato [dostęp: 12.01.2019]; idem, *Философия гибридной войны. Сравнительный анализ моделей гибридной войны и цветной революции*, Viperson, 13.10.2016, http://viperson.ru/articles/filosofiya-gibridnoy-voyny-sravnitelnyy-analiz-modeley-gibridnoy-voyny-i-tsvetnoy-revolyutsii [dostęp: 12.11.2016]; idem, *Гибридные войны будущего – прогнозирование и планирование. Как учесть новые угрозы в Военной доктрине России*, „Независимого военного обозрения", 19.12.2014, http://nvo.ng.ru/concepts/2014-12-19/1_war.html [dostęp: 28.12.2016]; А.В. Манойло, *Гибридные войны и цветные революции в мировой политике*, „Право и политика" 2015, № 7, s. 918–929; В. Горбулин, *„Гибридная война" как ключевой инструмент российской геостратегии реванш*, ZN.UA, 26.01.2015, http://zn.ua/columnists/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-165061_.html [dostęp: 22.12.2018].

[23] A. Monaghan, *Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare'*, „Parameters" 2015–2016, vol. 45, nr 4, s. 67.

czynników pozapaństwowych[24]. Celem będzie nie fizyczne unicestwienie wojsk, lecz destrukcja ekonomiczna i polityczna przeciwnika[25]. Rosja też nigdy nie zrezygnowała z walki o pozycję dominującą lub współdecydującą w globalnych stosunkach międzynarodowych i zmierza do powrotu do *status quo* sprzed 1989 r.[26].

Należy pamiętać, że Rosja, planując wcześniej działania destabilizujące na Ukrainie, z pewnością wykorzystała przede wszystkim swoje doświadczenia, a nie założenia pochodzące z zachodnich koncepcji – od ponad 100 lat w rosyjskiej myśli wojskowej toczono bowiem rozważania nad różnymi formami działań destrukcyjnych o charakterze innym niż klasyczne, konwencjonalne operacje wojskowe[27]. Rosyjscy teoretycy wojskowości, a także eksperci polityczni i ideolodzy prowadzili badania nad efektywnym połączeniem wszystkich elementów (wojskowych i pozamilitarnych) aktywnej gry politycznej z korzyścią dla Matki Rosji – czy to rządzonej przez Romanowów, czy to bolszewickiej satrapii. Dlatego też Gierasimow mówił o nowych formach współczesnych wojen i konfliktów militarnych, i jednocześnie przekazał jasny sygnał, że Rosja jest gotowa do takiej formy wojowania i prowadzenia polityki. I to było istotą jego wystąpienia. A to, że posiłkował się metodologią i terminologią używaną przez zachodnich ekspertów, nie powinno dziwić, ponieważ jego przekaz musiał być zrozumiały dla Zachodu. Dlatego też należy się zgodzić z głównymi wnioskami Michała Wojnowskiego, który twierdził, iż wystąpienie Gierasimowa nie jest żadną doktryną czy strategią Rosji w obszarze militarnym, lecz działaniem o charakterze informacyjno-psychologicznym. Zwłaszcza że skrupulatna analiza licznych artykułów i opracowań pojawiających się na rynku wydawniczym

[24] Według rosyjskich ekspertów i teoretyków sztuki wojennej, praktyka wojskowa intensywnie weryfikuje koncepcje wojen kolejnej, VI generacji, które fundamentalnie różnią się od wojen przeszłości. W wojnach VI generacji zasadnicza rola przypada broni precyzyjnego uderzenia i obrony, a nie jak w przeszłości – masowym armiom. Cały potencjał uderzeniowy będzie skierowany na całkowite sparaliżowanie obiektów gospodarki przeciwnika poprzez wykonanie silnych uderzeń lotniczych i zmasowanych uderzeń broni precyzyjnego rażenia, różnorodnego bazowania, w warunkach globalnej lub regionalnej walki informacyjnej, zob. И. Капитанец, *Битва за мировой океан*, Москва 2002, s. 50–51.

[25] *Ibidem*, 56–57.

[26] Cele Federacji Rosyjskiej jednoznacznie zdefiniował były wicepremier Dmitrij Rogozin w 2013 r.: „Zadania dla współczesnej Rosji: stworzenie warunków pozwalających na spokojny i absolutnie bezpieczny rozwój kraju, poprzez stworzenie całkowicie bezpiecznego dla niej otoczenia; […] podniesienie prestiżu kraju. *Smart power* i *soft power* – dobre i właściwe określenia, ale prawdziwy *power*, z czym rzeczywiście się liczą – to siła oddziaływania fizycznego, kiedy zachodzi wysokie prawdopodobieństwo otrzymania uderzenia stalową pięścią w oko. Jest to siła, która najwyżej ceniona jest w tzw. cywilizowanym świecie. Trzeba nauczyć się rozpychać łokciami, ale nie dla samego rozpychania się, ale po to, aby osiągać swoje wyznaczone cele strategiczne", *В зоне персональной ответственности. Беседа с вице-премьером Правительства РФ Дмитрием Рогозиным*, [w:] *Завтра война! Вооруженные силы и военная реформа в России*, ред. А. Проханов, А. Нагорный, В. Шургин, Москва 2013, s. 30.

[27] Mit rosyjskich wojen hybrydowych niewątpliwie skutecznie obala Michał Wojnowski w swoich artykułach, zob. M. Wojnowski, *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13; idem, *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*; idem, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

w Rosji powinna już dawno uświadomić zachodnim analitykom wywiadu, iż Rosjanie z uwagą śledzą zmiany, jakie w ostatnich latach zachodzą w naukach o bezpieczeństwie oraz teorii i praktyce prowadzenia wojen. W rosyjskiej literaturze przedmiotu znajdujemy liczne odniesienia do historii, sztuki wojennej i doświadczeń z przeszłości, co pokazuje znaczenie tego sektora dla badań nad współczesną wojskowością i jego wpływ na rosyjską myśl wojskową i kulturę strategiczną. Dlatego też twierdzenia części ekspertów (np. Jolanty Darczewskiej), iż „małe wojny" są zjawiskiem amorficznym, sugeruje, iż nie rozumieją oni albo nie znają rosyjskich poglądów w obszarze szeroko rozumianej wojskowości i bezpieczeństwa[28].

Między *Małą wojną* M.A. Drobowa a teorią konfliktów hybrydowych Zachodu

Z pewnością to nie Amerykanie wymyślili wykorzystanie partii komunistycznych do zaprowadzenia nowego porządku poprzez wywołanie rebelii (rewolucji), lecz bolszewicy, którzy manipulując partiami socjalistycznymi i robotnikami, stworzyli wielomilionową armię posłusznych sobie informatorów oraz potencjalnych sabotażystów. Przykładów z zakresu organizacji i prowadzenia różnych form działań niekonwencjonalnych w rosyjskiej sztuce wojowania i uprawiania polityki znajdziemy tak wiele, że nie sposób ich przedstawić i omówić w jednym artykule. Dlatego też do wszelkich nowinek i prób zrozumienia Rosji przez pryzmat doświadczeń nauki i kultury Zachodu należy podchodzić z dużą dozą ostrożności, to bowiem, co wydaje się oczywiste na Zachodzie, wcale nie musi takie być w Rosji. Rosyjskie rozumienie wojen przyszłości jednak tak dalece nie odbiega od idei zachodnich teoretyków. Moskwa dopasowuje swoje doświadczenia do dorobku Zachodu, dlatego zjawisko „hybrydowości" w rosyjskim wykonaniu powinno być rozpatrywane m.in. przez pryzmat niezwykle ciekawej i wciąż ewoluującej teorii „małej wojny", jako szerokiego i złożonego zjawiska będącego podstawą różnych pochodnych form militarnego i pozamilitarnego oddziaływania na potencjalnego przeciwnika (m.in. współczesnych form wywiadu aktywnego, ukształtowanego w latach 20. XX w.).

We współczesnym rozumieniu „małe wojny" są najczęściej prowadzone pomiędzy asymetrycznie upodmiotowionymi przeciwnikami: tym potężniejszym, posiadającym znaczny potencjał militarny, i tym, który pozornie nie dysponuje możliwościami toczenia równorzędnej walki. Nie oznacza to jednak, że „małe wojny" muszą angażować ograniczone zasoby i małe jednostki. Na przykład „Wietnam" jest uważany przez część ekspertów za „małą wojnę", przy czym konflikt ten w żaden sposób nie był „mały" w konwencjonalnym znaczeniu tego słowa. Paradoksalnie, „małe wojny" mogą być dość „duże", jeśli będziemy je mierzyć wielkością użytych sił, liczbą ofiar śmiertelnych lub wielkością wydatkowanych środków. Istotny dla naszych rozważań będzie kontekst polityczny. Będzie on bowiem determinował charakter konfliktu o wiele bardziej niż teoretyczne lub faktyczne zdolności wojskowe uczestników starcia.

[28] *Ibidem*, s. 42.

W historycznym ujęciu działania realizowane w ramach „małych wojen" mają równie długie dzieje jak klasyczny konflikt lub wojna. Jedną z pierwszych definicji pozostawił brytyjski oficer kolonialny Charles Callwell:

> [małe wojny] są to wszystkie inne kampanie, w których spotykają się nierówni przeciwnicy […]. Obejmują wyprawy przeciwko dzikim i półcywilizowanym rasom realizowane przez zdyscyplinowanych żołnierzy […], kampanie podjęte w celu stłumienia zbuntowanych i prowadzących partyzanckie działania wojenne we wszystkich częściach świata, gdzie zorganizowane armie walczą z przeciwnikami, których nie spotkają w otwartym polu[29].

Z kolei Carl von Clausewitz uważał, że wojna partyzancka („mała wojna") jest pomocniczą formą dla działań sił głównych, a jej celem jest umiejętne stawianie oporu agresorowi. Oddziały partyzanckie powinny być wykorzystywane poza zasadniczym teatrem działań, najczęściej na skrzydłach i zapleczu przeciwnika. Clausewitz przedstawiał partyzantów jako „mglistych i nieuchwytnych", których opór „nie powinien nigdy materializować się jako konkretne ciało". W przeciwnym razie zostaną łatwo rozbici przez siły regularne[30].

Pojęcie „mała wojna" wyszło jednak z obiegu naukowego oraz z wojskowego piśmiennictwa teoretycznego na długo przed wybuchem największych konfliktów w dziejach ludzkości[31]. W jej miejsce na trwale wpisały się natomiast działania partyzanckie i ich formy, czyli powstania, rewolucje, ruchy narodowo-wyzwoleńcze, ruch oporu, operacje półwojenne (lub półwojskowe), a także działania specjalne (wojna specjalna[32]) i inne. Jednak swoista „niepopularność" pojęcia „mała wojna" jest zrozumiała. Dzieje ruchów antykolonialnych są bowiem ściśle związane z walką o niepodległość, którą uzyskano w wielu przypadkach dzięki działaniom partyzanckim, różnym formom dywersji, sabotażu, terroryzmowi i innym metodom przypisywanym „małej wojnie" (współcześnie nie wiedzieć dlaczego – wojnom hybrydowym). Należy pamiętać, iż większość zrodzonych w okresie zimnej wojny teorii wojen partyzanckich, ruchów narodowowyzwoleńczych i rewolucyjnych (Che Guevary czy Mao Zedonga) była badana, ale także celowo wypaczana. Według

[29] Cyt. za: S. Kalyanaraman, *Conceptualisations of Guerrilla Warfare*, „Strategic Analysis" 2003, vol. 27, nr 2, s. 172.

[30] C. von Clausewitz, *O wojnie*, tłum. A. Cichowicz, L. Koc, F. Schoener, Lublin 1995, s. 613–617.

[31] Wyjątek stanowi definicja zamieszczona w Podręczniku Korpusu Piechoty Morskiej USA z 1940 r., zatytułowanym *Small Wars Manual*: „Termin «mała wojna» jest często nieprecyzyjnym określeniem wielu różnych operacji wojskowych. W odniesieniu do Stanów Zjednoczonych, «małe wojny» to operacje podejmowane przez władzę wykonawczą, w których siła militarna jest połączona z presją dyplomatyczną w stosunku do innego państwa [lub innych państw], którego rząd jest uznany za niestabilny, niebezpieczny lub zagrażający interesom lub racji stanu USA", *Small Wars Manual. U.S. Marine Corps*, Washington 1940, s. 1.

[32] Warto zwrócić uwagę na jugosłowiańską teorię wojny specjalnej (*specijalni rat*), współcześnie zapomnianą i bagatelizowaną zarówno przez ekspertów, jak i teoretyków wojskowości, a mającą wiele wspólnych elementów z teoretycznymi podstawami wojen hybrydowych w ujęciu zachodnioeuropejskim, zob. A. Krzak, M. Kuś, *„Specijalni Rat" („wojna specjalna") w koncepcjach jugosłowiańskiej teorii powszechnej obrony narodowej jako forma zagrożeń asymetrycznych w latach 1970–1990*, [w:] *Asymetryczne Bałkany. Działania asymetryczne, militarne i polityka bezpieczeństwa na Półwyspie Bałkańskim w XX i XXI wieku*, red. D. Gibas-Krzak, Częstochowa 2015, s. 83–109.

rosyjskich teoretyków (m.in. M.A. Drobowa) pojęcie „mała wojna" z metodologicznego punktu widzenia powinno pełnić funkcję pojęcia ogólnego względem innych form, które należy scharakteryzować jednocześnie jako specjalne i indywidualne. Według Drobowa jest ona połączeniem zarówno szeroko rozumianej wojny partyzanckiej, jak i działań dywersyjnych. Przy czym dywersję rosyjski myśliciel rozumiał znacznie szerzej, niż wskazuje jej klasyczna definicja[33]. W jego ujęciu dywersja to zarówno terror, jak i sabotaż, propaganda oraz dezinformacja[34]. Drobow uważał, iż walka partyzancka jest f o r m ą „małej wojny", a dywersja to jedynie s p o s ó b[35]. Odpowiednio i zawczasu przygotowana akcja dywersyjna z pewnością w okresie konfliktu przyniesie wymierne korzyści broniącej się stronie. Może też być prowadzona w okresie poprzedzającym konflikt lub zmierzać do destabilizacji państwa wroga, bez wywoływania wojny i angażowania się w działania militarne. Ten pogląd, aktualny w latach 20. XX w., z powodzeniem został zatem przeniesiony na Ukrainę drugiej dekady XXI w.

Ze względu na upływ czasu oraz rozwój technologiczny, wprowadzenie nowych systemów uzbrojenia i wyposażenia, może nam się wydawać, iż przyjęcie rozważań nad paradygmatem „małej wojny" jako podstawy badań nad współczesnymi konfliktami o charakterze hybrydowym prowadzi na manowce. Należy zauważyć, iż Rosjanie od dłuższego czasu wspominają o zmianach zachodzących zarówno w środowisku konfliktu i wojny, jak i samej walki zbrojnej. Co więcej, analiza wojskowego piśmiennictwa opublikowanego w Rosji w ostatnich dwóch dekadach pokazuje, iż powstało co najmniej kilkadziesiąt interesujących prac, które w mniejszym lub większym zakresie omawiają kwestie związane ze zmiennym charakterem przyszłych konfliktów, jednak nie zaburzają paradygmatu teorii wojny Clausewitza. W pracy *Завтра война!* [Jutro wojna!] rosyjscy eksperci już w pierwszej dekadzie XXI w. przewidywali, iż

> [przyszłe wojny to] przede wszystkim zdalne i „bezkontaktowe" destabilizacje funkcjonowania struktur zarządzania i dowodzenia [innego państwa] przez stronę atakującą, inicjowanie rozpadu jego elit politycznych, naruszenie jego stabilności socjalnej poprzez połączenie operacji wywrotowych o charakterze propagandowo-psychologicznym, ekonomicznym i specjalnym[36].

Nie jest to ani definicja Hoffmana, ani Galeottiego, lecz zapowiedź tego, co czeka świat – wg prognoz znanych rosyjskich polityków, wojskowych i ekspertów

[33] Dywersja – działania niszczące lub osłabiające systemy obronne (militarne), gospodarcze, a także polityczne przeciwnika, realizowane w czasie wojny, konfliktu lub w okresie pokoju poprzedzającym stan wojny. Głównym ich celem jest dezorganizacja przeciwnika, osłabienie jego morale oraz niszczenie zasobów materiałowych. Wyróżniamy następujące rodzaje dywersji: militarną (wojskową), polityczną, gospodarczą, ideologiczną. Jedną z form dywersji może być sabotaż.

[34] М.А. Дробов, *Малая война. Партызанство и диверсии*, Б.м., 1998, s. 13.

[35] *Ibidem*. Dlatego też ze zdumieniem należy odczytać słowa J. Darczewskiej mówiące o jakimś amorfizmie *małej wojny*. Świadczy to o braku znajomości literatury przedmiotu i subiektywnej ocenie przedstawionej przez bądź co bądź osobę uchodzącą za eksperta w dziedzinie szeroko rozumianej problematyki bezpieczeństwa współczesnego państwa rosyjskiego, J. Darczewska, *op. cit.*, s. 42.

[36] *Россия-XXI: военный вектор. Доклад Изборского клуба по военному вопросу*, [w:] *Завтра война! Вооруженные силы…*, s. 44–45.

– w nieodległej przyszłości. Jest to pogląd zbliżony do teoretycznych rozważań, jakie kreślili w latach 20. ubiegłego wieku bolszewiccy teoretycy rewolucji[37]. Nikt z rosyjskich ekspertów wówczas nie przypuszczał, iż w niedalekiej przyszłości dojdzie do eskalacji konfliktu na Ukrainie, który negatywnie wpłynie na pozycję Rosji w stosunkach międzynarodowych. Rosja jest przeświadczona, iż otoczona jest przez samych wrogów, którzy chcą ją upokorzyć i zniszczyć[38].

Podsumowanie

Wydawałoby się, że po rozpadzie ZSRR zadany został ostateczny, druzgocący cios sektorowi bezpieczeństwa pierwszego państwa robotników. Pomimo „smuty Jelcynowskiej", wewnętrznego chaosu i utarty pozycji mocarstwa globalnego, nowa Rosja rozpoczęła żmudną drogę powrotu do poprzedniego statusu. Stosunkowo szybko odbudowano służby specjalne i nadano nowy kształt administracji oraz siłom zbrojnym. Nie zmieniły się tylko metody i sposoby prowadzenia polityki. Cel pozostał jasny: Rosji ma zostać przywrócona rola i miejsce przynajmniej takie, jakie państwo zajmowało w dobie zimnej wojny. Model polityki, który Rosja postanowiła narzucić wschodniej Europie, a także Zachodowi (Stanom Zjednoczonym oraz Unii Europejskiej), odzwierciedlający zderzenie, konflikt cywilizacji, jest jednym z elementów jej strategii, której głównym celem jest zmiana układu sił w ujęciu globalnym. I aby to uzyskać, Kreml sięgnie po wszelkie dostępne narzędzia, nawet te, które wydawałyby się amorficzne. W ten scenariusz doskonale wpisują się „małe wojny", które jak wiele innych idei (teorii/form) ewoluowały, przyjmując nowe oblicze w zmienionych warunkach. Jednak stosują te same zasady, co przed prawie wiekiem. Z pewnością nagromadzenie pojęć i definicji odnoszących się do tzw. działań asymetrycznych, hybrydowych, kompozytowych i innych prowadzi do wymieszania zjawisk na poziomie strategicznym i taktycznym, a co za tym idzie – do zacierania różnic między dwiema odrębnymi formami działań. Część badaczy nie dostrzega różnicy między „małą wojną" a współczesnymi teoriami „małych wojen", uważając je za zjawiska przestarzałe lub wręcz amorficzne. Prowadzi to do chaosu i niepotrzebnych poszukiwań, tworzenia nowych „superteorii", które miałyby w praktyce pomóc rozwiązać liczne dylematy narosłe wokół amerykańskiego przywództwa.

[37] Pierwszym z bolszewickich przywódców, który uważał, że przyszłe wojny będą miały charakter masowy, manewrowy oraz będą kombinacją różnych form działań (nieregularnych i regularnych), był Michaił Frunze. W 1921 r. w artykule pt. *Jedna doktryna wojenna i Armia Czerwona* powrócił do koncepcji „małej wojny", dostosowanej do warunków, sztuki wojennej i rozwoju technologicznego właściwego dla końca drugiej dekady XX w. Rozwinął teoretyczne zasady tworzenia systemu podziemia opartego na oddziałach partyzanckich. Jego poglądy zostały rozwinięte przez Drobowa, zob. В.В. Квачков, *Спецназ России*, Военная литература, 2004, http://militera.lib.ru/science/kvachkov_vv/index.html [dostęp: 12.03.2019].

[38] Ten zabieg nadal jest skutecznym narzędziem, przede wszystkim w polityce wewnętrznej – tworzy się dzięki niemu silną więź między władzami centralnymi a społeczeństwem, skupionym wokół realnego lub mitycznego wroga Matki Rosji. Zastosowano go z powodzeniem podczas kampanii napoleońskiej w 1812 r., w latach 20. XX w., a także w I fazie agresji III Rzeszy na Związek Radziecki.

Warto pamiętać, iż sposoby, których używano 100 i więcej lat temu, mogą okazać się równie skuteczne i śmiertelne, jak najnowszej generacji systemy uzbrojenia rakietowego (o czym przekonały sie władze ukraińskie w 2014 r.). Jeśli nie będziemy równie bezwzględni jak nasi przeciwnicy, to nadal triumfy będą święciły sprawdzone metody, sposoby i formy, wypracowane przez carów, a udoskonalane przez bolszewików Dzierżyńskiego i jego następców. Dlatego też „małą wojnę" należy współcześnie rozpatrywać jako jeszcze jedno narzędzie aktywnej polityki (zwłaszcza militarnej) prowadzonej przez Rosję – polityki coraz skuteczniejszej dzięki znacznemu postępowi technicznemu i kompletnemu zagubieniu się Zachodu i jego społeczeństw. Niski poziom wiedzy, poprawność polityczna, przekonanie, iż istnieje możliwość demokratyzacji Rosji, stanowią naturalną pożywkę dla destrukcyjnych działań Kremla.

Bibliografia

Źródła i opracowania w języku polskim i angielskim

Bassford Ch., *Na palcach wokół trójcy Clausewitza*, tłum. S. Górka, „Kwartalnik Bellona", 2017, nr 1.

Bērziņš J., *Russian New Generation Warfare is not Hybrid Warfare*, [w:] *The War in Ukraine: Lessons for Europe*, red. A. Pabriks, A. Kudors, Rīga 2015.

Clausewitz, C. von, *O wojnie*, tłum. A. Cichowicz, L. Koc, F. Schoener, Lublin 1995.

Compound Warfare: That Fatal Knot, red. T.M. Huber, Fort Leavenworth 2002.

Darczewska J., *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 18.

Eronen P., *Russian Hybrid Warfare: How to Confront a New Challenge to the West*, Washington, DC 2016.

Galeotti M., *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right*, b.m.w. 2016.

Galeotti M., *I'm Sorry for Creating the 'Gerasimov Doctrine'*, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [dostęp: 12.01.2019].

Galeotti M., *Służby wywiadowcze Rosji są w stanie (politycznej) wojny*, Przegląd NATO, 12/05/2017, https://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/PL/index.htm [dostęp: 12.01.2019].

Galeotti M., *„The 'Gerasimov Doctrine' and Russian Non-linear Warfare"*, Moscow's Shadows, July 6, 2014 https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war [dostęp: 12.01.2019].

Gorzkowicz A., *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1.

Grabowska K., *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, „Świat Idei i Polityki" 2015, t. 14.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna*, [w:] *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, red. W. Sokała i B. Zapała, Warszawa 2011.

Haines J.R., *Russia's Use of Disinformation in the Ukraine Conflict*, FPRI, E-Notes, February 17, 2015, https://www.fpri.org/docs/haines_on_disinformation.pdf [dostęp: 12.01.2019].

Hoffman F.G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington 2007.

Hoffman F.G., *Hybrid vs. Compound War. The Janus Choice: Defining Today's Multifaceted Conflict*, „Armed Forces Journal" 2009, October 1, http://www.armedforces journal.com/hybrid-vs-compound-war [dostęp: 1.04.2015].

Hoffman F.G., *Hybrid Warfare Challenges*, „Joint Force Quarterly" 2009, nr 52.

Kalyanaraman S., *Conceptualisations of Guerrilla Warfare*, „Strategic Analysis" 2003, vol. 27, nr 2.

Krzak A., Kuś M., *„Specijalni Rat" („wojna specjalna") w koncepcjach jugosłowiańskiej teorii powszechnej obrony narodowej jako forma zagrożeń asymetrycznych w latach 1970–1990*, [w:] *Asymetryczne Bałkany. Działania asymetryczne, militarne i polityka bezpieczeństwa na Półwyspie Bałkańskim w XX i XXI wieku*, red. D. Gibas-Krzak, Częstochowa 2015.

Lasica D.T., *Strategic Implications of Hybrid War: A Theory of Victory*, Fort Leavenworth 2009.

Monaghan A., *Putin's Way of War: The 'War' in Russia's 'Hybrid Warfare'*, „Parameters" 2015–2016, vol. 45, nr 4.

Myklín M., *Russian Non-Linear Warfare Through the Lenses of Strategic Culture*, Brno 2018.

Nemeth W.J., *Future War and Chechnya: A Case for Hybrid Warfare*, Monterey, CA 2002.

Perry B., *Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations,* Small Wars Journal, https://smallwarsjournal.com/index.php/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera [dostęp: 12.01.2019].

Rusnáková S., *Russian New Art of Hybrid Warfare in Ukraine*, „Slovak Journal of Political Sciences" 2017, vol. 17, nr 3–4.

Schnaufer T.A., *Redefining Hybrid Warfare: Russia's Non-linear War against the West,* „Journal of Strategic Security" 2017, vol. 10, no. 1.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*.

Small Wars Manual. U.S. Marine Corps, Washington 1940.

Steder Frank B., *Introduction: The Theory, History, and Current State of Hybrid Warfare*, „Combating Terrorism Exchange (CTX)" 2016, vol. 6, nr 4.

Tarnawski M., *Rosyjska koncepcja konfliktu nielinearnego*, [w:] *Czynnik wojskowy w środowisku międzynarodowym na przełomie XX i XXI wieku*, red. Ł. Jureńczyk, S. Sadowski, M. Jastrzębski, J. Waskan, Bydgoszcz 2016.

Wojnowski M., *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13.

Wojnowski M., *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*.

Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12.

Źródła i opracowania w języku rosyjskim

Бартош А., *Гибридные войны будущего – прогнозирование и планирование. Как учесть новые угрозы в Военной доктрине России*, „Независимого военного обозрения", 19.12.2014, http://nvo.ng.ru/concepts/2014-12-19/1_war.html [dostęp: 28.12.2016].

Бартош А., *Гибридные войны в стратегии США и НАТО,* Центр анализа террористических угроз (ЦАТУ), 23.10.2014, http://catu.su/analytics/874-gibridnye-vojny-v-strategii-ssha-i-nato [dostęp: 12.01.2019].

Бартош А., *Философия гибридной войны. Сравнительный анализ моделей гибридной войны и цветной революции*, Viperson, 13.10.2016, http://viperson.ru/articles/filosofiya-gibridnoy-voyny-sravnitelnyy-analiz-modeley-gibridnoy-voyny-i-tsvetnoy-revolyutsii [dostęp: 12.11.2016].

Домнин И.В., Савинкин А.Е., *Асимметричное воевание*, „Отечественные записки: Журнал" 2005, № 5, http://magazines.russ.ru/oz/2005/5/2005_5_5.html [dostęp: 12.01.2019].

Дробов М.А., *Малая война. Партизанство и диверсии*, Б.м., 1998.

Дубовицкий Н., *Без неба*, 12 марта 2014, http://ruspioner.ru/honest/m/single/4131 [dostęp: 12.01.2019].

Гареев М.А., *Итоги деятельности Академии военных наук за 2013 год и задачи академии на 2014 год*, „Вестник Академии военных наук" 2014, № 1.

Гареев М.А., *Война и современное международное противоборство*, „Независимое военное обозрение" 1998, № 1.

Герасимов В., *Ценность науки в предвидении*, „Военно-промышленный курьер", 27.02.2013, № 8.

Герасимов В., *Роль Генерального штаба в организации обороны страны в соответствии с новым Положением о Генеральном штабе, утверждённым Президентом Российской Федерации*, „Вестник Академии военных наук" 2014, № 1.

Горбулин В., *„Гибридная война" как ключевой инструмент российской геостратегии реванш*, ZN.UA, 26.01.2015, http://zn.ua/columnists/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-165061_.html [dostęp: 22.12.2018].

Грачиков Е.Н., *Гибридные войны: опыт Израиля*, „Вестник Московского университета" 2015, № 4.

Завтра война! Вооруженные силы и военная реформа в России, ред. А. Проханов, А. Нагорный, В. Шургин, Москва 2013.

Капитанец И., *Битва за мировой океан*, Москва 2002.

Кофман М., *Гибридная война России и другие темные искусства*, Спутник и Погром, 26.03.2016, http://sputnikipogrom.com/translated/52682/dark-russian-arts/#.WIeOuX3my M9 [dostęp: 12.03.2019].

Квачков В.В., *Спецназ России*, Военная литература, 2004, http://militera.lib.ru/science/kvachkov_ vv/index.html [dostęp: 12.03.2019].

Манойло А.В., *Гибридные войны и цветные революции в мировой политике*, „Право и политика" 2015, № 7.

Мятежевойна, „Независимое военное обозрение", 05.11.1999, http://nvo.ng.ru/history/1999-11-05/7_rebelwar.html [dostęp: 12.01.2019]

Рябчук В.Д., Солнышков Ю.С., *Военное науковедение и методология решения проблем управления. Военно-теоретический труд*, Москва 1998.

Серебрянников В.В., *Войны России: социально-политический анализ*, Москва 1999.

Слипченко В.И., *Бесконтактные войны*, Москва 2001.

Хочешь мира, Победи мятежевойну! Творческое наследие Е.Э. Месснера, Под общей редакцией В.И. Марченкова, Москва 2005, http://militera.lib.ru/science/0/pdf/messner_ea01.pdf [dostęp: 12.01.2019].

Rosyjskie rozwinięcia teorii „małej wojny". Wymiar historyczny i współczesny

Streszczenie

Po zimnej wojnie analitycy w wielu krajach nie mogli dokładnie zracjonalizować pojawiających się zagrożeń, które nie pasowały do ówczesnych koncepcji i nie można było ich jednoznacznie sklasyfikować. Poszukiwania nowego kanonu sztuki wojennej doprowadziły wojskowych, polemologów oraz ekspertów do zdefiniowania zjawiska nowych wojen jako konfliktów określanych mianem „wojen hybrydowych". Jednakże próba ta okazała się niewystarczająca – nie pozwala jednoznacznie określić charakteru przyszłych wojen i konfliktów, zwłaszcza wobec niejednoznaczności wydarzeń na Ukrainie czy w Afryce Północnej. Artykuł został poświęcony – istotnej z punktu widzenia teorii i praktyki sztuki wojennej – analizie poglądów zachodnich i rosyjskich autorów na zjawisko łączące różne formy i metody działań konwencjonalnych i nieregularnych (partyzanckich) w perspektywie historycznej i współczesnej.

Słowa kluczowe: wojny nieregularne, wojny partyzanckie, konflikt hybrydowy, wojna hybrydowa, wojna asymetryczna, wywiad aktywny, środki aktywne, dywersja, dezinformacja, mała wojna

The Russian Development of the "Small Wars" Theory: Historical and Contemporary Dimension

Abstract

After the Cold War, analysts in many countries were unable to accurately rationalise the emerging threats that did not fit into the contemporaneous concepts and could not be clearly classified. The search for a new canon of martial art led military people, polemologists and experts to define the phenomenon of new wars as conflicts referred to as „hybrid wars". However, this attempt turned out to be insufficient, as it did not allow to unequivocally determine the nature of future wars and conflicts, especially in view of the ambiguity of events in Ukraine or North Africa. The paper is devoted to the analysis of what is important from the point of view of the theory and practice of the art of war, i.e. the Western and Russian authors' views on the phenomenon that combines a variety of forms and methods of conventional and irregular (guerrilla) actions against a historical and contemporary backdrop.

Key words: irregular wars, guerrilla wars, hybrid conflict, hybrid war, asymmetrical warfare, active intelligence, active measures, diversion, disinformation, small war

Russische Entwicklung der Theorie des „kleinen Krieges". Historische und moderne Dimension

Zusammenfassung

Nach dem kalten Krieg konnten die Analytiker in vielen Ländern nicht die auftauchenden Bedrohungen rationalisieren, welche zu den damaligen Konzeptionen nicht passten und nicht eindeutig klassifiziert werden konnten. Die Suche nach einem neuen Kanon der Kriegskunst führten die Militärangehörigen, Friedensforscher und Experten zur Definierung des Phänomens der neuen Kriege als „hybride Kriegsführung". Dieser Versuch erwies aber als unzureichend – lässt nicht eindeutig den Charakter der künftigen Kriege

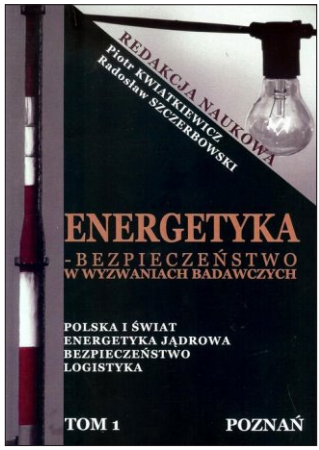
und Konflikte bestimmen , besonders in Bezug auf die Vieldeutigkeit der Ereignisse in der Ukraine oder in Nordafrika. Der Artikel wurde der aus der Perspektive der Theorie und Praxis der Kriegskunst wichtigen Analyse der Ansichten der westeuropäischen und russischen Autoren über die verschiedene Formen und Methoden der konventionellen und Gelegenheitsaktionen (Guerillakampf) verbindende Erscheinung in der historischen und modernen Perspektive gewidmet.
Schlüsselwörter: Guerillakampf, Guerilla-Aktionen, hybride Konfliktführung, hybride Kriegsführung, asymmetrischer Krieg, aktiver militärsicher Nachrichtendienst, aktive Maßnahmen, Ablenkung, Desinformation, kleiner Krieg

Российские разработки теории «малой войны». Исторический и современный аспекты
Резюме

После окончания холодной войны аналитики многих стран не могли дать точную оценку возникающим угрозам, которые не соответствовали существующим концепциям и не могли быть однозначно классифицированы. Поиски нового канона военного искусства позволили военным, полемологам и экспертам дать определение явлению новых войн как конфликтов, именуемых «гибридными войнами». Однако эта попытка оказалась недостаточной – она не позволяет однозначно определить характер будущих войн и конфликтов, особенно в связи с неоднозначностью событий в Украине или в Северной Африке. В статье представлен, важный с точки зрения теории и практики военного искусства, анализ взглядов западных и российских авторов на явление, связывающее различные формы и методы традиционных и иррегулярных (партизанских) действий в исторической перспективе и современном контексте.
Ключевые слова: иррегулярные войны, партизанские войны, гибридный конфликт, гибридная война, асимметричная война, активная разведка, активные средства, диверсия, дезинформация, малая война

Recenzje
Reviews
Rezensionen
Рецензии

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-011



Anna Bałamut

dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0001-7300-7367

Energetyka – bezpieczeństwo w wyzwaniach badawczych, red. Piotr Kwiatkiewicz, Radosław Szczerbowski, tom 1

[Fundacja na rzecz Czystej Energii, Poznań 2017, ss. 391]

Bezpieczeństwo to złożone zagadnienie, dlatego w literaturze nie ma jednej definicji, która je precyzuje. Można jednak najogólniej stwierdzić, że jest to pewien stan lub też proces, który daje poczucie braku zagrożenia. Bezpieczeństwo jest również pojęciem interdyscyplinarnym, co wskazuje, że jego analizą i badaniem zajmuje się szereg nauk, np. socjologia, politologia, nauki prawne. Jednym z jego elementów składowych jest bezpieczeństwo energetyczne rozumiane jako zagwarantowanie nieprzerwanych dostaw surowców energetycznych po możliwej do zapłacenia przez odbiorców cenie (tu również z uwagi na złożoność zagadnienia występuje wiele definicji). W XXI wieku spełnienie takiego założenia staje się coraz większym wyzwaniem zarówno dla państw, jak i podmiotów działających na rynku energetycznym. Wynika to z kilku elementów: zmniejszania się zasobów paliw kopalnych, trudności politycznych, przestarzałej infrastruktury, problemu ochrony środowiska naturalnego i kwestii ograniczania emisji CO_2. Zasoby energetyczne lub ich brak mają znaczący wpływ na charakter kontaktów gospodarczych pomiędzy poszczególnymi krajami, które uzależniają państwa importujące od eksporterów.

Książka została wydana przez Fundację na rzecz Czystej Energii w Poznaniu w 2017 r. pod red. dr. hab., prof. WAT-u Piotra Kwiatkiewicza oraz dr. inż. Radosława Szczerbowskiego, wykładowcy Politechniki Poznańskiej. Składa się z 28 rozdziałów

(w tym 1 w języku angielskim) napisanych zarówno przez przedstawicieli świata nauki, jak i osoby interesujące się tematyką bezpieczeństwa. Autorzy tomu skupili się na następujących zagadnieniach: polityce międzynarodowej, wykorzystaniu paliw jądrowych oraz logistyce i kwestiach obronnych. Wskazali, że popularność problematyki bezpieczeństwa jako przedmiotu analiz badaczy naukowych wynika z liberalizacji, czyli skupiania coraz większej uwagi na jednostce i jej potrzebach.

Recenzowana książka składa się z 391 stron. Posiada wstęp, w którym następuje charakterystyka Autorów oraz prezentowanych przez nich zwięzłych i przejrzystych treści. Pomimo iż publikacja była pisana przez kilkanaście osób, poszczególne rozdziały zawierają pewne elementy wspólne, takie jak: wstęp, tekst właściwy, zakończenie oraz wnioski końcowe w języku polskim i angielskim. Bibliografia – również w dwóch językach – została wymieniona na końcu każdego z rozdziałów. Składają się na nią przede wszystkim: opracowania książkowe, artykuły, dokumenty oraz źródła internetowe. Całość wzbogacona jest licznymi tabelami, schematami, wykresami i mapami, co podnosi wartość recenzowanej pracy zbiorowej.

W publikacji zabrakło jednak: wykazu skrótów, indeksu nazwisk, spisów tabel, wykresów i schematów. Elementy te ułatwiłyby czytelnikowi poszukiwanie i dotarcie do konkretnej informacji.

Pierwszy tekst, autorstwa Mirosława Skarżyńskiego, dotyczy kwestii miejsca terminali LNG w polityce energetycznej Finlandii, jako próby uniezależnienia się od dostaw gazu z Rosji. Istotą problemu jest potrzeba wybudowania dużego terminalu LNG albo rozbudowa już istniejącego. Kwestie finansowania i lokalizacji powodują, że inwestycja odsuwa się w czasie, co wpływa na obniżenie poziomu bezpieczeństwa energetycznego kraju.

Rozdział Marcina Tarnawskiego dotyczy *Roli i znaczenia porozumienia klimatycznego w Paryżu dla sektora gazu ziemnego w Europie*. Jak wskazuje Autor, wydarzenie to można nazwać sukcesem, ponieważ po 20 latach udało się wypracować wiążące porozumienie dla państw w sprawie długoterminowego celu, jakim jest ograniczenie globalnego ocieplenia do wartości poniżej 2°C.

Natomiast Joanna Modrzejewska-Leśniewska omawia miejsce OPEC na współczesnym rynku ropy naftowej i wskazuje trudności występujące między państwami członkowskimi związane z wypracowaniem jednolitej polityki wydobycia, a co za tym idzie kształtowania ceny surowca. Drugą kwestią jest konkurencyjność innych surowców, np. gazu ziemnego, czy też odnawialnych źródeł energii. Prowadzi to w konsekwencji do pytania (które sygnalizuje sama Autorka) o zasadność funkcjonowania wspomnianej organizacji.

Łukasz Wojcieszak wskazuje na trudności polityczne i logistyczne budowy Nord Stream 2, tj. inicjatywy transportu rosyjskiego gazu do Europy. Budzi ona kontrowersje nie tylko państw członkowskich UE, ale i Norwegii. Pomimo wspierania projektu przez polityków niemieckich, pojawia się pytanie o jego opłacalność. Z jednej strony UE mówi o dywersyfikacji dostaw surowców, a z drugiej niektóre państwa członkowskie popierają projekt. Co ciekawe nie prowadzi on przecież do uniezależnienia się od Rosji, ponieważ dostawca nadal pozostaje ten sam, stąd sprzeciwy m.in. Polski. W przypadku warunków logistycznych problematyczną kwestię mogą stanowić np. prądy morskie czy naprężenia statyczne i dynamiczne możliwe podczas budowy.

Marian Kopczewski i Paweł Olbrycht wskazują, że położenie Polski jest wyznacznikiem poziomu jej bezpieczeństwa energetycznego. Nie można się z tym stwierdzeniem nie zgodzić. Obszar Europy Środkowej charakteryzuje się słabym pod względem zasobności dostępem do surowców energetycznych. Pomimo centralnej lokalizacji dróg przesyłowych, Polska nie czerpie znaczących korzyści z faktu, że jest krajem tranzytowym również w ramach sektora energetycznego. Fakt ten znacząco obniża jej bezpieczeństwo energetyczne.

Tekst Tomasza Motowidlaka dotyczy aspektu *Bezpieczeństwa dostaw energii do Polski w warunkach funkcjonowania Unii Energetycznej*. Za Autorem należy podkreślić, że jest ono determinowane przez wiele czynników, takich jak: zależność od źródła i kierunku dostaw; infrastruktury logistycznej, tj. szlaków przesyłowych i zdolności magazynowych; sytuacji politycznej; stosunków z krajami eksporterami surowców energetycznych oraz ram instytucjonalno-prawnych. Jak mówi sam Autor, ze względu na rodzaj dobra jakim jest energia, zapewnienie bezpieczeństwa energetycznego przyjmuje wymiar polityczny. Propozycja Donalda Tuska dotycząca Unii Energetycznej wskazała m.in., że UE powinna utworzyć taką unię, aby zabezpieczyć dostawy gazu, uniezależnić się od Rosji oraz wzmocnić solidarność gazową poprzez jego wspólne zakupy. Dodatkowo jako rozwiązanie proponowano gaz łupkowy, ze względu na wielkość jego złóż w Polsce na tle innych państw Europy. Kooperacja z Unią Europejską w ramach wspólnych wytycznych rodzi pewne obawy o zasadność interesów, czego przykładem może być projekt Nord Stream 2 (uwzględniający interes tylko pewnych członków Unii) czy też nacisk na OZE (odnawialne źródła energii) i ograniczenie emisji dwutlenku węgla.

Łukasz Wojcieszak zwraca natomiast uwagę na bezpieczeństwo energetyczne Białorusi i jej zależność od Rosji. Kwestia dywersyfikacji dostaw surowców pojawiła się w białoruskiej polityce po 2004 r. i dotyczyła m.in. importu ropy z Wenezueli (zakończony w 2012 r.). Warto podkreślić rolę tego państwa jako partnera tranzytowego dla Rosji, która w ten sposób przesyła około 60 mln ton ropy rocznie. Dodatkowo Rosja oddziałuje na ceny ropy w rafineriach białoruskich. Rozwiązaniem w ramach dywersyfikacji źródeł pozyskania energii miała być budowa elektrowni atomowej. Była ona nawet przedmiotem tzw. rywalizacji politycznej w 2016 r. Co ciekawe środki na budowę tego obiektu pochodzą z rosyjskich źródeł, co budzi kontrowersje dotyczące niezależności inwestycji. Innym rozwiązaniem są OZE, jednakże system biurokracji znacząco utrudnia kreowanie inwestycji w tym sektorze. Można wskazać jednak pewne przykłady zainteresowania sektorem podmiotów zagranicznych oraz wykorzystania OZE dla potrzeb prywatnych, m.in. fotowoltaikę.

Drugi tekst Mariana Kopczewskiego i Pawła Olbrychta skupia uwagę czytelnika na *Bezpieczeństwie energetycznym Unii Europejskiej w kontekście współpracy z Federacją Rosyjską*. Rosja realizuje własne cele ekonomiczne oraz prezentuje obojętne lub negatywne stanowisko wobec unijnych inicjatyw. Powstaje jednak pewien paradoks – z jednej strony w interesie UE jest dywersyfikacja dostaw surowców, a tym samym uniezależnienie się od dostaw z Rosji, a z drugiej popierane są inicjatywy, które zwiększają ową współpracę, jak np. Nord Stream 2.

Kolejnym zagadnieniem poruszanym w książce jest energia jądrowa i jej wpływ na bezpieczeństwo energetyczne państwa. Mariusz Charchut i Iwona Grzesiak

uważają, że zwiększenie zapotrzebowania na energię elektryczną w Polsce wymusza dywersyfikację kierunków i źródeł pozyskania energii. Takim rozwiązaniem miała być budowa elektrowni jądrowej, która pomimo silnego wsparcia rządu w ramach struktur zarządzania projektem nie doczekała się realizacji. Problematycznymi kwestiami były m.in.: wybór lokalizacji i technologii oraz kwestia składowania odpadów radioaktywnych.

Kontynuację rozważań prowadzi Krzysztof Sala, wskazując na *Perspektywy wykorzystania energetyki jądrowej w Polsce w aspekcie bezpieczeństwa ekologicznego*. Dotyczy ono bezawaryjnego funkcjonowania elektrowni oraz bezpiecznej utylizacji odpadów radioaktywnych. Potrzeby budowy elektrowni potwierdzają również Karolina Madera-Bielawska, Wojciech Zacharczuk oraz Andrzej Tatarek w artykułach: *Rola energetyki jądrowej w polskim systemie elektroenergetycznym* oraz *Nuclear power in the context of Poland's long-term energy policy*. Problem bezpieczeństwa elektrowni z reaktorem AP1000 omawia natomiast Jakub Sierchuła.

Kolejna część książki analizuje kwestię bezpieczeństwa pod względem technicznym, co zaprezentowano w następujących artykułach: *Propozycja modyfikacji definicji bezpieczeństwa technicznego obiektów inżynierskich* (Tadeusz Chrzan), *Obrona i odbudowa zdolności wytwórczych elektrowni i elektrociepłowni w warunkach awarii katastrofalnych systemu elektroenergetycznego* (Daria Radsak, Krzysztof Sroka), *Bezpieczeństwo publiczne w obliczu awarii systemu elektroenergetycznego* (Jakub Adamkiewicz), *Bezpieczeństwo obiektów inżynierskich a działalność człowieka* (Tadeusz Chrzan), *Komputerowy program doboru zabezpieczeń ziemnozwarciowych jako element poprawy bezpieczeństwa pracy sieci dystrybucyjnych SN* (Jerzy Andruszkiewicz, Józef Lorenc, Bogdan Staszak) oraz *Akwizycja danych przy użyciu platformy arduino jako alternatywa dla zaawansowanych systemów pomiarowych* (Sławomir Szymocha).

Natomiast ostatnia część książki skupia się na kwestiach logistycznych. Można tutaj wskazać następujące artykuły: *Wybrane aspekty rozwoju sieciowej infrastruktury elektroenergetycznej* (Waldemar Dołęga), *Struktura przestrzenna energetyki rozproszonej opartej na odnawialnych zasobach energii w Polsce* (Piotr Hektus), *Wykorzystanie systemów magazynowania energii elektrycznej do optymalnego zarządzania energią elektryczną w sieciach typu smart grid* (Kazimierz Herlender), *Bariery rozwoju elektromobilności i płynące z niej zagrożenia* (Huber Igliński), *Możliwości inspekcji elementów linii wysokiego napięcia z wykorzystaniem metod przetwarzania obrazu* (Paweł Michalski, Jakub Osuchowski), *Przegląd metod diagnostycznych izolatorów linii napowietrznej* (Jakub Osuchowski), *Realizacja strategicznych inwestycji w zakresie sieci przesyłowych w świetle tzw. specustawy przesyłowej* (Józef Zaguła, Mariusz Rutkowski), *Pomiar natężenia pola elektromagnetycznego dla potrzeb inspekcji infrastruktury elektroenergetycznej obiektem UAV* (Sławomir Szymocha) oraz *Wpływ jakości energii elektrycznej na bezpieczeństwo energetyczne zakładu przemysłowego* (Marta Bątkiewicz-Pantuła).

Wielość omawianych zagadnień ma na celu uświadomienie oraz pokazanie czytelnikowi jak wielkie znaczenie mają poruszane problemy również w ujęciu technologicznym i technicznym, a także jak bardzo bezpieczeństwo oddziałuje na aspekt logistyczny i odwrotnie. Reasumując, adresatami publikacji są osoby

zainteresowane nie tylko kwestiami bezpieczeństwa, ale również kwestiami logistyki i technologii.

Książka może stanowić doskonałe źródło informacji zarówno dla studentów zarządzania, jak i dla osób chcących pogłębić swoją wiedzę na temat wyzwań, zagrożeń i perspektyw dotyczących pozyskiwania energii na świecie. Różnorodność prezentowanych treści zachęca nie tylko do przeczytania całości publikacji, ale i do dalszych poszukiwań, np. poprzez odwiedzenie wskazanych w bibliografii stron internetowych, zapoznanie się z proponowanymi pozycjami naukowymi czy też artykułami.

BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-012

Wojciech Huszlak

doktorant, Krakowska Akademia
im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0003-1272-8114

Adam Skrzypek, *Dojrzałość i doskonalenie organizacji*

[Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 2019, ss. 399]

Doskonalenie podmiotów wchodzących w skład systemu zarządzania bezpieczeństwem można analizować biorąc pod uwagę m.in. dorobek dotyczący doskonalenia organizacji. Istotne dla dorobku teoretycznego i praktycznego odnoszącego się do bezpieczeństwa mogą być również rozważania związane z dojrzałością organizacji, a tym samym z ciągłym ich modernizowaniem.

Przesłanką wyboru książki była aktualność tematyki dojrzałości organizacji, która stanowi atrybut zmian. Z tego powodu szczególnie interesująca może być analiza wątków związanych z dojrzałością dziedzinową, w szczególności odnoszącą się do zagadnienia bezpieczeństwa.

Recenzowana książka to monografia napisana przez Adama Skrzypka, pracownika naukowo-badawczego Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Autor posiada znaczący dorobek naukowy. Jego praca skupiona była początkowo na obszarach badawczych odnoszących się do: jakości zarządzania wiedzą i kapitałem intelektualnym, konkurencyjności i doskonalenia, zarządzania procesami i projektami oraz pomiaru procesów. Po uzyskaniu tytułu doktora, Skrzypek skoncentrował się na tematyce: dojrzałości organizacyjnej oraz jej związkach z doskonaleniem zarządzania (metody i narzędzia doskonalenia); zarządzania wiedzą; GOW; jakości zarządzania i systemów zarządzania nią; modeli organizacji;

nowoczesnych koncepcji; metod i narzędzi zarządzania organizacją oraz ryzyka i zarządzania nim. Efektem prac badawczych jest znaczący dorobek obejmujący 77 publikacji. Recenzowana książka stanowi jego ważny element i jest zwieńczeniem pracy naukowej w wyżej wskazanych obszarach.

Przedmiotem badań w najnowszej publikacji Skrzypka jest sposób postrzegania problemu dojrzałości organizacji przez ekspertów oraz instytucje wiodące w zakresie doskonalenia i osiągania kolejnych wymiarów dojrzałości. Praca wpisuje się w nurt badań nad tą tematyką w organizacjach funkcjonujących w warunkach zmian, niepewności i ryzyka oraz rosnącego znaczenia wiedzy we wszystkich obszarach życia.

Autor jako cel główny monografii postawił „opracowanie zintegrowanego modelu doskonalenia, opartego na wiedzy, uwzględniającego dojrzałość systemów zarządzania, modele dojrzałości i modele doskonałości" (s. 13). Wskazał również sześć celów szczegółowych odnoszących się do:

– rozpoznania tego, jak rozumiana jest dojrzałość i doskonalenie organizacji w teorii i w praktyce;
– usystematyzowania koncepcji dojrzałości i doskonałości organizacji;
– wskazania determinant doskonalenia organizacji, które przyczyniają się do wzrostu dojrzałości organizacji;
– wskazania poziomu dojrzałości i doskonałości badanych organizacji;
– określenia stosunku do wiedzy i zarządzania nią, który mógłby stanowić bazę dla integracji systemów zarządzania;
– określenia modeli dojrzałości i doskonałości, a także związków pomiędzy doskonaleniem i dojrzałością, które mogą być inspiracją dla zarządzających do wprowadzania zmian w sposobie podejścia do procesów umożliwiających integrację doskonalenia na bazie wiedzy.

Obok wskazanych celów Skrzypek sformułował jeszcze dwa: teoriopoznawcze (przegląd i systematyka krajowej i zagranicznej literatury przedmiotu w zakresie dojrzałości i doskonalenia oraz opracowanie narzędzia badawczego) i utylitarne (dostarczenie praktykom informacji na temat potrzeb i możliwości wdrażania rozwiązań służących doskonaleniu organizacji oraz zaproponowanie modelu integracji dojrzałości i doskonalenia w celu osiągania doskonałości organizacji).

Realizacji celów postawionych w książce służy jej układ. Praca składa się z sześciu rozdziałów o charakterze teoretycznym i empirycznym, które wzajemnie się uzupełniają i tworzą logiczną całość.

Wstęp do książki opiera się w głównej mierze na przedstawieniu wagi problemu badawczego oraz uzasadnieniu jego wyboru. Skrzypek zwraca uwagę na wzrost zainteresowania problemem dojrzałości organizacji, modelami dojrzałości oraz ich aplikacją w różnych segmentach gospodarki. Wskazuje także na konieczność poszukiwania „wyrafinowanych produktywnych i adaptacyjnych rozwiązań w obszarze zarządzania" (s. 11). Autor sformułował tezę mówiącą o tym, że badania dotyczące dojrzałości i jej związków z doskonaleniem znajdują się w fazie rozwoju. Dodatkowo wielość zagadnień poruszanych w publikacjach z tego zakresu skłoniła go do podjęcia próby uporządkowania dotychczasowych perspektyw i kierunków eksploracji naukowej oraz do wskazania najważniejszych płaszczyzn badawczych w ramach zagadnień dojrzałości i doskonałości.

Rozdział pierwszy został poświęcony dojrzałości. Skrzypek przedstawił w nim wyniki analizy bibliometrycznej, dowodząc skali zainteresowania tym problemem w literaturze światowej. Dokonał przeglądu definicji dojrzałości i podkreślił, że jest to pojęcie fundamentalne w teorii rozwoju i obszarach poszukujących inspiracji. Wskazał także na źródła dojrzałości oraz złożoność i wielowymiarowość tego problemu. Syntezując podejścia do dojrzałości, autor dokonał uogólnienia wskazującego, że jest to zdolność do osiągania celów organizacji, stałego jej doskonalenia oraz spełniania oczekiwań interesariuszy.

Skrzypek przedstawił również szeroki przegląd literatury światowej i krajowej, która odnosi się do poszczególnych rodzajów dojrzałości: innowacyjnej; technologicznej; procesowej; dojrzałości w zakresie jakości, wiedzy, zarządzania terminologią i wynikami; dojrzałości w odniesieniu do człowieka, klienta i sfery usług; dojrzałości jako stanu umysłu, zrównoważonych łańcuchów dostaw oraz dojrzałości projektowej. Omówił także uwarunkowania i konsekwencje dojrzałości organizacji oraz podkreślił, że problem ten ma swoje odniesienie w sferze rozważań teoretycznych, w badaniach oraz w rozwiązaniach praktycznych i normatywnych. Zaprezentował analizę i ocenę przejawów dojrzałości organizacji oraz zaznaczył, że w tym obszarze wyróżnia się grupę dojrzałości zintegrowanych i wyspecjalizowanych. Zwrócił uwagę, że dojrzałość organizacji rozpatrywana jest coraz częściej w kontekście paradygmatu rozwoju jako organizacji zrównoważonej. Autor scharakteryzował i dokonał oceny organizacji dojrzałej – dążącej do doskonałości – i niedojrzałej, wskazał na znaczenie dojrzałości systemu zarządzania organizacją oraz przedstawił jego istotę. Omawiając powiązania między dojrzałością i doskonaleniem, Skrzypek zaprezentował własne wyniki badań na temat doskonalenia zarządzania w opinii przedsiębiorstw, laureatów Polskiej Nagrody Jakości. Wymienił także korzyści wynikające z osiągnięcia dojrzałości.

W rozdziale drugim autor omówił problemy związane z modelami dojrzałości oraz przedstawił ich istotę (odwołując się do takich autorów jak: Joel Dean, Abraham Maslow, Simon Kuznetz, Richard L. Nolan, Philip Crosby), przegląd definicji i klasyfikacji, a także przybliżył genezę modeli dojrzałości oraz problemy dotyczące ich rozwoju. Wskazał na wpływ modelu CMM (Capability Maturity Model) jako źródło dynamicznego rozwoju modeli dojrzałości i zwrócił uwagę na dużą rolę, jaką odgrywa w nich wiedza. Skrzypek omówił również definicje modeli dojrzałości oraz ich funkcje, zadania i związek z doskonaleniem zarządzania. Wskazał, że modele te mogą być wykorzystane do oceny postępu organizacji w procesie doskonalenia, a także w aspekcie realizacji najważniejszych oczekiwań wynikających z wymogów oraz przewidywań interesariuszy. Modele dojrzałości stanowią zbiory najlepszych praktyk zarządzania i programy działania, które mogą pełnić rolę wzorca, zestawu wskazówek, który umożliwia implementację systemów zarządzania, oraz być narzędziem doskonalenia już istniejących systemów. Autor podał przykłady ich zastosowań np.: w obszarze benchmarkingu, przy charakterystyce i ocenie procesów organizacyjnych, ocenie słabych i mocnych stron organizacji, sterowaniu przedsięwzięciami usprawniającymi procesy czy przy ocenie ryzyka. Ten ostatni element można łączyć również z problematyką bezpieczeństwa, w szczególności gdy może on służyć jako narzędzie doskonalenia zarządzania bezpieczeństwem. Skrzypek omówił także korzyści związane z wdrożeniem modeli dojrzałości

w organizacji i wskazał m.in. na: efekty synergii wielu obszarów, które wpływają na lepsze wyniki niż przy podejściu indywidualnym w przypadku pojedynczych obszarów; możliwość sformalizowania działań zarządczych oraz ciągłego diagnozowania ich poziomu zaawansowania; poszukiwanie sposobów doskonalenia procesów; wykorzystanie modelu jako punktu odniesienia dla porównań; obniżenie kosztów realizacji procesów; podniesienie jakości wyrobów i usług, poprawę satysfakcji klientów; przyspieszenie zwrotu z inwestycji w procesy oraz ich informatyzację. Autor zwrócił również uwagę na efekty niematerialne, trudno mierzalne, np. na większe szanse pozyskania kontraktów w ramach przetargów czy nawiązanie kontaktów i podjęcie współpracy z kontrahentami.

Przegląd wybranych dziedzinowych modeli dojrzałości został zawarty w trzecim rozdziale. Autor przedstawił zagadnienie dojrzałości procesowej i podkreślił, że jej modele należą do modeli dziedzinowych rozwijanych przez środowiska naukowe i praktykę. Jednocześnie wskazał, że powinny one realizować cele opisowe, normatywne i porównawcze. Skrzypek zauważył wielość procesów w przedsiębiorstwach oraz rosnące zainteresowanie modelami dojrzałości w różnych obszarach zarządzania organizacją. Następnie przedstawił ujęcia dojrzałości procesowej proponowane przez różnych autorów oraz rolę i przydatność modeli dojrzałości procesowej w organizacji. Zwrócił uwagę na dynamiczny rozwój tych modeli, których liczbę niektórzy autorzy szacują na ponad 200. W sposób syntetyczny, poparty przejrzystym układem tabelarycznym pozwalającym na łatwe porównanie, autor zaprezentował wybrane modele dojrzałości procesowej, w tym modele referencyjne. W opisie uwzględnił również ich mocne i słabe strony. Istotną kwestią poruszoną w rozdziale jest analiza wyników badań w zakresie podejścia procesowego różnych autorów, m.in.: Wojciecha Cieślińskiego, Krzysztofa Dziekońskiego i Arkadiusza Jurczuka, Witolda Szumowskiego, Szymona Cyferta czy Elżbiety Skrzypek.

Autor odniósł się do modeli dojrzałości projektowej, która jest utożsamiana ze stanem zaawansowania w zarządzaniu projektami. Przedstawił przegląd definicji tego rodzaju dojrzałości, zaprezentował cechy organizacji zorientowanej projektowo oraz nurty teoretyczne w tym obszarze. Odniósł się do problemu badania dojrzałości projektowej organizacji, wskazując, że jest ona analizowana w odniesieniu do danego modelu. Zwrócił także uwagę na zagadnienia występujące w różnych modelach dojrzałości w zarządzaniu projektami.

W dalszej części rozdziału, która dotyczy modeli dojrzałości zarządzania ryzykiem, Skrzypek zaznaczył, że wzrost zainteresowania tego rodzaju zarządzaniem znajduje swoje odniesienie w poszukiwaniu sposobów oceny dojrzałości w tym obszarze funkcjonowania organizacji. Zaprezentował również najważniejsze modele dojrzałości zarządzania ryzykiem oraz zestawił (w postaci tabelarycznej) ich podobieństwa i różnice z wykorzystaniem własnych kryteriów.

Autor podkreśla duże znaczenie zarządzania wiedzą w organizacji, ponieważ ma ono wpływ na realizację działań prowadzących do poprawy jej dojrzałości i możliwości osiągania przez nią doskonałości. Wskazuje przy tym, że przedsiębiorstwo, aby stać się organizacją bardziej dojrzałą i coraz bardziej doskonałą, powinno systemowo, procesowo i strategicznie podchodzić do swoich zasobów wiedzy, wyceniać je i zarządzać nimi. Szczególnie istotnym elementem jest diagnoza i ocena zasobów wiedzy, które w kombinacji z zastosowanym modelem dojrzałości zarządzania

wiedzą mogą wskazywać na kierunki doskonalenia oraz stymulować do poszukiwania jego sposobów. W postaci tabelarycznej Skrzypek przedstawił różne kategorie zarządzania wiedzą oraz korzyści organizacji związane z dojrzałością w tym zakresie. Zaprezentował również koncepcję oceny dojrzałości zarządzania wiedzą wskazując na etapy rozwoju praktyk zarządzania nią. Podkreślił znaczenie mapowania wiedzy oraz niezbędnej „infrastruktury", która decyduje o dojrzałości zarządzania wiedzą w przedsiębiorstwie (pamięć organizacyjna, zasoby ludzkie, sieć, transfery technologii, infrastruktura Business Intelligence, infrastruktura współpracy). Zwrócił również uwagę na aspekt zarządzania talentami. Porównał i zaprezentował w sposób przejrzysty wybrane modele dojrzałości zarządzania wiedzą, a także dokonał analizy wyników badań w tym obszarze i jego dojrzałości.

Rozdział porusza również tematykę modeli dojrzałości dziedzinowych w zakresie jakości. Według autora dojrzałość jakościowa oznacza, że organizacja rozumie jakość w sposób kompleksowy, a zarządzanie jakościowe ukierunkowane na doskonalenie powinno być powiązane z aktywnością w zakresie innowacji. Skrzypek wskazał pojęcie dojrzałości jakościowej, jej elementy składowe oraz cechy. Przeanalizował i przedstawił ocenę poziomów dojrzałości funkcjonowania różnych systemów zarządzania jakością. Wymienił wyznaczniki dojrzałości organizacyjnej, jakimi są: kreatywność, przedsiębiorczość i innowacyjność, a także przedstawił kształtowanie się rozwoju modeli dojrzałości w ujęciu historycznym i porównał je. Zaprezentował niektóre metody i narzędzia prowadzące do dojrzałości jakościowej oraz dokonał analizy modelu ciągłego doskonalenia dojrzałości (Continuous Improvement Maturity Model).

W rozdziale czwartym autor poruszył kwestię istoty doskonalenia, dokonał analizy problemów z nim związanych oraz odniósł się do jego przesłanek, typów i wymiarów. Omówił zagadnienia związane z organizacją doskonałą, prezentując jej cechy oraz modele doskonalenia, a także zwrócił uwagę na korzyści z nim związane. Tematyka rozdziału została uzupełniona o zagadnienia instrumentarium wykorzystywane w doskonaleniu, a więc o jego koncepcje i modele. Skrzypek zaprezentował również szereg metod, które są stosowane w procesie doskonalenia oraz dokonał ich porównania w tabeli.

Niezwykle istotną kwestią poruszoną w książce jest analiza związków między modelami doskonalenia a modelami dojrzałości. Jedną z istotniejszych kwestii w ocenie dojrzałości jest określenie ich poziomów, czemu Skrzypek poświęcił fragment podrozdziału. Przedstawił w nim wybrane modele doskonalenia organizacji oraz dokonał przeglądu podejść wybranych autorów do relacji między dojrzałością organizacji a jej doskonaleniem.

W rozdziale piątym autor przedstawił istotę integracji zarządzania, jej obszary oraz narzędzia. Omówił warunki konieczne dla prowadzenia efektywnego i skutecznego zintegrowanego systemu zarządzania i zwrócił uwagę na ważną rolę jakości w tym procesie. Przedstawił mechanizmy doskonalenia zawarte w różnych normach oraz zaznaczył, że istnieje możliwość integracji elementów modeli Business Excellence z narzędziami zarządzania operacyjnego. Skrzypek przeanalizował korzyści związane z integracją systemów zarządzania i zwrócił szczególną uwagę na wiedzę, jako jej podstawę: „zarządzanie wiedzą pozwala na pełniejsze wykorzystanie istniejących w przedsiębiorstwie zasobów, łączenie zasobów informacji

i wiedzy skumulowanej w przedsiębiorstwie oraz utworzenie zintegrowanego systemu informacyjnego, który mógłby wpierać realizację kilku rozwiązań w zakresie zarządzania" (s. 263). Podkreślił, że integracja może objąć swym zasięgiem systemy zarządzania, modele dojrzałości i doskonalenia. Autor omówił wpływ dojrzałości i doskonalenia na integrację oraz możliwości integrowania na bazie połączonych modeli CMMI oraz ADAMS. Przedstawił również koncepcję zintegrowanego doskonalenia, tzw. doskonałość 5.0.

Podsumowanie rozdziału stanowi prezentację autorskiego zintegrowanego modelu dojrzałości i doskonalenia organizacji. Powstał on w wyniku szeroko zakrojonych studiów literatury światowej i krajowej oraz w wyniku badań własnych z obszaru doskonalenia, doskonałości, dojrzałości i integracji. W postaci graficznej i opisowej Skrzypek przedstawił jego elementy, cel, istotę oraz przydatność w organizacji. Z modelu wynika, że „doskonalenie organizacji wpływa na dojrzałość organizacji, a ta z kolei wpływa na doskonalenie zarządzania, które można rozumieć jako osiąganie wyników i zdolności organizacyjnych, które kształtują dojrzałość organizacji" (s. 270). Natomiast doskonalenie zarządzania tworzy bazę dla zintegrowanego doskonalenia opartego na wiedzy. Obejmuje ono rozwiązania zawarte w dojrzałych systemach zarządzania, modelach dojrzałości oraz doskonałości, które są nakierowane na osiąganie doskonałości 5.0. Efektem tych zależności i związków jest doskonałość organizacji oparta na wiedzy.

Ostatni, szósty rozdział to rozdział empiryczny. Autor przedstawił w nim metodykę, opis procesu badawczego, analizę i ocenę wyników, wnioski oraz kierunek dalszych badań. Zaprezentował cele (cel główny i cele cząstkowe), hipotezy, przedmiot i zakres badań. Omówił proces badawczy, próbę badawczą oraz zastosowane metody, narzędzia i techniki. Wszystkie etapy przedstawił w postaci rysunku (schematu) procesu badawczego, a wyniki w postaci graficznej – w formie modeli, tabel oraz wykresów.

Warto zwrócić uwagę na autorskie narzędzia wykorzystane w procesie badawczym. Przedmiotem badań Skrzypka były różne aspekty dojrzałości w percepcji przedstawicieli organizacji i ekspertów. Wnioski odnoszą się do części teoretycznej i badawczej – autor przedstawił wyniki badań jako analizę porównawczą odpowiedzi ekspertów i przedstawicieli stu przedsiębiorstw, co znacząco podnosi ich wartość. Odniósł się również do hipotez oraz wskazał dalsze kierunki badań.

Ostatnia część pracy to zakończenie, w którym Skrzypek udzielił odpowiedzi na postawione w pracy pytania badawcze. Potwierdził zrealizowanie celów wskazanych na początku książki oraz pozytywnie zweryfikował hipotezę.

Książka charakteryzuje się aktualnością poruszanych zagadnień i ma znaczenie poznawcze, wzbogacające wiedzę z zakresu problematyki związanej z doskonaleniem organizacji. Autor dokonał rozpoznania tego, jak w literaturze światowej i polskiej rozumiane są pojęcia: dojrzałości, doskonalenia i doskonałości organizacji w teorii i praktyce. Uporządkował koncepcje dojrzałości i doskonalenia organizacji, dokonał przeglądu i usystematyzowania rozwiązań koncepcyjnych w obszarze dojrzałości dziedzinowych uwzględniając ich ewolucję. Zidentyfikował determinanty doskonalenia organizacji, które wpływają na wzrost ich dojrzałości oraz wskazał, na jakim poziomie zarówno dojrzałości, jak i doskonalenia znajdują się organizacje uznane za dojrzałe. Podkreślił pozytywny stosunek badanych organizacji do wiedzy

i zarządzania nią jako podstawy dla integracji systemów zarządzania, modeli dojrzałości i doskonałości. Wskazał kierunki zmian w podejściu do procesów integracji.

Na uwagę zasługuje opracowany ideowy model zintegrowanej dojrzałości i doskonalenia na bazie wiedzy. Skrzypek wskazał potrzebę integracji dojrzałych systemów zarządzania, modeli dojrzałości i doskonałości. Z kolei autorski model stanowi przykład włączenia się autora w dyskusję na temat poszukiwania sposobów doskonalenia zarządzania w organizacjach, które zmierzają do dojrzałości i doskonałości oraz funkcjonują w warunkach zmian, niepewności i ryzyka. Skrzypek uwypuklił rangę zarówno wiedzy i zarządzania nią, jak i dojrzałości w zakresie wiedzy w procesach mających na celu doskonalenie organizacji i dążenie do doskonałości. Wskazał także poziom dojrzałości i doskonalenia w badanych przedsiębiorstwach w oparciu o metodę segmentacji.

Realizacja celu głównego pracy była możliwa dzięki weryfikacji proponowanego modelu ideowego integrującego dojrzałość i doskonalenie organizacji na bazie wiedzy. W tym celu autor zastosował metody ankietowania i przeprowadził wywiady z przedstawicielami organizacji i ekspertami. Skrzypek dysponuje bardzo wysokim poziomem warsztatu naukowego, na co wskazuje zaprezentowana metodyka, stosownie dobrana do rozwiązania podjętych problemów badawczych. Do osiągnięcia celów szczegółowych autor wykorzystał różnorodne metody, m.in.: krytyczną analizę literatury przedmiotu, metodę ankietowania i wywiadu bezpośredniego nieustrukturyzowanego, metodę delficką, analizę luki zarządzania, CAWI, kwerendy i TwoStep Cluster Analysis. Praca oparta została na bogatej literaturze obejmującej 668 pozycji, z czego blisko 300 to literatura anglojęzyczna.

Reasumując, przedstawiona książka stanowi szerokie i kompletne studium teoretyczne wsparte wynikami badań nad problematyką dojrzałości i doskonałości organizacji, które łączy zarządzanie wiedzą oraz dojrzałość w tym obszarze. Warto podkreślić jej istotne walory aplikacyjne, dzięki licznie opisanym wynikom badań i rekomendacjom dla przedsiębiorstw w zakresie działań związanych z doskonaleniem organizacji.

Poruszana tematyka może być kontynuowana i poszerzana, w szczególności z wykorzystaniem przedstawionego modelu dojrzałości i doskonalenia, np. w badaniu poziomów dojrzałości dziedzinowych pod kątem stanu i możliwości wzrostu. Szczególnie interesujące mogą być badania poziomu dojrzałości dziedzinowych w relacji do zapewnienia bezpieczeństwa (np. dojrzałość infrastruktury IT a bezpieczeństwo informacji).

Komunikaty, sprawozdania
Bulletins, Reports
Mitteilungen, Berichte
Сообщения, отчеты

BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA

e-ISSN 2451-0718
ISSN 1899-6264

DOI: 10.34697/2451-0718-btip-2019-4-013

Mirosław Kwieciński

dr hab., prof. KA, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0001-6917-5501

III Multidyscyplinarne Autorskie Seminarium Naukowe *Modus Securitas* „Determinanty skuteczności zarządzania bezpieczeństwem państwa i biznesu – koncepcje, modele, podejścia, praktyka, wizje, wyniki badań", Dwór Rychwałd, 22–23.09.2019 r.

W dniach 22–23 września 2019 r. w Dworze Rychwałd w Beskidzie Żywieckim miały miejsce obrady III Multidyscyplinarnego Autorskiego Seminarium Naukowego *Modus Securitas* pt. „Determinanty skuteczności zarządzania bezpieczeństwem państwa i biznesu – koncepcje, modele, podejścia, praktyka, wizje, wyniki badań". Tak jak w przypadku dwóch poprzednich edycji, pomysłodawcą oraz organizatorem obrad był dr hab. Mirosław Kwieciński, prof. Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. Seminarium organizowane było przy współudziale Fundacji Instytut Wywiadu Gospodarczego w Krakowie oraz dzięki wsparciu przedstawicieli lokalnego środowiska przedsiębiorców.

Wiodącymi tematami III edycji seminarium były:

– Zarządzanie bezpieczeństwem w obliczu zmian klimatycznych. Czy to początek końca znanej nam cywilizacji?
– Dylematy kształtowania i zachowania etosu funkcjonariusza służb państwowych. Czy grozi nam upadek etyki?

Poruszana tematyka, która cieszy się nadal wielkim zainteresowaniem zarówno wśród akademików, jak i służb oraz przedstawicieli świata biznesu, zwróciła uwagę blisko 25 uczestników. Środowisko akademickie reprezentowali przedstawiciele ośrodków z Warszawy, Łodzi, Krakowa, Wrocławia, Katowic i Bielska-Białej. Zgodnie

z zamierzeniami organizatora zasadniczym celem obrad było przedyskutowanie wyselekcjonowanych problemów dotyczących determinant skutecznego zarządzania bezpieczeństwem państwa oraz biznesu.

Zwyczajem stało się skoncentrowanie uwagi uczestników wykładu inauguracyjnego na jak najbardziej aktualnym problemie teorii i praktyki zarządzania bezpieczeństwem. W tym roku seminarium otworzył, w zastępstwie nieobecnego prelegenta mgr. Janusza Libera, dr hab. Mirosław Kwieciński, który przedstawił referat pt. *Przełom w zarządzaniu bezpieczeństwem w polskim biznesie. Ustawowe regulacje cywilizujące działalność podmiotów zbiorowych (spółek) oraz nowa perspektywa aktywności służb specjalnych*. Prelekcja stanowiła interesujący przekaz projektowanych zmian wraz z ich szerokimi konsekwencjami w przepisach dotyczących zgodności (*compiliance*) w spółkach, w tym w małych przedsiębiorstwach sektora MSP. Omawiane zagadnienie spotkało się z dużym zainteresowaniem ze strony uczestników.

W dalszej części seminarium przeprowadzono dyskusję w ramach I sesji pod hasłem: *Zarządzanie bezpieczeństwem w obliczu zmian klimatycznych. Czy to początek końca znanej nam cywilizacji?*. Obradom przewodniczył Dziekan Wydziału Zarządzania i Komunikacji Społecznej Krakowskiej Akademii, dr hab. Dariusz Fatuła, prof. KA. W panelu wygłoszono następujące referaty:

– *Kierunki przeobrażeń modelu zarządzania kryzysowego w samorządzie terytorialnym wobec zmian klimatu*, dr hab. inż. Katarzyna Sienkiewicz-Małyjurek, prof PŚ (Politechnika Śląska w Gliwicach);
– *Dylematy zarządzania obszarem bezpieczeństwa infrastruktury kolejowej wobec ocieplenia klimatu*, dr hab. inż. Adam Jabłoński, prof. WSB (Wyższa Szkoła Bankowa w Poznaniu, Wydział Zamiejscowy w Chorzowie).

Dwa kolejne referaty: *Wizja oferty produktów firm ubezpieczeniowych wywołana zmianą klimatu* dr. Wojciecha Topczewskiego (Prudential Polska SA) oraz *Ryzyko w zarządzaniu łańcuchem dostaw sektora FMCG w warunkach wzrostu temperatury powietrza – studium przypadku na przykładzie wybranych produktów* mgr. Janusza Libera (Fundacja Instytut Wywiadu Gospodarczego) nie zostały zaprezentowane z powodu nieobecności prelegentów. Okoliczność ta dała asumpt do podjęcia ożywionej dyskusji na wysokim poziomie merytorycznym nad wygłoszonymi referatami, z czego bardzo zadowoleni byli zarówno prelegenci, jak i sami uczestnicy dyskusji.

Różnorodność problematyki bezpieczeństwa kontynuowana była w ramach II sesji pt. *Dylematy kształtowania i zachowania etosu funkcjonariusza służb państwowych. Czy grozi nam upadek etyki?* toczącej się pod przewodnictwem dr hab. Zofii Wilk-Woś, prof. SAN, dyrektor Instytutu Bezpieczeństwa Narodowego Społecznej Akademii Nauk w Łodzi. Uwaga uczestników skoncentrowała się na następujących referatach:

– *Wybrane zagadnienia zarządzania służbami mundurowymi w związku z ustawą o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych*, płk SG w st. spocz. mgr Mirosław Hakiel (Wyższa Szkoła Bankowa w Bydgoszczy);
– *Etyka w podatkach*, dr Ryszard Bełdzikowski (Wyższa Szkoła Finansów i Prawa w Bielsku-Białej).

Oba wystąpienia były okazją do ożywionej dyskusji na temat znaczenia zarówno „miękkich", jak i „twardych" narzędzi zachowania bezpieczeństwa w systemie bezpieczeństwa państwa.

Obrady seminarium naukowego wieńczyła sesja III *Założenia naukowo-organizacyjne Letniej Szkoły Zarządzania Bezpieczeństwem 2020*, której przewodniczył prof. zw. dr hab. Andrzej Chodyński (KA). Uczestnicy obrad zgodnie potwierdzili istnienie potrzeby oraz wolę przeprowadzenia nowatorskiego przedsięwzięcia w postaci projektu Letniej Szkoły Zarządzania Bezpieczeństwem. Wypracowano pierwsze założenia programowo-organizacyjne, powołując jednocześnie do życia grupę inicjatywną. W jej skład weszli przedstawiciele: Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Społecznej Akademii Nauk w Łodzi, Uniwersytetu Ekonomicznego w Krakowie, Uniwersytetu Pedagogicznego w Krakowie, Wyższej Szkoły Ekonomiczno-Humanistycznej w Bielsku-Białej, Wyższej Szkoły Finansów i Prawa w Bielsku-Białej oraz Fundacji Instytut Wywiadu Gospodarczego w Krakowie.

Przeprowadzona podczas seminarium ożywiona dyskusja udowodniła potrzebę kontynuacji badań, a także prowadzenia edukacji dotyczącej szeroko nakreślonego współczesnego fenomenu jakim jest bezpieczeństwo – podstawowa przesłanka bytu człowieka. Dobór tematyki wystąpień wskazał na istnienie wielu zagrożeń związanych ze zmianami klimatycznymi i wynikającej z nich potrzeby uczenia się życia na nowo. Dyskusja podkreśliła także wartość podejmowanych przedsięwzięć w celu poprawy poziomu bezpieczeństwa, szczególnie na rzecz uświadamiania znaczenia etycznych zachowań oraz praktyk w obszarze działań funkcjonariuszy państwa.

W opinii uczestników III edycja seminarium potwierdziła w pełni potrzebę spotkań naukowych skoncentrowanych na autorsko wyselekcjonowanej tematyce podejmowanej przez zaproszone grono ekspertów. Zebrani podkreślali wysoki poziom zarówno naukowy, ekspercki, jak i organizacyjny seminarium. Uczestnicy wskazali na potrzebę uruchomienia zorganizowanego przekazu zagadnień problematyki bezpieczeństwa dla wszystkich zainteresowanych osób w postaci letniej szkoły.

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-014

Jadwiga Mazur
dr hab., prof. UP, Uniwersytet Pedagogiczny w Krakowie
ORCID: 0000-0001-7766-7864

XXX Międzynarodowa Konferencja Naukowa „Socjologia grup dyspozycyjnych. Pomiędzy teorią nauk społecznych a praktyką", Wrocław, 9–10.05.2019 r.

Głównymi organizatorami XXX Międzynarodowej Konferencji Naukowej „Socjologia grup dyspozycyjnych. Pomiędzy teorią nauk społecznych a praktyką", która odbyła się w dniach 9–10 maja 2019 r. we Wrocławiu byli: Zakład Socjologii Grup Dyspozycyjnych Instytutu Socjologii Uniwersytetu Wrocławskiego, Akadémia Ozbrojených Síl gen. Milana Rastislava Štefánika ze Słowacji oraz Akademickie Koło Naukowe Security & Society IS UWr. Należy nadmienić, że było to również jubileuszowe wydarzenie naukowe, które uświetniło 10-lecie istnienia Zakładu Socjologii Grup Dyspozycyjnych.

Współorganizatorami wydarzenia byli: Zakład Socjologii Edukacji IS UWr, Polskie Towarzystwo Socjologiczne – Oddział Wrocławski, Sekcja Socjologicznych Problemów Bezpieczeństwa Narodowego PTS, Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Urząd Marszałkowski Województwa Dolnośląskiego, Starostwo Powiatowe we Wrocławiu oraz Safety Project.

Partnerami konferencji były podmioty zaangażowane w budowę systemu bezpieczeństwa: Dolnośląskie Wodne Ochotnicze Pogotowie Ratunkowe, Górskie Ochotnicze Pogotowie Ratunkowe Grupa Wałbrzysko-Kłodzka, Górskie Ochotnicze Pogotowie Ratunkowe Grupa Karkonoska, Państwowa Straż Pożarna, Pogotowie Ratunkowe, Policja Dolnośląska, Ratownictwo Wodne Rzeczypospolitej, Służba Więzienna, Straż Graniczna, Lotnicze Pogotowie Ratunkowe, Drogowe Ochotnicze Pogotowie Ratunkowe, Grupa Ratownictwa Specjalistycznego OSP Wisznia Mała, Grupa Ratownictwa Specjalistycznego OSP Starówka, Starostwo Powiatowe w Nysie i Starostwo Powiatowe we Wrocławiu.

Patronat honorowy nad wydarzeniem objął Prezes Najwyższej Izby Kontroli Krzysztof Kwiatkowski, a patronat medialny dwumiesięcznik „Ochrona Mienia i Informacji".

Od blisko 30 lat konferencja stwarza możliwość prowadzenia twórczych dyskusji nad bezpieczeństwem i wypracowywania nowych perspektyw poznania i opisu rzeczywistości społecznej w tym obszarze. Jak wskazują organizatorzy, głównym adresatem spotkań i zarazem rozważań konferencyjnych są grupy dyspozycyjne lokowane w zinstytucjonalizowanych przestrzeniach społecznych. Wskazuje się także na ich aktywne zaangażowanie w budowanie nauki, która w swoim założeniu ma wpływać na wzmacnianie bezpieczeństwa jako dobra wspólnego.

Tematy podejmowane podczas XXX edycji konferencji skupiały się wokół kwestii bezpieczeństwa, które (współ)kształtuje praktyki życia codziennego. Organizatorzy zgodnie z tytułem zaadresowali ją zarówno do środowisk naukowych, jak i władz samorządowych, terenowych organów administracji rządowej, instytucji publicznych, organizacji pozarządowych i przedstawicieli biznesu. Konferencja stała się w ten sposób wielowymiarową płaszczyzną wymiany rozważań i wyników badań naukowych połączonych z doświadczeniami praktyków zaangażowanych zawodowo i biznesowo w sferę zarządzania bezpieczeństwem.

Formuła konferencji zakładała 9 modułów tematycznych, które miały sprzyjać twórczym dyskusjom i wymianie doświadczeń. Zaproszeni uznani naukowcy i praktycy z dziedziny bezpieczeństwa dążyli do wypracowania wniosków z zakresu łączenia nauki i praktyki w tym zakresie.

W trakcie uroczystego otwarcia konferencji podpisano porozumienie o współpracy International Police Association pomiędzy Policją Republiki Włoskiej (płk dr Orazio Anania), Policją Polską oraz Policją Republiki Rumunii.

Wykład inauguracyjny wygłosił prof. dr hab. Kazimierz W. Frieske, który mówił o nowym paradygmacie badań nad stosowaniem wiedzy naukowej w praktyce. W panelu dyskusyjnym pt. *Praktyczno-prawne aspekty zapewnienia poczucia bezpieczeństwa mieszkańców powiatów* uczestnicy podzielili się posiadanymi doświadczeniami w zakresie organizacji bezpieczeństwa i poczucia bezpieczeństwa wśród mieszkańców. Wśród głównych dyskutantów byli: Roman Potocki – Starosta Powiatu Wrocławskiego; mł. insp. Jacek Taboł, b. z-ca Miejskiego Komendanta Policji; Grzegorz Miś – Powiatowy Rzecznik Konsumentów oraz Beata Pierzchała – Dyrektor Wydziału Organizacyjno-Prawnego (moderator panelu).

Pierwsza sesja plenarna dotyczyła m.in. kwestii związanych z bezpieczeństwem jako przedmiotem badań naukowych; aktualnych problemów w edukacji zawodowej żołnierzy zawodowych w siłach zbrojnych Republiki Słowackiej; bezpieczeństwa w społeczeństwie ponowoczesnym, ze wskazaniem na jego główne cechy i konsekwencje dla budowy systemów bezpieczeństwa. Przedstawiono także ważny problem funkcjonowania grup dyspozycyjnych z perspektywy społecznej odpowiedzialności. W sesji zwrócono uwagę na kwestie związane z fake newsami i dezinformacją powodującą w konsekwencji ryzyko dla bezpieczeństwa. Poruszono tematykę grup dyspozycyjnych jako zasadniczego elementu sprawnie funkcjonującego państwa, a następnie wskazano różnice między niebezpieczeństwem percypowanym a bezpieczeństwem zaawansowanym. Podjęto również rozważania dotyczące terroryzmu islamskiego.

W sesji drugiej rozmawiano na temat migracji jako wyzwania dla bezpieczeństwa narodowego Polski oraz ewolucji zagrożeń dla bezpieczeństwa publicznego stanowiącego wyzwanie dla grup dyspozycyjnych. Omówiono także wybrane przykłady dezinformacji społecznej w strategicznych inwestycjach publicznych. Problematykę tę kontynuowano w sesji trzeciej i rozważaniach dotyczących walki (wojny) informacyjnej jako przykładu broni nieśmiercionośnej. Kolejne wystąpienia poruszały m.in. tematykę społeczno-ekonomicznych aspektów obecności jednostek wojskowych w gminach z perspektywy terytorialnej i organizacyjnej. Dyskusja dotyczyła również problematyki edukacji w zakresie bezpieczeństwa i nowych wyzwań, które się przed nią pojawiają.

Drugiego dnia konferencji rozmawiano m.in. na temat: kultury bezpieczeństwa, tworzenia wizerunku grup dyspozycyjnych, a także bezpieczeństwa państwa i bezpieczeństwa społecznego, w tym dylematów francuskich sił porządkowych po latach stanu wyjątkowego i wybuchu ruchu żółtych kamizelek na tle kryzysu instytucji europejskich.

Nie pominięto również kwestii udziału organizacji pozarządowych w systemie wsparcia bezpieczeństwa w lokalnych społecznościach, a także jego społecznego i zdrowotnego kontekstu. Ważnym zagadnieniem było również łączenie społecznej teorii z praktyką z perspektywy doskonalenia działania europejskich organów ścigania.

Wartością dodaną konferencji było spotkanie przedstawicieli dwóch perspektyw – teoretycznej i praktycznej. Pozwoliło to na opracowanie końcowych wniosków zarówno poszczególnych sesji, jak i całej konferencji. Wskazują one na potrzebę dalszych spotkań i dyskusji dotyczących bezpieczeństwa, które mogą przybrać w przyszłości wymiar konkretnych badań oraz dalszych rozważań teoretycznych, w tym rozważań pozwalających na tworzenie nowych perspektyw badawczych i rozwiązań zastosowanych w praktyce.

Ponadto należy podkreślić, że dzięki dużej liczbie uczestników konferencji, zarówno z kraju, jak i z zagranicy (Włoch, Francji, Ukrainy, Słowacji czy Rumunii), może być ona elementem kreowania nowego typu bezpieczeństwa, które zgodnie z ogólnymi wnioskami z konferencji należy traktować holistycznie i dążyć do modyfikacji jego istniejących systemów i podsystemów. Długą tradycję wrocławskich spotkań konferencyjnych z pewnością warto kontynuować.

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-4-015

Mirosław Kwieciński

dr hab., prof. KA, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
ORCID: 0000-0001-6917-5501

IX Konferencja Naukowa „Bezpieczeństwo i zarządzanie kryzysowe", Społeczna Akademia Nauk w Łodzi, Łódź, 18–19.09.2019 r.

W dniach 18–19 września 2019 r. w siedzibie Społecznej Akademii Nauk w Łodzi miała miejsce dziewiąta edycja konferencji naukowej, tym razem zorganizowana pod hasłem „Bezpieczeństwo i zarządzanie kryzysowe". Po raz pierwszy jednak jej organizatorami były trzy instytucje: Instytut Bezpieczeństwa Narodowego i Katedra Zarządzania Społecznej Akademii Nauk w Łodzi, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego oraz Fundacja Instytut Wywiadu Gospodarczego w Krakowie.

Jak co roku, głównym celem konferencji była dyskusja i wymiana doświadczeń w gronie przedstawicieli środowiska naukowego oraz praktyków bezpieczeństwa i zarządzania kryzysowego, którzy wywodzą się ze służb, administracji i świata biznesu. Zamysłem dziewiątej edycji konferencji było poświęcenie szczególnej uwagi problematyce zarządzania bezpieczeństwem na poziomie lokalnym oraz zagadnieniom roli wywiadu i kontrwywiadu w praktyce biznesu. Organizatorzy przewidzieli szczegółowy zakres tematyczny, do którego należały następujące kwestie:

– zarządzanie bezpieczeństwem na poziomie lokalnym;
– bezpieczeństwo społeczności lokalnych;
– programy prewencyjne w budowaniu bezpieczeństwa społeczności lokalnych;
– wywiad i kontrwywiad w praktyce biznesu (specjalny panel);
– zarządzanie kryzysowe i ratownictwo;
– ochrona informacji niejawnych;
– współpraca cywilno-wojskowa;
– przygotowania do militaryzacji;
– polityka bezpieczeństwa, w tym strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej;

– planowanie operacyjne i programowanie obronne;
– realizacja zadań na rzecz Sił Zbrojnych Rzeczypospolitej Polskiej i wojsk sojuszniczych;
– ochrona ludności w warunkach prowadzonych działań obronnych;
– ochrona obiektów kultury szczególnie cennych dla dziedzictwa narodowego.

Otwarcia obrad dokonała dr hab. Zofia Wilk-Woś, prof. SAN, dyrektor Instytutu Bezpieczeństwa Narodowego Społecznej Akademii Nauk w Łodzi. Zwróciła uwagę na pewne nowe aspekty organizacji konferencji, które wynikają z powiększenia się liczby jej organizatorów, co daje podstawy do dalszej współpracy. W tym duchu przewodnicząca obrad poprosiła przedstawicieli poszczególnych organizatorów o wypowiedź na temat *Perspektywy współpracy oraz możliwości wspólnych badań i działań w obszarze bezpieczeństwa i zarządzania kryzysowego*. Głos zabrali kolejno:
– dr hab. Mirosław Kwieciński, prof. KA, Prezes Zarządu Fundacji Instytut Wywiadu Gospodarczego;
– prof. zw. dr hab. Sławomir Mazur, Dziekan Wydziału Nauk o Bezpieczeństwie KA;
– dr hab. Piotr Rozwadowski, prof. SAN.

W kolejnej części konferencji, którą był panel *Bezpieczna Europa?* podjęto interesujące i aktualne zagadnienia o wielowątkowej treści. Wystąpili:
– dr hab. Bogdan Panek, prof. SAN i dr hab. Mirosław Banasik, prof. Uniwersytetu Jana Kochanowskiego w Kielcach z referatem *Przyszłość Europy i konsekwencje dla polskiej polityki bezpieczeństwa i obrony – dwugłos*;
– dr Krzysztof Skusiewicz (SAN), *Od „Cara Puszki" do „Łoszarika". O słabości Rosji i jej konsekwencjach dla bezpieczeństwa europejskiej.*

W obu przypadkach referaty wywołały burzliwą dyskusję już w trakcie ich prezentacji.

W dalszej części przedpołudniowych obrad interesujący referat pt. *Modelowanie zagrożeń bezpieczeństwa i porządku publicznego – propozycja metodyczna* przedstawił dr hab. Janusz Ziarko, prof. KA. Wystąpienie stanowiło kolejną okazję do ożywionej dyskusji dotyczącej obszaru metodologii nauk o bezpieczeństwie.

Autorem ostatniego wystąpienia przed przerwą obiadową był dr hab. Piotr Rozwadowski, prof. SAN, który wygłosił referat *Kaszmir 2019 – eskalacja konfliktu czy próba stabilizacji. Zarządzanie kryzysowe na terenach spornych.*

Druga część obrad stała się domeną specjalistów praktyków w ramach specjalnie przygotowanego przez Fundację Instytut Wywiadu Gospodarczego panelu *Wywiad i kontrwywiad w praktyce biznesu*. Również w tej części konferencji uczestnicy podjęli momentami bardzo ożywioną dyskusję. Z kolejnymi referatami wystąpili:
– mgr Zdzisław Mazurski (Perfect Business Consulting, Warszawa), *Wywiad i kontrwywiad w działalności agencji detektywistycznych*;
– mgr Janusz Liber (Fundacja Instytut Wywiadu Gospodarczego), *Kontrwywiad biznesowy jako jeden z elementów bezpieczeństwa korporacyjnego na przykładzie międzynarodowych organizacji*;
– dr Ryszard Bełdzikowski (Wyższa Szkoła Finansów i Prawa w Bielsku-Białej), *Aktualne zagrożenia bezpieczeństwa rozwoju społecznego na Podbeskidziu. Problem lokalny czy systemowy?*.

Rzeczowego podsumowania panelu dotyczącego wywiadu i kontrwywiadu gospodarczego podjął się gen. bryg. (rez.) Paweł Pruszyński, pracownik naukowy SAN w Łodzi, Filia w Warszawie, były zastępca Szefa Agencji Bezpieczeństwa Wewnętrznego, który w znakomity analityczny sposób omówił walory, ale także dyskusyjne elementy przedstawionych wystąpień.

Drugi dzień obrad wypełniony został referatami kolejnych uczestników. Głos zabrali:
– prof. zw. dr hab. Sławomir Mazur (KA), *Zadania Sił Zbrojnych w zarządzaniu kryzysowym Polski*;
– dr hab. Jadwiga Mazur, prof. UP (Uniwersytet Pedagogiczny im. KEN w Krakowie), *Bariery i czynniki wspierające w realizacji wybranych programów profilaktycznych w ocenie ich beneficjentów na przykładzie miasta Łódź*;
– mgr Barbara Standarska, doktorantka (KA), *Nowe zastosowanie bezzałogowych statków powietrznych podczas realizacji zadań militarnych dla zwiększenia bezpieczeństwa społeczności lokalnej*;
– dr hab. Monika Ostrowska, prof. KA i dr Cezary Podlasiński, prof. KA, *Patrole rozminowania w systemie zarządzania kryzysowego*;
– dr Michał Stępiński (SAN), *Wpływ ustawy o działaniach antyterrorystycznych na funkcjonowanie instytucji, organizacji, przedsiębiorców i osób fizycznych*;
– mgr Marek Krzywonos, doktorant (KA), *Działania interesariuszy wewnętrznych i zewnętrznych w poprawie bezpieczeństwa drogowego transportu towarów na terenie UE.*

Szerokie spektrum poruszanej problematyki wywołało falę ożywionej dyskusji. Uczestnicy konferencji w liczbie blisko 25 osób potwierdzili ogromne pożytki płynące z kolejnej okazji do wymiany doświadczeń, myśli i rezultatów badań. Efektem obrad będzie publikacja zawierająca referaty wygłoszone podczas konferencji.

Informacje dla Autorów
Information for Authors
Informationen für Autoren
Информация для авторов

BEZPIECZEŃSTWO • TEORIA I PRAKTYKA 2019 nr 4
e-ISSN 2451-0718
ISSN 1899-6264
strona internetowa: btip.ka.edu.pl

Instrukcja przygotowania artykułów do czasopisma „Bezpieczeństwo. Teoria i Praktyka”

Formatowanie i redagowanie

Tekst artykułu (objętość ok. 12–20 stron) powinien być złożony pismem Times New Roman o wielkości 12 punktów z interlinią 1,5. Terminy i wyrażenia obcojęzyczne oraz tytuły artykułów i książek należy pisać kursywą (*italic*). Nie należy stosować wytłuszczeń (bold). Nie należy stosować podkreśleń. Prosimy o konsekwentne stosowanie skrótów (np., r., w. itp.) w całym artykule. Jeśli artykuł podzielony jest śródtytułami na części, to prosimy rozpocząć od „Wprowadzenia”, a na końcu umieścić „Podsumowanie”. Nie ma potrzeby numerowania śródtytułów.

Ilustracje

Rysunki, wykresy i fotografie powinny być dostarczone na płytach CD lub pocztą elektroniczną w formie zeskanowanej lub jako elektroniczny plik w jednym z formatów: *.bmp, *.tif, *.jpg lub *.psd.

Ilustracje zaczerpnięte z innych prac i podlegające ochronie prawa autorskiego powinny być opatrzone informacją bibliograficzną w postaci odsyłacza do literatury, umieszczonego w podpisie rysunku (np. Źródło: N. Davies, *Europa. Rozprawa historyka z historią*, Kraków 1998, s. 123).

Tabele

Tabele należy umieszczać możliwie blisko powołania i numerować kolejno. Tabele tworzy się, stosując polecenie: *Wstawianie – Tabela*. Wskazane jest unikanie skrótów w rubrykach (kolumnach) tabel. Tekst w tabeli powinien być złożony pismem mniejszym niż podstawowy. Ewentualne objaśnienia należy umieścić w linii bezpośrednio pod tabelą, a nie w samej tabeli.

Przypisy

Obowiązują przypisy dolne, które należy tworzyć, stosując polecenie: *Odwołania* / *Wstaw przypis dolny.* W polu, które pojawi się na dole kolumny, wpisujemy tekst przypisu (pismo wielkości 8–9 pkt.).
Przykłady:

- publikacje książkowe
  S. Grodziski, *Habsburgowie*, [w:] *Dynastie Europy*, red. A. Mączak, Wrocław 1997, s. 102–136.
- artykuły w czasopismach
  S. Waltoś, *Świadek koronny – obrzeża odpowiedzialności karnej*, „Państwo i Prawo” 1993, z. 2, s. 16.

W przypisach do oznaczania powtórzeń można stosować terminologię łacińską lub polską, czyli: *op. cit*., *ibidem* (tamże), *idem* (tenże), *eadem* (taż). Bezwzględnie należy jednak zadbać o konsekwentny zapis i nie mieszać zapisu łacińskiego z polskim. Po adresie strony internetowej podajemy w nawiasie kwadratowym datę dostępu. W zapisie dat generalnie używamy cyfr arabskich.

Istnieje również możliwość nadsyłania tekstów o charakterze historycznym (do działu „Z kart historii”), recenzji oraz komunikatów i sprawozdań.

Recenzje

Autorzy piszący recenzje proszeni są o dostarczenie zeskanowanej okładki recenzowanej publikacji (może być w skali szarości), a także o umieszczenie w nagłówku recenzji następujących danych: autor i tytuł książki (ew. jej redaktor), tłumacz, nazwa wydawnictwa, miejsce i rok wydania, liczba stron. W przypadku publikacji obcojęzycznych mile widziany jest przekład ich tytułu.

Streszczenia

Prosimy Autorów o dostarczenie kilkuzdaniowych streszczeń artykułów w językach: polskim, angielskim i rosyjskim, wraz z tłumaczeniem tytułu artykułu.

Prosimy również o dołączenie krótkiej notki o autorze (tytuł/stopień naukowy, uczelnia/organizacja), a także oświadczenia, że artykuł nie był wcześniej publikowany ani że nie narusza on praw autorskich innych osób.

Teksty niespełniające powyższych wymogów będą odsyłane autorom z prośbą o uzupełnienie.

BEZPIECZEŃSTWO • 2019 nr 4
TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
strona internetowa: btip.ka.edu.pl

Podstawowe zasady recenzowania artykułów w czasopismach

1. Do oceny każdej publikacji powołuje się co najmniej dwóch niezależnych recenzentów spoza jednostki.
2. W przypadku tekstów powstałych w języku obcym co najmniej jeden z recenzentów jest afiliowany w instytucji zagranicznej innej niż narodowość autora pracy.
3. Rekomendowanym rozwiązaniem jest model, w którym autor(-rzy) i recenzenci nie znają swoich tożsamości (tzw. *double-blind review process*).
4. W innych rozwiązaniach recenzent musi podpisać deklarację o niewystępowaniu konfliktu interesów. Za konflikt interesów uznaje się zachodzące między recenzentem a autorem: bezpośrednie relacje osobiste (pokrewieństwo, związki prawne, konflikt), relacje podległości zawodowej, bezpośrednia współpraca naukowa w ciągu ostatnich dwóch lat poprzedzających przygotowanie recenzji.
5. Recenzja musi mieć formę pisemną i kończyć się jednoznacznym wnioskiem co do dopuszczenia artykułu do publikacji lub jego odrzucenia.
6. Zasady kwalifikowania lub odrzucenia publikacji i ewentualny formularz recenzencki są podane do publicznej wiadomości na stronie internetowej czasopisma lub w każdym numerze czasopisma.
7. Nazwiska recenzentów poszczególnych publikacji/numerów nie są ujawniane; raz w roku czasopismo podaje do publicznej wiadomości listę recenzentów współpracujących.

W trosce o rzetelność naukową i jakość publikowanych artykułów wydawnictwo wdraża procedurę zabezpieczającą przed zjawiskiem *ghostwritingu*. Zarówno *ghostwriting*, jak i *guest authorship* są przejawem nierzetelności naukowej.

Ghostwriting – autor/współautor publikacji wniósł istotny wkład w powstanie publikacji, nie ujawnia jednak swojego udziału jako jeden z autorów lub nie wymienia się jego roli w podziękowaniach zamieszczonych w publikacji.

Guest authorship – udział autora jest znikomy lub w ogóle nie miał miejsca, a pomimo to jest autorem/współautorem publikacji.

Redakcja informuje, że wszystkie wykryte przypadki *ghostwriting* i *guest authorship* będą demaskowane, włącznie z powiadomieniem odpowiednich podmiotów, a także będą dokumentowane wszelkie ujawnione przejawy nierzetelności naukowej.

ZACHĘCAMY DO PRENUMERATY

Zamówienia na prenumeratę prosimy kierować pocztą elektroniczną na adres: ksiegarnia@kte.pl lub faksem (nr 12 25-24-593).

Należy podać następujące dane:

– imię i nazwisko (nazwę) osoby (instytucji) zamawiającej

– adres zamieszkania (siedziby)

– numer identyfikacji podatkowej (NIP)

– adres, na który ma być przesyłane czasopismo

– liczbę kolejnych zamówionych numerów

– liczbę egzemplarzy każdego numeru.

Do ceny zostanie doliczony indywidualny koszt przesyłki.

Szczegółowe warunki prenumeraty
oraz formularz zamówienia dostępne pod adresem:
www.ka.edu.pl/ksiegarnia/czasopisma/bezpieczenstwo

W sprzedaży dostępne również inne czasopisma
Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego:

„European Polygraph”

„Krakowskie Studia Międzynarodowe”

„Państwo i Społeczeństwo”

„Studia Prawnicze”

„Studia z Dziejów Państwa i Prawa Polskiego”

Zapraszamy na stronę internetową kwartalnika

btip.ka.edu.pl

BEZPIECZEŃSTWO • 2019 nr 4 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
strona internetowa: btip.ka.edu.pl

Lista recenzentów za rok 2019

W 2019 roku artykuły zgłoszone do „Bezpieczeństwa. Teorii i Praktyki" opiniowali pod kątem ich naukowej przydatności do rozpowszechniania:

dr hab. Tadeusz Ambroży, prof. AWF
prof. dr hab. Ewa Bujwid-Kurek
dr hab. inż. Zbigniew Ciekanowski
dr hab. Anna Citkowska-Kimla, prof. UJ
płk dr hab. Leszek Elak
dr hab. Artur Gruszczak
dr hab. Małgorzata Kamola-Cieślik, prof. US
prof. dr hab. inż. Marian Kopczewski
dr hab. Michał Kosman
dr Przemysław Łukasik
prof. dr hab. Ewa Maj
dr hab. Justyna Miecznikowska
dr hab. Krzysztof Miszczak, prof. SGH
dr Kamilla Schoell-Mazurek
dr hab. Anna Szczepańska-Dudziak
dr hab. Małgorzata Świder, prof. UP
prof. dr hab. Krzysztof Tarka
dr hab. Aleksandra Trzcielińska-Polus, prof. UO
dr hab. Łukasz Wojcieszak
prof. dr hab. Waldemar Zubrzycki
dr hab. Krzysztof Żarna, prof. UR