KRAKOWSKA AKADEMIA IM. ANDRZEJA FRYCZA MODRZEWSKIEGO
ANDRZEJ FRYCZ MODRZEWSKI KRAKOW UNIVERSITY

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA

SECURITY
THEORY AND PRACTICE

BEZPIECZEŃSTWO BIZNESU. ASPEKTY ZARZĄDCZE

redakcja
Andrzej Chodyński

e-ISSN 2451-0718
ISSN 1899-6264

Kraków 2023
Nr 4 (LIII)

KRAKOWSKA AKADEMIA IM. ANDRZEJA FRYCZA MODRZEWSKIEGO
ANDRZEJ FRYCZ MODRZEWSKI KRAKOW UNIVERSITY

BEZPIECZEŃSTWO
TEORIA I PRAKTYKA

SECURITY
THEORY AND PRACTICE

BEZPIECZEŃSTWO BIZNESU. ASPEKTY ZARZĄDCZE

redakcja
Andrzej Chodyński

Kraków 2023
Nr 4 (LIII)

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE

e-ISSN 2451-0718
ISSN 1899-6264

2023
Nr 4 (LIII)

Redakcja/Office:
ul. Gustawa Herlinga-Grudzińskiego 1, A, pok. 215
30-705 Kraków
tel. (12) 25 24 665
btip.ka.edu.pl

Czasopismo punktowane w rankingu Ministerstwa Edukacji i Nauki oraz indeksowane w następujących bazach / The journal is ranked by the Ministry of Education and Science and indexed in the following bases:
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; EBSCO

e-ISSN 2451-0718
ISSN 1899-6264

Na zlecenie / Commissioned by:
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
www.ka.edu.pl

Wydawca / Publisher: Oficyna Wydawnicza KAAFM

BEZPIECZEŃSTWO SECURITY
TEORIA I PRAKTYKA THEORY AND PRACTICE
e-ISSN 2451-0718 2023
ISSN 1899-6264 Nr 4 (LIII)

Spis treści

ARTYKUŁY

VARIA

SPRAWOZDANIA

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-000

Andrzej Chodyński
prof. dr hab., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-4962-5143

Bezpieczeństwo biznesu. Aspekty zarządcze. Wprowadzenie

Współczesne przedsiębiorstwa funkcjonują w warunkach silnej turbulencji otoczenia. Skutki tej turbulencji przejawiają się w postaci możliwych kryzysów przedsiębiorstw, zarówno o charakterze ekonomicznym (m.in. w wyniku zawirowań na rynkach finansowych czy recesji), jak i pozaekonomicznym (wywoływanych przez wojny, katastrofy naturalne, terroryzm, skutki globalnego ocieplenia, pandemie itd.). Narastanie zjawisk o charakterze globalnym (pandemie, katastrofalne zjawiska naturalne, np. huragany, susze i trzęsienia ziemi) powoduje, że podmioty gospodarcze powinny wykazywać się zdolnościami o charakterze rezylientnym[1] – zapewniać sobie przetrwanie poprzez dostosowywanie się (na ile to możliwe) do występujących zmian.

Istotne znaczenie mają aspekty zarządcze związane z bezpieczeństwem przedsiębiorstwa (biznesu). Bezpieczeństwo jest rozpatrywane jako cecha przedsiębiorstwa przejawiająca się w jego zdolności do przeciwdziałania zdarzeniom zakłócającym funkcjonowanie tego podmiotu. Czynności związane z przeciwdziałaniem zdarzeniom negatywnym (zagrożeniom) zależą od czasu ich wystąpienia (przeszłego,

[1] Zachowania rezylientne opisano w publikacji: A. Chodyński, *Kryzys pozaekonomiczny przedsiębiorstwa – ekologiczny aspekt rezyliencji organizacyjnej*, [w:] *Zrównoważony rozwój, systemy informacyjne i zarządzanie bezpieczeństwem w perspektywie długoterminowej przedsiębiorstw*, red. A. Chodyński, D. Fatuła, M.A. Leśniewski, Oficyna Wydawnicza AFM, Kraków 2022, s. 11–31.

obecnego oraz przyszłego)[2]. Bezpieczeństwo przedsiębiorstwa jest rozpatrywane głównie z punktu widzenia zapobiegania ewentualnym stratom[3].

Kluczowa jest zatem odpowiedź na dwie grupy pytań. Grupa pierwsza, odnosząca się do rozważań o charakterze globalnym, obejmuje następujące zagadnienia:

- czy na poziomie kadry menedżerskiej występuje świadomość ryzyka związanego z zagrożeniami dla funkcjonowania biznesu i czy świadomość ta jest uwarunkowana kulturowo?
- czy znana jest i brana pod uwagę świadomość zagrożeń u partnerów biznesowych?
- czy znana jest i brana pod uwagę świadomość klientów odnośnie do zagrożeń oraz czy (i ew. jakie) działania w kontakcie z rynkiem są podejmowane przez organizacje biznesowe?
- na ile bezpieczeństwo i zapewnienie ciągłości działania biznesu jest zagrożone w związku ze skutkami globalnego ocieplenia? (huragany, powodzie, susze); jakie są działania firm w tym zakresie?
- w jaki sposób występujące zagrożenia wpłyną na prowadzone działania doradcze i szkoleniowe dla firm, w tym w zakresie zapewnienia bezpieczeństwa biznesu?

Druga grupa pytań dotyczy różnych aspektów zarządzania bezpieczeństwem na poziomie lokalnym oraz na poziomie konkretnych podmiotów. Przyjęto pogląd, że zarządzanie bezpieczeństwem przedsiębiorstwa stanowi proces zapobiegania, reagowania oraz korygowania mający na celu przeciwdziałanie zdarzeniom zakłócającym funkcjonowanie organizacji[4].

Zarządzanie bezpieczeństwem obejmuje nie tylko identyfikację potencjalnych zagrożeń, ale także podejmowanie przedsięwzięć mających na celu niedopuszczenie do ich wystąpienia, zaś w przypadku wystąpienia zagrożeń – odnosi się do podjęcia działań w zakresie ich kontroli, eliminacji, usunięcia skutków, a także wyciągnięcia wniosków na przyszłość. Proponuję zatem przyjąć, że zarządzanie bezpieczeństwem biznesu będzie zorganizowanym działaniem z użyciem dostępnych zasobów w celu zmniejszania potencjalnych zagrożeń i zapewnienia funkcjonowania podmiotu gospodarczego[5].

Odpowiedzi na pytania z pierwszej grupy zawarto w przeprowadzonej przez Andrzeja Chodyńskiego i Dariusza Fatułę rozmowie z czterema praktykami w zakresie

---

[2] P. Cabała, *Planowanie scenariuszowe w zarządzaniu bezpieczeństwem strategicznym przedsiębiorstwa*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków 2012 (Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie. Monografie, nr 213), s. 84.

[3] J. Konieczny, *Bezpieczeństwo państwa a bezpieczeństwo biznesu. Studium metodologiczne*, „Bezpieczeństwo. Teoria i Praktyka" 2015, nr 4, s. 17.

[4] P. Cabała, *Strategie zarządzania bezpieczeństwem przedsiębiorstwa w warunkach zagrożeń sektorowych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 420: *Strategie. Procesy i praktyki*, s. 36–45.

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

doradztwa biznesowego oraz szkoleniowego w skali globalnej, posiadającymi doświadczenie w USA, Gwatemali i Hiszpanii. Odniesiono się m.in. do problematyki świadomości menedżerskiej dotyczącej możliwości wystąpienia zagrożeń (z uwzględnieniem aspektów kulturowych), zarządzania ryzykiem działalności biznesowej, roli partnerstwa strategicznego, wpływu katastrof na funkcjonowanie biznesu oraz tworzenia strategii rezyliencji z uwzględnieniem aspektów społecznych i ekologicznych. Do tych zagadnień odnoszą się także artykuły: Dominiki Marciniak (logistyka pomocy humanitarnej w sytuacji wojen, trzęsień ziemi czy chorób cywilizacyjnych), Mirosława Laszczaka (systemy cyberbezpieczeństwa) oraz Jadwigi Mazur (bezpieczeństwo hybrydowe i zapobieganie dezinformacji – rozważania wsparte konkretnym studium przypadku).

Na poziomie przedsiębiorstwa zarządzanie bezpieczeństwem odnosi się do następujących zagadnień:

- roli menedżera bezpieczeństwa (kwestię przedstawia artykuł Michała Adama Leśniewskiego),
- bezpieczeństwa projektów informatycznych (artykuł Piotra Komsty),
- problemów bezpieczeństwa społecznego na przykładzie młodych pracowników (artykuł Barbary Oliwkiewicz),
- bezpieczeństwa danych w systemach rachunkowości (artykuł Wojciecha Kozioła i Pawła Łojka);
- bezpieczeństwa danych w małej firmie (artykuł Mariusza Grzyba i Marty Woźniak-Zapór).

Oprócz opracowań dotyczących konkretnych problemów bezpieczeństwa biznesu, niniejszy numer BTiP zawiera także odniesienia do wybranych zagadnień bezpieczeństwa państwa: dział „Artykuły" kończy tekst Tomasza Banasika i Katarzyny Banasik o działalności konkretnej organizacji non-profit na rzecz obronności; w dziale „Varia" zamieszczono opracowanie dotyczące Wojsk Obrony Terytorialnej autorstwa Bartosza Włodarczyka.

Numer zamykają trzy sprawozdania z konferencji i seminariów na temat współczesnych zagrożeń dla bezpieczeństwa. Anna Bałamut oraz Krzysztof Waśniewski zaprezentowali sprawozdanie z konferencji Krynica Forum 2023, odbywającej się pod hasłem *Empowering the Region*. Panele dyskusyjne Forum odbywały się w ramach siedmiu „ścieżek programowych": Bezpieczeństwo strategiczne; Bezpieczeństwo energetyczne; Bezpieczeństwo klimatyczne; Ukraina – wsparcie, współpraca, odbudowa; Forum Koreańsko-Polskie; Biznes i gospodarka; Patrząc w przyszłość.

Anna Bałamut oraz Izabela Kapera przedstawiły wnioski dotyczące bezpieczeństwa i zarządzania nim wynikające z Ogólnopolskiej Konferencji Naukowej „Zarządzanie w układzie Przedsiębiorstwo–Miasto–Region w zmiennym otoczeniu. Wpływ współczesnych zagrożeń" (Kraków, 2023; organizatorzy: Krakowska Akademia im. Andrzeja Frycza Modrzewskiego oraz Towarzystwo Naukowe Organizacji

i Kierownictwa – Oddział w Kielcach przy udziale partnera: Politechniki Świętokrzyskiej – Wydziału Zarządzania i Modelowania Komputerowego).

Mirosław Kwieciński zaprezentował sprawozdanie z VI Multidyscyplinarnego Autorskiego Seminarium Naukowego *Modus Securitas*: „Determinanty skuteczności zarządzania bezpieczeństwem państwa i biznesu – koncepcje, modele, podejścia, praktyka, wizje, wyniki badań" (Rychwałd, 2023).

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
No. 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-00W

Interview with Bartolomeo Rafael Bialas, Hania Krück, Dr. Ioseb "Soso" Gabelaia, Miguel Blanco

Interviewers:
Professor Andrzej Chodyński; Dariusz Fatuła, PhD, DSc,
Associate Professor Andrzej Frycz Modrzewski Krakow University

Bartolomeo Rafael Bialas (Las Vegas, USA) is an international expert on brand management, strategic thinking, and consumer behavior. He has consulted for and worked with many business and government organizations, including MGM Grand Las Vegas, Wynn Las Vegas, The Rivers Casino in Pittsburgh, Goodwill Industries International, Aldec, White Square Gallery, ING Group, RDG Advertising, Keane Creative, Nevada Governor's Office Of Economic Development/International Trade and Diplomatic Protocol, Consulate General of the Republic of Poland in Los Angeles.

He has been a visiting professor at various universities around the world, including Belize, Guatemala, Poland, Latvia, Portugal, USA, Slovakia, Argentina, Hungary, UK, Croatia, Aruba. He has also lectured at the prestigious Craft Acting Studio co-founded by the actor and Emmy Award-Winner Brad Garrett. He is currently a visiting professor at Andzej Frycz Modrzewski Krakow University where he is teaching original content courses in Strategic Brand Management, Market Research, International Marketing, and Disruptive Business Models.

Hania Krück is a lawyer and notary graduated from Rafael Landívar University (Guatemala), with more than 14 years of experience in national and international intellectual property matters, with a specialization in Law & Digital Business from the

University of Salamanca (Spain). Director of Innova IP, the intellectual property division of the Guatemalan law firm A.D. Sosa & Soto. Visiting professor and speaker working for many organizations, including the World Intellectual Property Organization (WIPO). She has been rated and recognized internationally through the evaluations of the prestigious publications of The Legal 500 and Chambers and Partners.

Dr. Ioseb "Soso" Gabelaia is an assistant professor of Business Administration at the C.H. Sandage School of Business at Graceland University (USA). He is a marketing communication and management specialist with over 12 years of extensive experience. He is a Certified Six Sigma Master Black Belt (CSSMBB) and Master Scrum Accredited Certified (MSAC) committed to educating, coaching, and mentoring students/learners to achieve lifelong goals. He is a member of the American Marketing Association (AMA) and the European Marketing and Management Association (EUMMAS). Dr. Gabelaia holds a Doctor of Business Administration Degree with an emphasis in Marketing. Additionally pursuing a second doctoral degree in Education Leadership.

Dr. Gabelaia leads the Marketing and Management program at Graceland University. He is also involved in the development of the MBA program.

Miguel Blanco graduated in Business Administration from Rafael Landívar University (Guatemala), with a master's degree in Marketing Management and a master's degree in Local Development and Territorial Planning from the University of Valencia in Spain. He is currently pursuing a PhD degree in Social Economy at the University of Valencia. He has been a consultant on strategic planning, finance and family business management as well as a university professor and researcher.

Andrzej Chodyński, Dariusz Fatuła: Are businesspeople aware of the risks that can manifest themselves in areas other than the domestic/global economy? Is this awareness universally present? Would this awareness be affected by cultural factors?

Bartolomeo Rafael Bialas: It's easy to assume that every organization, every manager, every entrepreneur, every investor, and every management consultant wants to be aware of potential risks – and be prepared for the unexpected. Unfortunately, many businesspeople have persistent misconceptions about risk management. It's a common misconception that effective risk management significantly reduces risk factors that can lead to unmitigated market disasters. However – as Alla Valente, a senior analyst at Forrester Research said – "We don't manage risks so we can have no risk. We manage risks so we know which risks are worth taking, which ones will get us to our goal, which have enough of a payout to even take them." Therefore, businesspeople

must be aware of potential risks to stay vigilant to new sources of danger and loss. There is no doubt that global risks are currently making many CEOs anxious and jittered. The businesspeople I work with understand that there is a growing spotlight on sustainability, environmental, social, and governance issues. In January 2023, the World Economic Forum published the Global Risk Report[1] in which it described the consequences of climate inaction, deterioration of societal cohesion, and nature loss as the most pressing and critical risks on a global scale over the next 10 years. Given the complexity of today's global risks, organizations looking to grow internationally are increasingly turning to cross-cultural strategy consultants to better understand the global business environment, better protect their operations and supply chains, and better tackle the unexpected business challenges. I always tell my clients and my MBA students that in risk management the key is to plan early. There is no question that there are several competencies that businesspeople can cultivate to create a high-performance corporate culture that can significantly contribute to the development of forward-thinking, future-fluent, and risk-ready organization.

Another problem concerns the role culture plays in influencing people's risk assessment. Despite its critical importance, culture keeps being overlooked when thinking about risk management in business. Culture plays a profound role in business, management, and decision making. Culture influences people's risk assessment because it influences their subjective interpretation of what a risk, danger, or a hazard is and how they should respond to it. Culture also influences the local norms and risk tolerance levels. For example, what is considered too risky? Miami-Dade County for instance has a very high natural disaster risk score of 68%. As far as I remember, over the past 20 years, most of the disasters that transpired in that county were related to hurricane incidents. Simply put, people who live in Miami-Dade County are willing to endure a considerably high level of risk compared to people who live in other parts of the US. Numerous anthropologists and social psychologists have recognized that managers' thought patterns, actions – or inaction – are linked to culture. Cultural values and norms influence the willingness and readiness to accept, change, or discard risk assessment procedures. Although the influence of cultural factors is being debated in many academic fields, in business and strategic management there is still a strong focus on financial issues. I would contend that many businesspeople I work with lack cultural sensitivity and their ethnocentrism hinders them from learning about other cultures and potential sources of risk.

Hania Krück: From the legal perspective, it is my experience that businesspeople are transitioning into being more aware of risks, but there is still a long way to go. The corporate compliance programs produce guidelines, processes, and different forms of control that generate stable practices over time related to many areas of business such

[1] *Global Risks Report 2023*, WHO, 11 January 2023, https://www.weforum.org/publications/global-risks-report-2023 [accessed: 12.12.2023].

as taxes, labor, advertising, consumer protection, intellectual property, among others. The different mandatory, or voluntary, compliance programs have helped managers to become more aware of risks and take appropriate measures to reduce them, seeking continuous and sustainable improvement.

Cultural factors affect the awareness and consciousness of every individual, since some of the risks may be related – to a greater or lesser extent – to the local circumstances, regulations, and/or customs, beliefs, superstitions, prejudices, and convictions. In addition, in countries where the compliance culture dominates due to mandatory regulations, managers are more involved and aware of the risks. On the other hand, in countries in which integrating compliance programs to the business is relatively new, managers may not be fully aware of all the variety of risks, but it is my experience that managers – or businesspeople in general – who know their markets well, are very aware of the major risks – other than the domestic/global economy – that play important role in their industries.

Ioseb "Soso" Gabelaia: According to World Bank chronicles, economic activity in developed and emerging markets and developing economies (EMDEs) has shrunk since COVID-19 as domestic demand and supply, trade, and finance have been disturbed. Hence, businesspeople need to recognize market conditions' exposure, vulnerability, and volatility before or while developing resilience strategies. Therefore, we must refrain from conversations about price indexes, monetary policies, unemployment rates, exchange rates, interest rates, agriculture exports, and the availability of raw materials. Besides, risks related to the social, environmental, legal, political, and technological environment require businesspeople to be aware and to stay consistent with it. For example, climate change is a global phenomenon impacting local/global economies. Therefore, the physical risk which impacts economies varies based on region. Furthermore, remembering the impact COVID-19 had and continues to have on local and global economies. Moreover, technological advancements provide new threats to businesses.

As a professional applying the Six Sigma philosophy in various industries and practicing design thinking, businesspeople are aware of those risks; however, not about universal awareness. It varies due to the size of the business and its operations. Moreover, cultural factors should have a massive role in different geographic regions; we have different cultures, such as individualistic vs. collectivist. Therefore, decisions are made differently, especially in a post-pandemic environment.

Miguel Blanco: Today's entrepreneurs are perfectly aware of the different factors that affect their businesses. Another issue is, of course, how prepared they are to face and overcome them. The risk factors in the last two decades have multiplied, both due to the global connection of the markets, and due to the technological factors that change so rapidly. The best-prepared businessmen have had to migrate to the data and trend analysis tools, which help them anticipate transcendental changes in the

industry within which they operate. Numerous professional associations and chambers of commerce have been supporting – of course, to a certain extent – small and medium-sized entrepreneurs to have access to this type of market analysis through technological tools.

A. Chodyński, D. Fatuła: Do businesspeople consider the value of strategic alliances in order to stave off risk factors – other than economic – that can emerge precipitously and threaten the existence of their organizations?
B.R. Bialas: It's important to know that in recent years, strategic alliances have experienced rampant growth. This is due mostly to factors like new technology, desire to expand, and the increasing importance of innovative business models and ecosystems. Strategic alliances are multidimensional phenomena, typically involving intricate interactions between partners. Essentially, strategic alliances are defined as two or more organizations working together to accomplish a mutually beneficial objective. It's important to note that each participating firm preserves its autonomy and independence in a strategic alliance. Strategic alliances play a central role in strategic management. Organizations may use alliance strategies to enter into a new market, expand their customer base, experiment with new technology, grow business, or obtain a competitive advantage. Strategic alliances can also significantly contribute to economies of scale and increased market share.

What is interesting is that strategic alliances have evolved over the years. In the 1990s, competition and cooperation were mutually exclusive. Today, competition and cooperation – or so-called co-opetition – have become the staple of business practices. For example, Apple simultaneously competes and cooperates with Samsung, Ford competes and cooperates with GM, DHL competes and cooperates with UPS, and Google is competing and cooperating with Yahoo. Depending on the business reality one must face, one can opt for the expansion of the global sourcing activities. This can be done on either an intra- or an interfirm basis. More and more organizations rely on a wide variety of collaborative efforts to anticipate and adapt to the future more effectively. The fact is that organizations around the world are currently learning how to better leverage strategic alliances as important and effective vehicles for exploring new technologies, honing their unique skills and core competencies, and staving off risks and challenges. The problem with strategic alliances is that many managers tend to perpetuate a dangerous belief that strategic alliances can lead to short-term cost advantages. Quite the opposite, in fact, is true: strategic alliance strategy can become the source of sustainable competitive advantage. Strategic alliances can significantly contribute to the creation of a unique business ecosystem of strategic partnerships that can, in turn, lead to maximization of competitive advantages of all partners involved. For example, in 2014 Uber teamed up with Spotify to create car music playlist partnership. Another successful partnership was forged

between Red Bull and GoPro in 2016. This strategic alliance is deeply rooted in the DNA of these two brands: the sense of adventure and spontaneousness. As a result, Red Bull and GoPro can share the resources, promote content, increase their influence, and foray into the new markets. In 2014 BMW rolled out the i8. The i8 was the crème de la crème of all BMW vehicles. In order to effectively promote this technological marvel, BMW teamed up with Louis Vuitton. The basic rationale behind this partnership was – once again – deeply rooted in the same shared values of creativity, aesthetics, and perfectionism. Both organizations decided to test – and push – the envelope on what technology and style can do in culture.

There is no doubt that strategic alliances allow partners to learn and acquire from each other the skills, knowledge, design, products, technologies, and customers that are not otherwise available to them, and – even more importantly – to their rivals.

I can't stress enough how important it is for participating partners to clearly understand and articulate the range of the risks inherent in the strategic alliance. There is an old Chinese proverb that perfectly captures the dark side of strategic alliances: "One bed, different dreams." In order to fully leverage the enormous potential of strategic alliances, they must be managed by managers who "dream the same dreams". Organizations combining resources in unique ways by leveraging strategic partnerships may develop a competitive advantage over rivaling organizations that are unable or unwilling to do so.

H. Krück: Strategic alliances are determining factors to face a wide variety of business challenges, such as growth, expansion, transformation, sustainability, access to financial capital, synergies, competitiveness, and, also, staving off risk factors.

As far as I remember, there was an article published in 2016 written by Antonio de Oliveira, Felipe Mendes Borini, Roberto Carlos Bernardes, and Mauro de Oliveira[2], who asserted that strategic alliances are not only useful to large companies, but also to small and medium sized companies, since they provide opportunities to learn new capabilities related, for example, to technology, or to reduce costs and risks associated with innovation.

Strategic alliances can be used by partners that have different levels of power, for example between a well-established company and a small-sized company. Therefore, it is important to note that strategic alliances *per se* may also represent business risk, depending on the position in the alliance. That is why, in order to manage the risk, strategic alliances also require planification, clarity on the expected results, performance standards, and from the legal standpoint, clear and written conditions among parties.

---

[2] A.B. de Oliveira Junior, F.M. Borini, R.C. Bernardes, M.J. de Oliveira, 'Impact of Entrepreneurial Orientation on Strategic Alliances and the Role of Top Management', *Revista de Administração de Empresas*, 2016, vol. 56, no. 3, pp. 315–329, https://www.scielo.br/j/rae/a/5GvymdWTWZN7sFD5Gck7shD/?format=pdf&lang=en [accessed: 12.12.2023].

I. Gabelaia: Short statement – strategic alliance is a must-do in today's volatile business and economic environment. Businesspeople need help to sustain their local or global operations due to scarcity of raw materials, complicated supply chain operations, etc. I have experienced seeing business benefit and strengthen their presence and operations through strategic alliances. However, I also have seen businesses file for bankruptcy.

Many businesspeople struggle to create or accept strategic alliances due to their complexity. And with complexity, I mean the pros and cons of cooperation. For example, on one side, this partnership might be strategic or political to create a competitive advantage. On the other hand, it might be costly, or/and uneven power distribution where in alliance, one has more power and would create a disadvantage, miscommunication, etc. However, to fight all risk factors such as the social, environmental, legal, political, and technological, and be sustainable a strategic alliance is a must-do.

M. Blanco: Strategic alliances have always played a fundamental role in business success, whether they are used to reach international markets, grow businesses, or face competition in the local market. Entrepreneurs are aware of the importance of creating strategic alliances to add value to their business models. They understand that strategic alliances should be viewed as a key management tool for survival and future success.

A. Chodyński, D. Fatuła: Is there a need among managers to monitor their client's knowledge about the risk factors other than economic?

B.R. Bialas: Let's start with the functions of management. At the most fundamental level, management concerns five functions: planning, organizing, staffing, leading, and controlling. After strategies are formulated and plans are established, management's primary task is to ensure that these strategies and plans are executed and/or altered. This is the critical control function of management. Risk is part of any business and access to the right information is of paramount importance. Effective controlling is entirely dependent on the quality of information. In this brave new noisy and digital world, one truth holds true: Information overload reduces managers' capacity to function effectively, which, in turn, can lead to poor decisions. In other words, managers need the ability to access accurate information, make sound decisions, and compare their actual business processes with the intended ones, and validate that everything is in order at any given time. This, of course, requires continuous and – ideally – automated data discovery in order to buttress up-to-date flow mapping. Moreover, today organizations must focus on data verification. In a nutshell, data verification involves performing a check of the current data to ensure that it is accurate, consistent, and reflects its intended purpose.

In this context, monitoring and ascertaining a client's knowledge becomes a prerequisite to fostering a full understanding of the business ecosystem. Let's be honest:

Knowledge is power, and understanding your client's knowledge, concerns, fears, and strategic outlook will give your organization a competitive edge. Moreover, understanding how your organization fits into your client's overall strategic objectives is absolutely necessary for its success. This is especially important in the B2B segment. If organizations don't know their role in client relationships, they run the risk of underperforming. However, with the constant deluge of unverified information, it has become hard to keep track of all the ways in which organizations can get to know their clients better. Nevertheless, every organization must learn everything there is to learn about their clients' knowledge, strategies, concerns, and challenges. By understanding your clients' knowledge, your chances of losing a client dwindle, and you will be better equipped to face mutual challenges and risks.

H. Krück: Businesses seek to satisfy their client's needs with products or services. Therefore, managers need to know and understand everything about their clients, including the client's knowledge about risk factors. Acknowledging and understanding the clients' knowledge allows managers to implement, maintain, or adjust business strategies.

In addition, clients' loyalty is fundamentally a result of trusting the business. Being aware of what the client considers as risk factors allows the company to inform and implement measures to reduce or eliminate the risk factors and make sure the client feels safe.

As a lawyer, it is my experience that my clients' knowledge about risk factors, other than economic, is mostly – and unfortunately – limited. It is also true that 'risk factors' is a very generic label. The truth is that different types of risk are related to many different aspects of the business, including jurisdiction, so it is very difficult to have absolute control over them. Therefore, it is very common that managers focus on just a few risk areas. However, sometimes the risk factors they consciously – or unconsciously – neglect to monitor can represent a considerable legal and financial liability, or they could be underestimating the value of some categories of assets: intangible assets illustrate this perfectly well.

I have had various experiences with global corporations underestimating the risk of a not well-planned marketing campaign, or a marketing campaign launched without legal clearance. In one of the cases, third parties considered themselves affected by a marketing campaign, and in the other case, the marketing campaign was already launched, and it did not fulfill the local requirements for the type of products they advertised. In both cases, it had a tremendous – and adverse – financial impact, and the marketing campaigns had to be removed. Both situations could have been prevented, but the businesses ended up wasting money, time, and effort.

In addition, as an intellectual property lawyer, I have also had experience with companies that lack understanding on this matter, which has many consequences as: investing time and resources in trademarks that cannot be registered or used, the need

to change the trademark name and image after being launched, lack of information security which results in disclosed trade secrets, data privacy breach, unfair competition, among many others.

In consequence, the lack of legal knowledge adversely affects the performance of the business, and inevitably increases the business risks.

I. Gabelaia: What a great question. We usually monitor our competition and see how they perform in the face of complex market conditions. Nevertheless, looking at clients is another approach that is a must-do. As we all know, business has moved from product-based to customer-based approaches. Businesses now practice data-based, evidence-based, and just-in-time data to make smart and measurable decisions. Measuring a client's knowledge is massive in this context, as managers can learn much from them. Using facts, data, and metrics will enable us to align them with strategic organizational objectives or initiatives.

Clients can provide and suggest current societal, political, or technological trends. Consequently, managers need to measure this information using various tools such as Power BI, tableau, etc. Today, monitoring data is massive, and if managers apply this to operations and develop strategies based on that, it will be phenomenal.

M. Blanco: Monitoring the knowledge of customers is essential, especially monitoring their tastes and preferences. In addition to knowing the customer's opinion in reference to our products and services, this allows us to know the satisfaction of our customers in order to make what we offer more competitive in the market. This real-time monitoring is of great importance to adapt the organization's strategies and anticipate the competition.

A. Chodyński, D. Fatuła: Do managers take action (for example, marketing campaigns) in order to deter the emergence of a crisis other than economic?

B.R. Bialas: In recent years, there has been a shift in consumption habits as consumers become savvier and more belief-driven. Building a strong brand requires more than manufacturing a great product or service. Building a strong brand – one characterized by longevity – requires focusing on values. Today's consumers want to know what your brand stands for, what your brand values and believes in. Today's consumers are less budget-conscious and more socially-conscious. This means that they are actively searching for brands that inspire by changing the world. According to the 2018 Edelman Earned Brand report[3], 1 in 2 people are belief-driven. This means that they select, switch, avoid or boycott a brand based on its stand on social issues. 67% of consumers buy a brand because of its position on a controversial issue. This belief-driven mindset spans generations and income levels. More and more

[3] *Brands Take a Stand*, Edelman Earned Brand Global Report, October 2018, https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Earned_Brand_Global_Report.pdf [accessed: 12.12.2023].

consumers believe that brands can be a powerful force for social and environmental change. 46% of consumers believe that brands have better ideas for solving a country's problems than government. 53% of consumers believe that brands can do more to solve social and environmental problems than government. Every organization must select, cultivate, articulate, and promote ideals and values that resonate emotionally and intellectually with consumers. Unfortunately, the vast majority of brands have trouble doing this well – if they do it at all. According to the 2019 Axios/Harris poll[4], consumers want and support brands that promise a better future. Global brands that are perceived as monolithic corporate goliaths, ignoring social and environmental issues, will find themselves facing rivalry from purpose-driven brands that embrace strong values and ideals, and are involved in social and political issues.

In 2022 the world experienced an unprecedented number of disasters, both natural and humanitarian: hurricanes, floods, wildfires, wars. More and more organizations are talking about purpose-driven management. A purpose that transcends profit. Organizations that want to ensure financial security for their shareholders, cost efficiency, and healthy profits must focus on providing positive contribution to the community, finding effective and feasible solutions to social and ecological problems, and investing the company's profits in ecologically and socially sustainable ways. Given the plethora of challenges our societies face, it makes perfect sense that brands increasingly look beyond profit. Brands that roll out social good campaigns send a powerful message to consumers. These brands take a strong stance on political, social, and ecological issues. They are not shying away from controversial issues, such as racism, immigration, gerrymandering. For example, Sarah Kauss founded S'well company in 2010 with the mission to rid the world of plastic water bottles. She understands that it is an audacious goal, but this goal constitutes the very backbone of this organization, one that many consumers identify with.

The days of a company's only responsibility being to initiate a transaction, sell a product, and make a profit are long gone. Brands whose DNA is deeply rooted in social causes are entering the mainstream. They are growing exponentially and increasingly represent a greater share of the market. When it comes to building a loyal customer base, being viewed as a brand that really cares about the common good is quickly becoming indispensable.

H. Krück: Marketing campaigns are one of the communication channels with consumers and it is one of the tools to build a bond with consumer. As it was reflected in a paper published in 2020 in the *Journal of Brand Strategy*, by Bridgitte Kiprop and Leila Samii[5], the more a corporation express its position on any polarizing social issue,

[4] *The Axios Harris Poll 100 reputation rankings*, March 6, 2019, https://www.axios.com/2019/03/06/axios-harris-poll-corporate-reputations [accessed: 12.12.2023].

[5] B. Kiprop, L. Samii, 'Cause-related marketing in a polarised global marketplace', *Journal of Brand Strategy*, 2020, vol. 9, no. 3, pp. 271–283, https://hstalks.com/article/5999/cause-related-marketing-in-a-polarised-global-mark [accessed: 12.12.2023].

the greater the psychological bond they can create with consumers and employees. However, not all the issues a company takes a stand on are polarizing topics, but the causes brands embrace express their espoused values and ideals. This can significantly contribute to brand loyalty.

Therefore, marketing campaigns are used to deliver messages to consumers, that may deter the emergence of a crisis. However, it is challenging to create a marketing campaign that is deemed congruent in terms of the delivered message to consumers and the values of the company. Otherwise, the lack of coherence may lead to increased risk for the business and erosion of brand loyalty.

I. Gabelaia: Businesses are trying to create awareness about the social, environmental, legal, political, and technological challenges which are constantly emerging. Of course, the economic crisis is one part of the puzzle, but today we have political, social, and technological challenges that are becoming stronger. For example, new conflicts and wars in various parts of the world impact people, raw material distribution, etc. Moreover, the growing population creates more social issues, adding to existing issues.

Furthermore, technology provides many opportunities but, at the same time, limits businesses and people. Transparency and corporate social responsibility are some elements to show people that businesses are taking action, but do they really? I have to bring the concept of a triple bottom line 'people – planet – profit.' No matter what we try to do, it still leads and results in direct or indirect profits.

Lastly, as managers, we need to take action and show clients or the general public that a crisis exists and that we are far away from solving it. Marketing campaigns are good, but they must be more effective!

M. Blanco: At the present time, companies must be prepared to handle the crisis, whether due to economic factors external to the organization, as well as issues within the organization and its operation. Marketing will always be an ideal tool to adequately manage crises, since it allows managing the information provided by the company for its external and internal environment (employees, customers, suppliers, competition, etc.). Marketing campaigns have diversified to a great extent and have become sophisticated by integrating technological tools, not only to communicate ideas and messages, but also in the form, colors and experiences that can inspire and galvanize consumers.

A. Chodyński, D. Fatuła: To what extent are marketing messages reflecting the potential threats (other than economic) businesses might face in the foreseeable future?

B.R. Bialas: It is undeniable that increasing public concern over social and environmental issues has forced many organizations to affiliate their brands with a range of popular social, political, and environmental causes. This strategy is commonly referred

to as cause-related marketing, or CRM. There is no doubt that the most important – and visible – aspect of CRM is advertising. CRM is primarily used for creating positive change and driving brand loyalty. Organizations that have learned how to cultivate social impact have experienced unprecedented growth, enriched and up-leveled their brands, and aligned them with socially conscious marketing campaigns. Despite the soaring popularity of CRM, this deceptively simple strategy is still not well understood by many managers I work with. Before the organization rolls out a CRM campaign, managers must clearly articulate the overarching idea that will later become the bedrock of the CRM strategy. What is it, exactly, that you want to achieve? This idea must spell out the cause that aligns with your brand's DNA, values, strategic intent, identity, and positioning. This first step is of paramount importance because it will help you build credibility and a clear and consistent thread that will run throughout all your marketing campaigns. This idea must also resonate with your customers and stakeholders. Emotional contagion can explain – at least to a certain extent – the effectiveness of CRM. It is a well-recognized neuroscientific fact that people tend to think with their hearts. Emotional arousal can lead to the activations of such feelings as pleasure, guilt, anger, happiness. By simply looking at the cause-related advertisement, people can feel sympathy. This, in turn, can lead to the formation of positive attitudes towards the brand behind the CRM campaign. Managers must learn how to educate their clients/customers about the real impact their support/brand loyalty makes. They also need to learn how to magnify causes they support and cultivate. And – finally – they need to learn how to elevate their brands by showing that their organizations are fully committed to the causes and are unwaveringly mission-driven. For example, in 2016, ice-cream brand Ben & Jerry's rolled out a new flavor to actively promote democracy. They called this flavor 'Empower Mint'. The entire CRM campaign – brilliantly called 'Democracy is in Your Hands' – focused on educating consumers about gerrymandering and other barriers placed in low-income and ethnic communities to prevent them from voting. The campaign proclaims that 'Voting Gives Everyone a Taste of Empowerment'. But for Ben & Jerry's this slogan – 'Democracy is in Your Hands' – is not just another fancy marketing gimmick aimed at increasing profitability. The brand actively publishes articles about gerrymandering and voter suppression, and by doing so, sends a powerful and emotionally evocative message that resonates with socially conscious individuals.

H. Krück: It is an undeniable fact that more and more organizations are increasingly turning their attention to social responsibility. Some are focusing on women's rights; others are trying to tackle poverty. There are certainly considerable benefits associated with social responsibility. It has been recognized that social responsibility initiatives can significantly boost employee morale in the workplace and, as a consequence, improve productivity. According to one study conducted quite recently by Harvard Business School, almost 70% of employees in the US admitted that they

wouldn't want to work for an organization whose values are either diluted or morally questionable. And almost 90% of employees who currently work for organizations with well-articulated set of purposes admitted that they feel loyal, inspired, and motivated. For example, a couple of years ago, the Coca-Cola Company fully embraced corporate social responsibility by introducing an ambitious program called 5x20. The major objective of this program was to employ five million women in developing countries by 2020.

Corporate social responsibility initiatives can significantly reflect the scope of potential threats that a company deems serious or dangerous. But corporate social responsibility is definitely more than just a smart business strategy. Businesses increasingly recognize that they can instigate change, and by doing this, they can contribute to the betterment of society.

I. Gabelaia: Today strong marketing content can move mountains; consequently, a strong message must be a massive part of any industry or region to underline potential threats. However, the message must not have to create panic. Messages must be through-through with distinct short-term and long-term goals.

Sometimes I feel like messages are "pluff" because they do not have continuity. We can see some of them throughout traditional or digital media, and that is it. Then, afterward, nobody talks about it. For example, we can discuss and campaign a lot about green marketing, however, my question will be is it really green marketing or greenwashing? It confuses people who care, and that's why many are not committed. This is why those campaigns must have a media plan on how to reach massive audiences.

M. Blanco: These threats can be understood as the complex and sophisticated apparatus that has been developed by the internet and the different technological and communication tools. Not only should the future potential of marketing messages be analyzed, but also what is currently experienced, since within the field of neuromarketing it is possible to understand the impact that messages are having on the consumer and the general public, either to sell a product or to shape public opinion, as it has been seen in some countries, which manage to influence a large part of the population to lead them on a defined path.

A. Chodyński, D. Fatuła: How are natural disasters affecting businesses and how are businesses protected from them?

B.R. Bialas: We are all acutely aware of the fact that the effects of natural disasters on businesses can be devastating. There is no doubt that in order to mitigate damage, organizations must be diligent, foresightful, prescient, and strategic. We must face up to grim reality: Climate change is quickly affecting all areas of life, including business. It is unfortunate that natural disasters are becoming a common occurrence within the United States and – according to many sources – are projected to rise. From earthquakes and droughts to hurricanes and floods, major weather and climate disasters

have been occurring more frequently and with greater potency, creating a serious financial and operational risk to organizations around the world. According to the United Nations Office for Disaster Risk Reduction report of 2020[6] the 7,348 natural disastrous incidents that transpired around the world from 2000 to 2019 caused approximately US$2.97 trillion in losses to the global economy. In comparison, the previous 20-year period (1980–99) saw 4,212 reported disasters from natural hazards, with economic losses of US$1.63 trillion. Given the magnitude of these economic losses, it's easy to state that natural – and man-made – disasters have catastrophic effects on the local – and global – economy. We must also understand that there is a plethora of factors that trigger disasters: various natural forces caused by biological, hydrological, geophysical, climatological, and meteorological forces. But let's not forget human involvement: urbanization, over-farming, over-fishing, industrialization, population growth.

Let's be crystal clear about one thing: managers must learn how to achieve business resiliency to natural – and man-made – disasters. This learning process must begin with understanding and understanding begins by identifying one's commitment to disaster preparation.

H. Krück: Natural disasters evidently affect the continuity of business. However, after the pandemic crisis of 2020, companies established and executed many different measures, managerial and technological, which have been improving with time, in order to ensure business continuity. Now, those measures allow businesses to be more prepared to maintain business continuity in a reasonable way, since some natural disasters have consequences beyond human imagination.

Usually, well established businesses protect themselves from natural disasters through the proper safety measures and procedures, widely considered related to personnel, technological, industrial, financial, etc., as well as the business continuity plan. In addition, to the proper insurance coverages. This might not be the case for all the SMEs that could have an area of opportunity, due to the financial cost all these measures could represent.

From the legal standpoint, in addition to the insurance coverage, businesses protect themselves from natural disasters through agreements with strong clauses related to force majeure.

I. Gabelaia: Indeed a vast question that impacts local and global businesses and economies. Well, how many natural disasters can we count on within the last three years, and can we put together how big of an impact they had on businesses but not only. For example, the environment! Nevertheless, let us look at the sneak peek on

[6] *The human cost of disasters: an overview of the last 20 years (2000–2019)*, Centre for Research on the Epidemiology of Disasters, United Nations Office for Disaster Risk Reduction, October 12, 2020, https://www.undrr.org/publication/human-cost-disasters-overview-last-20-years-2000-2019 [accessed: 12.12.2023].

what is considered a natural disaster, and we will realize its impact. For example, some elements include a call for international assistance, a hundred or more people affected, ten or more killed, or declaring a state of emergency.

Global Sustainable Development Goals are there to help to battle natural issues and push businesses to be more environmentally sustainable, but how much have we achieved? In my calculations, a little. Indeed, we are still learning and investing in it, but we still need to convince people to show the goodness and trustworthiness of these campaigns.

M. Blanco: Natural disasters have been understood as phenomena external to companies, but everything has changed in recent decades, since there are many experiences in which organizations have managed to add positive points with their consumers by collaborating, mitigating or supporting a project or action related to natural disasters. Latin America has always been affected by various natural disasters, since it presents a fragility in its geography and its infrastructure, but the majority of companies have come out ahead, operating in an environment of constant crisis makes organizations and their leaders evolve, the latter carry the responsibility to prepare and define better strategies for the future, both to overcome the crisis and to take advantage of the opportunities it presents.

A. Chodyński, D. Fatuła: Given the fact that organizations around the world are making far-reaching changes across their operational footprints, is there a growing demand for consulting firms and change management consulting services?

B.R. Bialas: The management consulting industry is expected to grow to $973 billion dollars in 2024 at a compound annual growth rate of 9.2%. The management consulting industry consists of companies offering everything from providing advice and assistance on organizational planning, project management expertise, marketing strategies, human resource practices, designing new organizational structures, financial budgeting, administration policies, and production and logistics scheduling, business process improvement, market research, quality assurance, quality control. Global management consultants offer audit services and routinely advise on their clients' tax strategies. Many governments around the world are currently dependent on the services offered to them by the global consulting firms. There is a tremendous problem with consulting firms offering their services to governments. Consulting firms have absolutely no incentive to improve their clients' – in this case, governments' – performance. If they do, they will not get a future contract. With the increasing impact of technology on business, consulting firms are forced to quickly adapt and offer sophisticated and internationally-oriented data analytics services to help their clients stay ahead of the curve. Management consulting firms are becoming more popular, and this increasing popularity is attributed to the automation of consultancy processes

and developments in data security. Clients are actively searching for consultants who can help them understand, formulate, and execute purpose-driven strategies. These strategies are becoming more and more important as they are aimed at fostering and boosting employee engagement and improving employee satisfaction.

H. Krück: As mentioned before, managers are aware of the fact that they cannot control all the aspects of the business. Therefore, they require advice and assistance on many different specialized matters. In consequence, there is a growing demand for consulting firms and change management consulting services. Moreover, globalization requires managers to consider many different jurisdictions, which makes it even more difficult to handle if they do not collaborate with the proper consultants.

As part of a legal consulting firm for the last 14 years, I have observed that there is an increasing trend to seek consulting services in a preventive way, or as a support in change management. More often, companies hire consulting services to execute due diligence, to establish or improve compliance programs in their companies, or even to adapt their implemented compliance programs in different countries and cultural realities. More and more, due to the complexity of globalization, specialized consultants are required to cover different priority areas of the business.

I. Gabelaia: Absolutely. The demand for consulting firms is enormous. I personally consult small and medium-sized companies on various marketing and business strategies. I advise building continuous and sustainable strategies that benefit organizations, the planet, and people. As I mentioned above, my practice's triple-bottom-line impact is massive. Many businesses are involved in upskilling their employees, whether in-person or hybrid modes. This is one way to train employees on their leadership qualities to be more sustainable and socially responsible.

M. Blanco: Most organizations do not adapt as quickly as they should to the changes that constantly occur in today's competitive markets. Consulting services are always necessary to support organizations to minimize their weaknesses, take advantage of their strengths, prepare for threats and achieve sustainable development through the opportunities that arise.

Change management is a process that never ends for organizations that want to remain competitive in the market, so consulting and support services must be present at all levels, both for management and for operational lines, understanding that resistance to change is something natural for human beings. Therefore, it is necessary to support the processes that are to be promoted and accompany the organization at all times so that its evolution is a constant that promotes its permanence over time.

Artykuły

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718 2023
ISSN 1899-6264 Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-001
Data wpłynięcia: 10.05.2023
Data akceptacji: 13.09.2023

Dominika Marciniak

mgr, doktorantka, Politechnika Śląska
https://orcid.org/0000-0002-5499-0754

Przygotowanie logistyczne podmiotów realizujących pomoc humanitarną w Polsce

Wprowadzenie

Potrzeby w zakresie pomocy humanitarnej rosną[1]. Przyczynia się do tego degradacja środowiska, szybka urbanizacja oraz rozprzestrzenianie się chorób cywilizacyjnych w krajach rozwijających się[2]. Wojna rosyjsko-ukraińska[3], trzęsienie ziemi w Turcji i Syrii[4] oraz konflikt wewnętrzny rujnujący Syrię[5] to przykłady miejsc i zdarzeń,

1 M.M. Ershadi, H.S. Shemirani, *A multi-objective optimization model for logistic planning in the crisis response phase*, „Journal of Humanitarian Logistics and Supply Chain Management" 2022, vol. 12, nr 1, s. 30–53; Z. Wang, J. Zhang, *Agent-based evaluation of humanitarian relief goods supply capability*, „International Journal of Disaster Risk Reduction" 2019, nr 36, s. 101–105.

2 C.F. Agostinho *Humanitarian Logistics: How to help even more*, „IFAC Proceedings Volumes (IFAC Papers-OnLine)" 2013, vol. 46, nr 24, s. 206–210, https://doi.org/10.3182/20130911-3-BR-3021.00075.

3 D.D. Kasprzycki, *Konflikt zbrojny na Ukrainie w kontekście rosyjskiej koncepcji wojny nowej generacji*, „Rocznik Bezpieczeństwa Międzynarodowego" 2022, t. 16, nr 1, s. 79–107, https://doi.org/10.34862/rbm.2022.1.5.

4 Uniwersytet Otwarty Uniwersytetu Warszawskiego, Wydział Geologii, *Katastrofalne trzęsienie ziemi w Turcji i Syrii – dlaczego musimy badać uskoki?*, https://www.youtube.com/watch?v=MzzkluAvxZc [dostęp: 13.09.2023].

5 *Wojna domowa gorsza od kataklizmu. Syryjski reżim stara się zadbać przede wszystkim o swoich*, Rzeczpospolita, 10.02.2023, https://www.rp.pl/kleski-zywiolowe/art37934751-wojna-domowa-gorsza-od-kataklizmu-syryjski-rezim-stara-sie-zadbac-przede-wszystkim-o-swoich [dostęp: 03.03.2023].

które wymagają dużych nakładów pomocy humanitarnej. Organizacje humanitarne starają się sprostać tym wyzwaniom w szybki i skuteczny sposób, tak aby możliwie jak najwięcej osób otrzymało potrzebną pomoc[6]. Unia Europejska i ONZ przeznaczają na pomoc humanitarną miliardy euro, np. dzięki organizacji wideokonferencji darczyńców (29–30 marca 2021 r.), na której udało się zebrać 5,3 mld euro w dotacjach oraz 5,9 mld euro w niskooprocentowanych pożyczkach na pomoc dla Syryjczyków[7]. Ponadto Komisja Europejska przeznaczyła około 144,6 mln euro dla Polski na pomoc uchodźcom ukraińskim opuszczającym terytorium Ukrainy z powodu trwającej wojny. Środki te zostały przekazane Polsce 26 sierpnia 2022 r. – 10 dni po złożeniu wniosku aplikacyjnego do Komisji Europejskiej przez Ministerstwo Spraw Wewnętrznych i Administracji[8].

Organizacja świadcząca pomoc musi pamiętać o następujących trzech zasadach: szybkości, adekwatności i możliwie niskich kosztach administracyjnych[9]. Istotne jest, aby pomoc dotarła do potrzebujących w jak najkrótszym czasie od katastrofy, w następstwie której powstał kryzys humanitarny. Sprawne dostarczenie pomocy oznacza zmniejszenie szkód spowodowanych przeciągającym się kryzysem. Ponadto pomoc powinna w pełni odpowiadać potrzebom ludności dotkniętej kryzysem. Oznacza to konieczność pozyskiwania informacji zarówno od władz państw potrzebujących pomocy, jak i na podstawie analiz polskich placówek dyplomatycznych, a także od organizacji pozarządowych, w szczególności międzynarodowych[10].

Badania na temat logistyki humanitarnej są szeroko opisywane w literaturze międzynarodowej[11]. W Polsce badania na ten temat są znacznie skromniejsze. Prowadzone są przede wszystkim w zakresie podstaw zarządzania kryzysowego[12] oraz

---

6 *Ibidem*.

7 A. Wolska, *UE i ONZ zebrały 5,3 mld euro na pomoc humanitarną dla Syryjczyków*, EURACTIV.pl, 31.03.2021, https://www.euractiv.pl/section/polityka-zagraniczna-ue/news/ue-onz-syria-pomoc-humanitarna-wojna-domowa [dostęp: 25.10.2022].

8 *Prawie 700 mln zł z UE na wsparcie dla uchodźców z Ukrainy*, Gov.pl, 19.10.2022, https://www.gov.pl/web/mswia/prawie-700-mln-zl-z-ue-na-wsparcie-dla-uchodzcow-z-ukrainy [dostęp: 25.10.2022].

9 W. Drewek, *Działalność organizacji humanitarnych w systemie logistyki humanitarnej*, „Logistyka" 2013, nr 6, s. 95–102.

10 *Ibidem*.

11 C.F. Agostinho, *op. cit.*; J. Bealt, J.C. Fernández Barrera, S.A. Mansouri, *Collaborative relationships between logistics service providers and humanitarian organizations during disaster relief operations*, „Journal of Humanitarian Logistics and Supply Chain Management" 2016, vol. 6, nr 2, s. 118–144; M.S.M Daud *et al.*, *Humanitarian logistics and its challenges: The literature review*. „International Journal of Supply Chain Management" 2016, vol. 5, nr 3, s. 108; Directorate General for European Civil Protection and Humanitarian Aid Operations, *Humanitarian Logistics Policy*, Publications Office of the European Union, Luxembourg 2022; M.M. Ershadi, H.S. Shemirani, *op. cit*.

12 I. Denysiuk, *Zarządzanie kryzysowe w Polsce jako specyficzne zadanie administracji publicznej realizowane na rzecz ochrony ludności*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2020, t. 2, nr 6, s. 168–184; F.R. Krynojewski, *Proces zarządzania kryzysowego*,

charakterystyki zagrożeń bezpieczeństwa i ich źródeł[13]. Pojawiają się również nieliczne publikacje dotyczące usprawnienia systemu zabezpieczenia logistycznego sytuacji kryzysowych[14], modelowania i informatycznego wspomagania decyzji[15] oraz koncepcji zintegrowanej platformy symulacyjnej dla podmiotów zarządzania kryzysowego[16]. Aby wypełnić istniejącą lukę w badaniach tej problematyki, w niniejszym artykule podjęto próbę analizy przygotowania logistycznego podmiotów uczestniczących w działaniach niesienia pomocy humanitarnej. Cel ten zostanie osiągnięty w oparciu o poszukiwanie odpowiedzi na następujące pytania badawcze – w ramach badań przeprowadzonych w 2021 r. metodą PAPI (Papier and Pencil Interview) i CAPI (Computer-Assisted Personal Interview) w Polsce:

1. Czy na wypadek wystąpienia zagrożenia lub potrzeby udzielenia pomocy humanitarnej w badanych organizacjach pracują osoby odpowiedzialne za prowadzenie kontroli i ewidencji wszystkich działań logistycznych?
2. Czy w badanych organizacjach pracują osoby odpowiedzialne za organizowanie transportu ewakuacyjnego i zaopatrzeniowego?
3. Czy badane organizacje posiadają unormowane zasady współpracy z dostawcami środków pomocowych w przypadku wystąpienia zagrożenia i sytuacji kryzysowej?
4. Czy w badanych organizacjach przeprowadzane są przetargi na zakup niezbędnych środków rzeczowych?
5. Czy środki pomocowe dostarczane poszkodowanym w ramach pomocy humanitarnej są zgodne z ich potrzebami?
6. Czy organizacja konwojów z pomocą humanitarną jest skuteczna?

Istota logistyki w pomocy humanitarnej

Pomoc humanitarna (ang. *humanitarian aid*) obejmuje pomoc materialną i logistyczną dla osób potrzebujących. Rola logistyki w pomocy humanitarnej jest bardzo

2018, s. 2, https://www.jastrzebie.pl/fileadmin/user-files/aktualnosci/2018/10-pazdziernik/straz-miejska/Zarzadzanie-kryzysowe.pdf [dostęp: 10.08.2023].

[13] M. Dzimińska-Mosio, *Instytucja stanów nadzwyczajnych a stan wojenny*, „Przegląd Policyjny" 2017, nr 3 (127), s. 167–182; *Zagrożenia i instytucje bezpieczeństwa międzynarodowego*, red. E. Cziomer, Oficyna Wydawnicza AFM, Kraków 2016.

[14] K. Ficoń, *Zastosowanie teorii masowej obsługi do analizy systemu zabezpieczenia logistycznego sytuacji kryzysowych*, „Systemy Logistyczne Wojsk" 2017, nr 47, s. 59–79.

[15] *Modelowanie, symulacja i informatyczne wspomaganie decyzji w zarządzaniu kryzysowym*, Zespół badawczy modelowania, symulacji i informatycznego wspomagania decyzji w sytuacjach konfliktowych i kryzysowych (kierownik zespołu: A. Najgebauer, prezentacja: Dariusz Pierzchała), https://docplayer.pl/15135724-Modelowanie-symulacja-i-informatyczne-wspomaganie-decyzji-w-zarzadzaniu-kryzysowym-prezentacja-dariusz-pierzchala.html [dostęp: 28.11.2022].

[16] G. Gudzbeler, M. Nepelski, *Zintegrowana Platforma Symulacyjna Podmiotów Zarządzania Kryzysowego – spójne środowisko wirtualne*, „Bezpieczeństwo i Technika Pożarnicza" 2015, t. 38, nr 2, s. 89–96.

wyraźnie akcentowana. Logistyka jest istotnym elementem planów reagowania w sytuacjach kryzysowych oraz pomocy humanitarnej w celu zapewnienia dostępności właściwych artykułów we właściwej lokalizacji, we właściwym czasie i odpowiedniej ilości[17].

Aby skutecznie realizować zadania mające na celu zapewnienie pomocy humanitarnej, niezbędne są siły i środki, określane mianem zabezpieczenia logistycznego[18]. Wieloaspektowość oraz rola zabezpieczenia logistycznego w pomocy humanitarnej staje się szczególnie ważna w sytuacjach kryzysowych, kiedy zgromadzone zasoby logistyczne zapewniają skuteczną pomoc dla zagrożonej ludności oraz mienia[19].

Zasoby te służą do wsparcia nie tylko ofiar danej sytuacji kryzysowej, ale również sił ratowniczych realizujących przydzielone zadania. Z punktu widzenia poszkodowanej ludności potrzeby logistyczne mieszczą się w trzech zasadniczych obszarach zabezpieczenia logistycznego, tj. 1) dostaw zaopatrzenia i usług gospodarczo-bytowych; 2) zabezpieczenia medycznego; 3) usług transportowych[20].

Na potrzeby zarządzania kryzysowego i pomocy humanitarnej – na każdym poziomie administracyjnym – tworzy się magazyny ze sprzętem. Obowiązujące akty prawne posługują się terminem „magazyn przeciwpowodziowy"[21]. Środki pomocowe przechowywane w magazynach można podzielić na dwie grupy: konsumpcyjne i niekonsumpcyjne[22].

Realizacja dostaw środków pomocowych możliwa jest dzięki usługom transportowym. Dostawy zaspokajające najpilniejsze potrzeby ludności poszkodowanej realizowane są za pomocą wszystkich dostępnych środków transportu[23]. Podstawowe dostawy dotyczą wody i żywności, co uwarunkowane jest głównie względami fizjologicznymi oraz wydajnością energetyczną organizmu[24]. Punktem startowym dostaw zaopatrzeniowych są składy i magazyny (magazyny przeciwpowodziowe), czasem również hurtownie sieci handlowych.

---

17 D. Malindžák, T. Olejarz, *Logistyka w zarządzaniu kryzysowym*, „Przegląd Nauk o Obronności" 2017, t. 2, nr 4, s. 141–142..

18 A. Bujak, M. Witkowski, *Zabezpieczenie logistyczne w zarządzaniu kryzysowym*, „Logistyka" 2014, nr 3, s. 891–898.

19 *Ibidem*.

20 B. Pac, *Istota zarządzania zabezpieczeniem logistycznym w sytuacjach kryzysowych i stanach nadzwyczajnych*, „Prace Naukowe Uniwersytetu Ekonomicznego" 2015, nr 383, s. 133.

21 Art. 7, ust. 1, pkt 14, Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz.U. z 1990 r., nr 16, poz. 95; Art. 4, ust. 1, pkt 16, Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym, Dz.U. z 1998 r., nr 91, poz. 578.

22 *Standard products catalogue*, International Federation of Red Cross and Red Crescent Societies, https://itemscatalogue.redcross.int [dostęp: 17.03.2023].

23 K. Ficoń, *Logistyka kryzysowa. Procedury, potrzeby, potencjał*, Bel Studio, Warszawa 2011, s. 237.

24 *Ibidem*, s. 243.

Pomoc humanitarna dostarczana jest także konwojami. Mimo że pojęcie to figuruje w źródłach internetowych czy publikacjach naukowych, jego znaczenie nie jest sprecyzowane. Należy przede wszystkim opierać się na podstawowej definicji konwoju. Konwój umożliwia lepszą organizację ruchu, współpracę i wzajemną pomoc uczestników grupy w przypadku wystąpienia awarii bądź wypadku. Niejednokrotnie część konwoju stanowi eskorta o charakterze zbrojnym, dzięki czemu zapewnione zostaje bezpieczeństwo jego uczestników w razie wrogiego ataku[25].

Szczególne zasady dotyczą transportu zwłok ludzkich, do którego wykorzystywane są specjalnie przystosowane pojazdy. Zwłoki w warunkach polowych okrywa się czarnymi workami foliowymi, a każdy worek musi zostać zaopatrzony w identyfikator z danymi denata. Transport zwłok odbywa się pod ścisłą kontrolą na wszystkich etapach podróży, a niezapewnienie ochrony i szacunku osobom zmarłym podlega sankcjom karnym[26].

Z kolei logistyka ewakuacji jest stosunkowo prosta, jeśli władze mają czas na poinformowanie zagrożonej ludności o zbliżającym się niebezpieczeństwie i potrzebie opuszczenia danego terenu. Natomiast poważne problemy logistyczne mogą pojawić się w trakcie realizowania transportu i zapewniania noclegów dużej liczbie mieszkańców[27]. Nie wszyscy są na tyle mobilni, by móc skorzystać z własnych bądź zbiorowych środków transportu (np. autobusów). Niektórzy wymagają transportu specjalistycznego, np. karetką. Należy uwzględnić także ewakuację zwierząt domowych, jak również zapewnić im schronienie[28].

Biorąc pod uwagę przesłanki organizowania skutecznej pomocy humanitarnej, niniejszy artykuł koncentruje się na odpowiedzialności za realizację procesów logistycznych, adekwatności środków pomocowych i skuteczności organizacji konwojów humanitarnych.

Metodyka badań

Pytania w ankiecie przygotowano na podstawie krytycznego przeglądu literatury. W części dotyczącej przygotowania logistycznego podmiotów uczestniczących w działaniach niesienia pomocy humanitarnej uwzględniono zagadnienia odnoszące się do:

---

[25] *Konwój*, Wikipedia, https://pl.wikipedia.org/wiki/Konw%C3%B3j [dostęp: 24.02.2023].

[26] K. Ficoń, *Logistyka kryzysowa. Procedury...*, *op. cit.*, s. 236–237.

[27] M.K. Lindell, *Evacuation planning, analysis, and management*, [w:] *Handbook of Emergency Response: A Human Factors and Systems Engineering Approach*, red. A.B. Badiru, L. Racz, https://www.researchgate.net/publication/284091989_Evacuation_planning_analysis_and_management [dostęp: 23.11.2022].

[28] *Ibidem*.

- odpowiedzialności za ewidencję działań logistycznych[29],
- odpowiedzialności za transport ewakuacyjny i zaopatrzeniowy[30],
- współpracy z dostawcami[31],
- organizacji przetargów na zakup środków pomocowych[32],
- adekwatności środków pomocowych[33],
- skuteczności organizacji konwojów humanitarnych[34].

W ankiecie wykorzystano 7-stopniową skalę Likerta, która umożliwia respondentom określenie stopnia, w jakim zgadzają się bądź nie zgadzają z daną kwestią: zdecydowanie nie (1), nie (2), raczej nie (3), nie mam zdania (4), raczej tak (5), tak (6), zdecydowanie tak (7). Odpowiedzi udzieliło 101 osób z 75 organizacji. W badaniu najmniej licznie reprezentowane były organizacje pozarządowe (3,8%) – nie wyrażały one chęci udziału w badaniach, wskazując m.in. na brak wiedzy w badanych obszarach lub brak czasu. Ponadto w badaniu uczestniczyli przedstawiciele Centrów Zarządzania Kryzysowego Urzędów Wojewódzkich (10,4%) oraz pozostałych jednostek, które muszą zachować anonimowość (23,5%). Najliczniejszą grupę stanowią jednostki Państwowej Straży Pożarnej (62,3%), które chętnie wzięły udział w badaniu. Zgodnie z obowiązującymi aktami prawnymi podstawową formacją prowadzącą działania w strefach niebezpiecznych jest Państwowa Straż Pożarna, która koordynuje działania – i z perspektywy logistyki wiedza i doświadczenie pracowników Państwowej Straży Pożarnej są kluczowe.

W badaniu wzięły udział osoby posiadające dużą wiedzę w zakresie organizowania pomocy humanitarnej w Polsce, również ze względu na piastowane wysokie

---

29 A. Blecken, *A Reference Task Model for Supply Chain Processes of Humanitarian Organisations*, Doctoral thesis, Heinz Nixdorf Institute of the Paderborn University, 2009, s. 293.

30 K. Ficoń, *Logistyka kryzysowa. Procedury…*, *op. cit.*, s. 227–256.

31 M. Jahre, *Humanitarian supply chain strategies – a review of how actors mitigate supply chain risks*, „Journal of Humanitarian Logistics and Supply Chain Management" 2017, vol. 7, nr 2, s. 82–101.

32 K. Berger, E. Garyfalakis, *Procurement policies in disaster relief: Analysis of sourcing practices applied by humanitarian organizations in the field of disaster response*, Master's thesis, Jönköping University, 2013, https://www.diva-portal.org/smash/get/diva2:632749/fulltext01.pdf, s. 8 [dostęp: 13.09.2023]; Emeregency Tender Notice for Purchase of Miscellaneous Relief Items, Director General, Provincial Disaster Management Authority, Khyber Pakhtunkhwa, Hayatabad, Peshawar, [2022], https://pdma.gov.pk/sub/uploads/Tender%20Notice%20Emergency%20Relief%20Items%20(Submission%20Date%20On%20or%20before%20August%2031,%202022%20at%201130%20Hours).pdf [dostęp: 13.09.2023].

33 Y. Ye, H. Yan, *Disaster Relief Supply Management*, [w:] *Natural Hazards: Impacts, Adjustments and Resilience*, red. E.N. Farsangi, IntechOpen, London 2020, s. 10.

34 A. Bassil, *Armed escorts to humanitarian convoys: An unexplored framework under international humanitarian law*, „International Review of the Red Cross" 2020, vol. 102, nr 914, s. 559–578, https://doi.org/10.1017/S1816383121000734; Alliance for Public Health, *Humanitarian Convoys of the APH: 111 days on the road, 111 days of aid*, Situational Report as of 20.06.2022, https://aph.org.ua/wp-content/uploads/2022/06/APH_WarSitRep_Humanitarian-Convoys_20June2022_eng_final.pdf [dostęp: 04.03.2023].

stanowiska: naczelnik i zastępca naczelnika – 21,9%; stanowisko specjalistyczne – 14,3%; dowódca i zastępca dowódcy – 13,3%; kierownik i zastępca kierownika – 8,6%; komendant i zastępca komendanta – 7,6%; szef sekcji – 6,7%; oficer i podoficer – 4,8%; technik, starszy technik – 6,3%; dyrektor i zastępca dyrektora – 10,4%; funkcjonariusz – 2,3%; inspektor, starszy inspektor – 3,8%. Średni stażu pracy tych osób w organizacjach prowadzących działania z zakresu zarządzania kryzysowego wynosi 17 lat.

Uzyskane w trakcie badań wyniki poddano analizie statystycznej. Miarami wykorzystanymi do analiz były: dominanta (moda), mediana, pierwszy kwartyl (Q1), trzeci kwartyl (Q3) oraz średnia. Miary te umożliwiły obiektywną ocenę uzyskanych informacji.

Wyniki badań

Statystyki opisowe stanowiły podstawę interpretacji uzyskanych wyników badań. W przypadku każdego badanego zagadnienia analiza statystyczna została przeprowadzona indywidualnie. Uzyskane wyniki zostały zaprezentowane w tabelach 1–6.

Tabela 1. Odpowiedzialność za ewidencję działań logistycznych

Odpowiedzi [%]							Miary położenia					
zdecydowanie nie (1)	nie (2)	raczej nie (3)	nie mam zdania (4)	raczej tak (5)	tak (6)	zdecydowanie tak (7)	Q1	Mediana	Q3	Moda	S	Średnia
Czy na wypadek wystąpienia zagrożenia lub potrzeby udzielenia pomocy humanitarnej jest w Pana/i organizacji osoba odpowiedzialna za prowadzenie kontroli i ewidencji wszystkich działań logistycznych?												
1,98	8,91	9,90	8,91	22,77	38,61	8,91	4	5	6	6	1,53	4,93

Źródło: opracowanie własne na podstawie badań.

Zgodnie z informacjami przedstawionymi w tabeli 1 w 70,29% organizacji pracują osoby odpowiedzialne za prowadzenie kontroli i ewidencji wszystkich działań logistycznych. Odpowiedzi pozytywne rozkładają się następująco: 22,77% („raczej tak"), 38,61% („tak"), 8,91% („zdecydowanie tak"). W jednej na pięć organizacji nie prowadzi się ewidencji działań logistycznych (9,9% „raczej nie", 8,91% „nie", 1,98% „zdecydowanie nie").

Respondentów, którzy odpowiedzieli afirmująco, dodatkowo zapytano, na jakich stanowiskach pracują specjaliści odpowiedzialni za ewidencję działań logistycznych. Były to następujące stanowiska: Dyżurny Operacyjny OKW, Naczelnik Wydziału Logistyki, Kierownik sekcji, Komendant lub Z-ca Komendanta, Kwatermistrz, Inspektor, Kierownik do spraw kwatermistrzowsko-technicznych,

Specjalista ds. obrony cywilnej, Wyznaczony Oficer Operacyjny do zarządzania kryzysowego, Logistics Manager i Logistics Officer, Członek zarządu i Dyrektor, Naczelnik Wydziału Techniki i Zaopatrzenia.

Następnie zanalizowano odpowiedzialność za realizację transportu ewakuacyjnego i zaopatrzeniowego (tabela 2).

Tabela 2. Odpowiedzialność za realizację transportu ewakuacyjnego i zaopatrzeniowego

Odpowiedzi [%]							Miary położenia					
zdecydowanie nie (1)	nie (2)	raczej nie (3)	nie mam zdania (4)	raczej tak (5)	tak (6)	zdecydowanie tak (7)	Q1	Mediana	Q3	Moda	S	Średnia
Czy w Pana/i organizacji jest osoba odpowiedzialna za organizowanie transportu ewakuacyjnego i zaopatrzeniowego?												
1,98	6,93	10,89	7,92	13,86	46,53	11,88	4	6	6	6	1,55	5,11

Źródło: opracowanie własne na podstawie badań.

Z danych z tabeli 2 wynika, że w 72,27% badanych organizacji (łączny odsetek odpowiedzi pozytywnych) pracują osoby odpowiedzialne za organizowanie transportu ewakuacyjnego i zaopatrzeniowego. Dominanta wynosi 6, czyli „tak" (46,53%). W jednej na pięć organizacji nie pracują specjaliści zajmujący się transportem ewakuacyjnym i zaopatrzeniowym.

Dodatkowo zapytano, na jakich stanowiskach pracują specjaliści zajmujący się tymi kwestiami. Respondenci wymienili następujące: Szef Zespołu, Kwatermistrz, Dowódca Kampanii Powodziowo-Ewakuacyjnej, Dowódca JRG, Naczelnik Wydziału, Funkcjonariusz odpowiedzialny za sprawy kwatermistrzowskie oraz dowódcy Jednostki Ratowniczo-Gaśniczej, Komendant Miejski PSP, Naczelnik Wydziału Logistycznego.

Następnie respondenci odnieśli się do kwestii współpracy z dostawcami środków pomocowych na wypadek wystąpienia zagrożenia i sytuacji kryzysowej (tabela 3).

Tabela 3. Współpraca z dostawcami środków pomocowych

Odpowiedzi [%]							Miary położenia					
zdecydowanie nie (1)	nie (2)	raczej nie (3)	nie mam zdania (4)	raczej tak (5)	tak (6)	zdecydowanie tak (7)	Q1	Mediana	Q3	Moda	S	Średnia
Czy Pana/i organizacja posiada unormowane zasady współpracy z dostawcami niezbędnych środków pomocowych w przypadku wystąpienia zagrożenia i sytuacji kryzysowej?												
0	6,93	1,98	9,9	41,58	30,69	8,91	5	5	6	5	1,20	5,13

Źródło: opracowanie własne na podstawie badań.

Z danych zaprezentowanych w tabeli 3 wynika, że 81,19% organizacji (łącznie odpowiedzi pozytywne) posiada unormowane zasady współpracy z dostawcami niezbędnych środków pomocowych, jednak większość respondentów nie była pewna swojej odpowiedzi, czego wyrazem jest dominanta 5 – odpowiedź „raczej tak". Pojawiło się 8,91% odpowiedzi negatywnych, a 9,90% respondentów nie miało zdania na ten temat.

Kontynuując wątek środków pomocowych, respondentów zapytano, czy ich organizacje przeprowadzają przetargi na zakup niezbędnych środków pomocowych takich jak: koce, żywność, lekarstwa, namioty, kontenery, środki czystości (tabela 4).

Tabela 4. Przetargi na zakup środków pomocowych

Odpowiedzi [%]							Miary położenia					
zdecydowanie nie (1)	nie (2)	raczej nie (3)	nie mam zdania (4)	raczej tak (5)	tak (6)	zdecydowanie tak (7)	Q1	Mediana	Q3	Moda	S	Średnia
Czy Pana/i organizacja przeprowadza przetargi na zakup niezbędnych środków rzeczowych np. koce, żywność, lekarstwa, namioty, kontenery, środki czystości?												
2,97	19,8	4,59	5,94	14,85	37,62	13,86	3	6	6	6	1,85	4,78

Źródło: opracowanie własne na podstawie badań.

Na podstawie danych w tabeli 4 stwierdza się, że 66,34% organizacji (łącznie oceny pozytywne) przeprowadza przetargi na zakup środków pomocowych. Moda wynosi 6, co oznacza, że respondenci nie mieli wątpliwości i z pewnością przedstawili swoje zdanie. Z kolei 27,72% organizacji nie realizuje takich przetargów, a 5,94% respondentów nie potrafiło odpowiedzieć na to pytanie.

W następnej kolejności rozważono adekwatność środków pomocowych do sytuacji i potrzeb (tabela 5).

Tabela 5. Adekwatność środków pomocowych

Odpowiedzi [%]							Miary położenia					
zdecydowanie nie (1)	nie (2)	raczej nie (3)	nie mam zdania (4)	raczej tak (5)	tak (6)	zdecydowanie tak (7)	Q1	Mediana	Q3	Moda	S	Średnia
Czy uważa Pan/i, że środki pomocowe dostarczane poszkodowanym w czasie pomocy humanitarnej są zgodne z ich potrzebami?												
0	1,98	6,93	10,89	56,44	19,80	3,96	5	5	5	5	0,96	4,97

Źródło: opracowanie własne na podstawie badań.

Zgodnie z informacjami zawartymi w tabeli 5, środki pomocowe dostarczane w czasie pomocy humanitarnej są raczej adekwatne do potrzeb poszkodowanych (56,44% „raczej tak"). Ogólnie 80,20% organizacji stwierdza adekwatność środków

pomocowych względem potrzeb. W 8,91% organizacji stwierdzono, że decyzje co do wyboru środków pomocowych są nietrafione, a 10,89% nie ma zdania w badanym obszarze.

Ostatnie pytanie dotyczyło oceny skuteczności organizacji konwojów humanitarnych (tabela 6).

Tabela 6. Skuteczność organizacji konwojów humanitarnych

Odpowiedzi [%]							Miary położenia					
zdecydowanie nie (1)	nie (2)	raczej nie (3)	nie mam zdania (4)	raczej tak (5)	tak (6)	zdecydowanie tak (7)	Q1	Mediana	Q3	Moda	S	Średnia
Czy Pana/i zdaniem organizacja konwojów z pomocą humanitarną jest skuteczna?												
0,99	3,96	2,97	38,61	31,69	17,82	3,96	4	5	5	4	1,20	4,65

Źródło: opracowanie własne na podstawie badań.

Z tabeli 6 wynika, że największa część respondentów (38,61%) nie ma zdania na temat skuteczności organizacji konwojów humanitarnych (moda – 4 „nie mam zdania"). Ponad połowa badanych organizacji (53,47%) uważa, że organizacja konwojów humanitarnych jest skuteczna. Jednak wśród odpowiedzi twierdzących największy udział ma odpowiedź „raczej tak", co wskazuje na pewien stopień niepewności w deklarowanym poglądzie ankietowanych. 7,92% organizacji stwierdza, że organizacja konwojów humanitarnych jest nieskuteczna.

Podsumowanie i wnioski

Zabezpieczenie logistyczne akcji humanitarnych dotyczy przede wszystkim przygotowania kadr, czyli personelu opiniotwórczo-doradczego, decyzyjnego i technicznego[35]. Ponadto odnosi się ono do sprzętu, który jest niezbędny do prawidłowego wykonywania działań[36]: urządzeń, środków technicznych oraz aparatury teleinformatycznej. Generalnie, logistyka to narzędzie usprawniające prowadzenie akcji humanitarnych[37]. Jakub M. Marcinkowski podkreśla, że znaczenie logistyki w sytuacjach kryzysowych i pomocy humanitarnej wzrasta, ponieważ udzielanie pomocy potrzebującym przebiega w ramach międzynarodowych i krajowych strumieni przepływów rzeczowych, finansowych, ludzkich oraz informacyjnych[38]. Zadaniem logistyki

[35] A. Bujak, M. Witkowski, *op. cit.*

[36] *Ibidem*.

[37] J. Szołtysek, *Typologia obszarów stosowania logistyki – propozycja rozwiązania*, „Gospodarka Materiałowa i Logistyka" 2010, nr 8, s. 2–6.

[38] J.M. Marcinkowski, *Humanitarny łańcuch dostaw w sytuacji wystąpienia katastrof naturalnych na przykładzie ugrupowania regionalnego ASEAN*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2019, s. 7.

w akcjach humanitarnych jest szybka reakcja w celu ocalenia i utrzymania przy życiu ludzi oraz zapobieżenie lub ulżenie cierpieniu ludzkiemu wszędzie, gdzie zachodzi taka potrzeba[39].

Tworzenie „strategii działań, ich planowanie, później organizowanie, połączone z przewodzeniem i kontrolą na każdym etapie, a także ciągła wymiana informacji od dostawców zadań logistycznych i medycznych, aż do ich odbiorców, mają przede wszystkim ratować ludzkie zdrowie i życie"[40].

Organizacje uczestniczące w badaniu, którego wyniki przedstawiono w niniejszym artykule, pozytywnie oceniły swój stan przygotowania logistycznego do działań z zakresu pomocy humanitarnej. W niemal trzech na cztery organizacjach pracują specjaliści odpowiedzialni za prowadzenie kontroli i ewidencji działań logistycznych (70,29% odpowiedzi twierdzących) oraz specjaliści w zakresie organizowania transportu ewakuacyjnego i zaopatrzeniowego (72,27% odpowiedzi twierdzących). Osoby zajmujące się logistyką w badanych organizacjach zwykle zajmują kierownicze stanowiska.

W kontekście środków pomocowych okazuje się, że badane organizacje posiadają unormowane zasady współpracy z dostawcami (81,19% odpowiedzi twierdzących), chociaż wśród odpowiadających twierdząco największy odsetek (41,58%) stanowią osoby niepewne swoich opinii. Badane organizacje przeprowadzają także przetargi na zakup niezbędnych środków pomocowych (66,34%). Jednak niepokojący może być fakt, że większość respondentów uznała bez przekonania, że środki pomocowe dostarczane w czasie pomocy humanitarnej są adekwatne do potrzeb poszkodowanych. Mimo że odpowiedzi afirmujących jest łącznie 80,20%, to większość z nich stanowią odpowiedzi „raczej tak" (56,44%). W przypadku oceny skuteczności organizacji konwojów humanitarnych respondenci nie mają wypracowanej opinii. Uzyskano 38,61% odpowiedzi „nie mam zdania". Ponad połowa ankietowanych stwierdza skuteczność organizacji konwojów humanitarnych, a 7,92% uznaje organizację konwojów humanitarnych za nieskuteczną. Z tego względu można uznać, że organizacja konwojów humanitarnych oraz zapewnienie adekwatności środków pomocowych do potrzeb stanowią wyzwania dla podmiotów realizujących pomoc humanitarną w Polsce i istnieje potrzeba podjęcia inicjatyw usprawniających w tych obszarach.

---

[39] *Logistyka humanitarna i zarządzanie kryzysowe. Wybrane problemy*, red. T. Pokusa, M. Duczmal, Wydawnictwo Wyższej Szkoły Zarządzania i Administracji w Opolu, Opole 2009.

[40] D. Malindžák, T. Olejarz, *op. cit.*, s. 137–147.

Bibliografia

Agostinho C.F., *Humanitarian Logistics: How to help even more*, „IFAC Proceedings Volumes (IFAC Papers-OnLine)" 2013, vol. 46, nr 24, s. 206–210, https://doi.org/10.3182/20130911-3-BR-3021.00075.

Alliance for Public Health, *Humanitarian Convoys of the APH: 111 days on the road, 111 days of aid*, Situational Report as of 20.06.2022, https://aph.org.ua/wp-content/uploads/2022/06/APH_WarSitRep_Humanitarian-Convoys_20June2022_eng_final.pdf [dostęp: 04.03.2023].

Bassil A., *Armed escorts to humanitarian convoys: An unexplored framework under international humanitarian law*, „International Review of the Red Cross" 2020, vol. 102, nr 914, s. 559–578, https://doi.org/10.1017/S1816383121000734.

Bealt J., Fernández Barrera J.C., Mansouri S.A., *Collaborative relationships between logistics service providers and humanitarian organizations during disaster relief operations*, „Journal of Humanitarian Logistics and Supply Chain Management" 2016, vol. 6, nr 2, s. 118–144.

Berger K., Garyfalakis E., *Procurement policies in disaster relief: Analysis of sourcing practices applied by humanitarian organizations in the field of disaster response*, Master's thesis, Jönköping University, 2013, https://www.diva-portal.org/smash/get/diva2:632749/fulltext01.pdf [dostęp: 13.09.2023].

Blecken A., *A Reference Task Model for Supply Chain Processes of Humanitarian Organisations*, Doctoral thesis, Heinz Nixdorf Institute of the Paderborn University, 2009.

Bujak A., Witkowski M., *Zabezpieczenie logistyczne w zarządzaniu kryzysowym*, „Logistyka" 2014, nr 3, s. 891–898.

Daud M.S.M., Hussein M.Z.S.M., Nasir M.E., Abdullah R., Kassim R., Suliman M.S., Saludin M.R., *Humanitarian logistics and its challenges: The literature review*. „International Journal of Supply Chain Management" 2016, vol. 5, nr 3, s. 107–110.

Denysiuk I., *Zarządzanie kryzysowe w Polsce jako specyficzne zadanie administracji publicznej realizowane na rzecz ochrony ludności*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2020, t. 2, nr 6, s. 168–184.

Directorate General for European Civil Protection and Humanitarian Aid Operations, *Humanitarian Logistics Policy*, Publications Office of the European Union, Luxembourg 2022.

Drewek W., *Działalność organizacji humanitarnych w systemie logistyki humanitarnej*, „Logistyka" 2013, nr 6, s. 95–102.

Dzimińska-Mosio M., *Instytucja stanów nadzwyczajnych a stan wojenny*, „Przegląd Policyjny" 2017, nr 3 (127), s. 167–182.

Emeregency Tender Notice for Purchase of Miscellaneous Relief Items, Director General, Provincial Disaster Management Authority, Khyber Pakhtunkhwa, Hayatabad, Peshawar, [2022], https://pdma.gov.pk/sub/uploads/Tender%20Notice%20Emergency%20Relief%20Items%20(Submission%20Date%20On%20or%20before%20August%2031,%202022%20at%201130%20Hours).pdf [dostęp: 13.09.2023].

Ershadi M.M., Shemirani H.S., *A multi-objective optimization model for logistic planning in the crisis response phase*, „Journal of Humanitarian Logistics and Supply Chain Management" 2022, vol. 12, nr 1, s. 30–53.

Ficoń K., *Logistyka kryzysowa. Procedury, potrzeby, potencjał*, Bel Studio, Warszawa 2011.

Ficoń K., *Trzy logistyki. Wojskowa, kryzysowa, rynkowa*, Bel Studio, Warszawa 2015.

Ficoń K., *Zastosowanie teorii masowej obsługi do analizy systemu zabezpieczenia logistycznego sytuacji kryzysowych*, „Systemy Logistyczne Wojsk" 2017, nr 47, s. 59–79.

Fitzsimmons M.F., *Hard hearts and open minds? Governance, Identity, and Counterinsurgency Strategy*, Institute for Defense Analyses, Alexandria, VA 2008, https://apps.dtic.mil/sti/pdfs/ADA491404.pdf [dostęp: 10.08.2023].

Gudzbeler G., Nepelski M., *Zintegrowana Platforma Symulacyjna Podmiotów Zarządzania Kryzysowego – spójne środowisko wirtualne*, „Bezpieczeństwo i Technika Pożarnicza" 2015, t. 38, nr 2, s. 89–96.

Iqbal Q., Mehler K., Yildirim M.B., *Comparison of Disaster Logistics Planning and Execution for 2005 Hurricane Season. Final Report*, Midwest Transportation Consortium, Ames, IA 2007.

Jahre M., *Humanitarian supply chain strategies – a review of how actors mitigate supply chain risks*, „Journal of Humanitarian Logistics and Supply Chain Management" 2017, vol. 7, nr 2, s. 82–101.

Kamau C.W., *Humanitarian Supply Chain Management in Kenya*, A Research Project Submitted in the Partial Fulfillment of the Requirements of the Masters of Business Administration Degree School of Business University of Nairobi, http://erepository.uonbi.ac.ke/handle/11295/76156?show=full [dostęp: 04.03.2023].

Kasprzycki D.D., *Konflikt zbrojny na Ukrainie w kontekście rosyjskiej koncepcji wojny nowej generacji*, „Rocznik Bezpieczeństwa Międzynarodowego" 2022, t. 16, nr 1, https://doi.org/10.34862/rbm.2022.1.5.

Krynojewski F.R., *Proces zarządzania kryzysowego*, 2018, https://www.jastrzebie.pl/fileadmin/user-files/aktualnosci/2018/10-pazdziernik/straz-miejska/Zarzadzanie-kryzysowe.pdf [dostęp: 10.08.2023].

Lindell M.K., *Evacuation planning, analysis, and management*, [w:] *Handbook of Emergency Response: A Human Factors and Systems Engineering Approach*, red. A.B. Badiru, L. Racz, https://www.researchgate.net/publication/284091989_Evacuation_planning_analysis_and_management [dostęp: 23.11.2022].

Logistyka humanitarna i zarządzanie kryzysowe. Wybrane problemy, red. T. Pokusa, M. Duczmal, Wydawnictwo Wyższej Szkoły Zarządzania i Administracji w Opolu, Opole 2009.

Malindžák D., Olejarz T., *Logistyka w zarządzaniu kryzysowym*, „Przegląd Nauk o Obronności" 2017, t. 2, nr 4, s. 137–147.

Marcinkowski J.M., *Humanitarny łańcuch dostaw w sytuacji wystąpienia katastrof naturalnych na przykładzie ugrupowania regionalnego ASEAN*, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2019.

Marzantowicz Ł., *Prewencyjna rola logistyki w katastrofie*, „Acta Universitatis Nicolai Copernici. Ekonomia" 2016, t. XLVI, nr 2, s. 173–184.

Międzynarodowa Federacja Czerwonego Krzyża i Czerwonego Półksiężyca. Relief items. Pobrano z: https://www.ifrc.org/en/what-we-do/disaster-management/responding/ongoing-operations/haiti-earthquake/relief-items (17.03.2023 r.).

Model Tender Document for Procurement of Goods, Government of India, Ministry of Finance, Department of Expenditure, 31.10.2021.

Modelowanie, symulacja i informatyczne wspomaganie decyzji w zarządzaniu kryzysowym, Zespół badawczy modelowania, symulacji i informatycznego wspomagania decyzji w sytuacjach konfliktowych i kryzysowych (kierownik zespołu: A. Najgebauer, prezentacja: Dariusz Pierzchała), https://docplayer.pl/15135724-Modelowanie-symulacja-i-informatyczne-wspomaganie-decyzji-w-zarzadzaniu-kryzysowym-prezentacja-dariusz-pierzchala.html [dostęp: 28.11.2022].

Pac B., *Istota zarządzania zabezpieczeniem logistycznym w sytuacjach kryzysowych i stanach nadzwyczajnych*, „Prace Naukowe Uniwersytetu Ekonomicznego" 2015, nr 383, s. 132–153.

Pomoc humanitarna w świetle prawa i praktyki, red. P. Grzebyk, E. Mikos-Skuza, Wydawnictwo Naukowe Scholar, Warszawa 2016.

Prawie 700 mln zł z UE na wsparcie dla uchodźców z Ukrainy, Gov.pl, 19.10.2022, https://www.gov.pl/web/mswia/prawie-700-mln-zl-z-ue-na-wsparcie-dla-uchodzcow-z-ukrainy [dostęp: 25.10.2022].

Standard products catalogue, International Federation of Red Cross and Red Crescent Societies, https://itemscatalogue.redcross.int [dostęp: 17.03.2023].

Szołtysek J., *Typologia obszarów stosowania logistyki – propozycja rozwiązania*, „Gospodarka Materiałowa i Logistyka" 2010, nr 8, s. 2–6.

Tomasini R.M., Van Wassenhove L.N., *From Preparedness to Partnerships: Case Study Research on Humanitarian Logistics*, „International Transactions in Operational Research" 2009, vol. 16, nr 5, s. 549–559.

Uniwersytet Otwarty Uniwersytetu Warszawskiego, Wydział Geologii, *Katastrofalne trzęsienie ziemi w Turcji i Syrii – dlaczego musimy badać uskoki?*, https://www.youtube.com/watch?v=MzzkluAvxZc [dostęp: 13.09.2023].

Van Wassenhove L.N., *Blackett Memorial Lecture. Humanitarian aid logistics: supply chain management in high gear*, „Journal of the Operational Research Society" 2006, nr 57, s. 475–489.

Walker P., Hein K., Russ C., Bertleff G., Caspersz D., *A Blueprint For Professionalizing Humanitarian Assistance*, „Health Affairs" 2010, vol. 29, nr 12, https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2010.1023 [dostęp: 28.07.2022].

Wang Z., Zhang J., *Agent-based evaluation of humanitarian relief goods supply capability*, „International Journal of Disaster Risk Reduction" 2019, nr 36, s. 101–105.

Weiss T.G., *Humanitarian business*, Polity Press, Cambridge 2013.

Wojna domowa gorsza od kataklizmu. Syryjski reżim stara się zadbać przede wszystkim o swoich, Rzeczpospolita, 10.02.2023, https://www.rp.pl/kleski-zywiolowe/art37934751-wojna-domowa-gorsza-od-kataklizmu-syryjski-rezim-stara-sie-zadbac-przede-wszystkim-o-swoich [dostęp: 3.03.2023].

Wolska A., *UE i ONZ zebrały 5,3 mld euro na pomoc humanitarną dla Syryjczyków*, EURACTIV.pl, 31.03.2021, https://www.euractiv.pl/section/polityka-zagraniczna-ue/news/ue-onz-syria-pomoc-humanitarna-wojna-domowa [dostęp: 25.10.2022].

Ye Y., Yan H., *Disaster Relief Supply Management*, [w:] *Natural Hazards: Impacts, Adjustments and Resilience*, red. E.N. Farsangi, IntechOpen, London 2020.

Zagrożenia i instytucje bezpieczeństwa międzynarodowego, red. E. Cziomer, Oficyna Wydawnicza AFM, Kraków 2016.

Akty prawne

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym, Dz.U. z 1990 r., nr 16, poz. 95.

Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym, Dz.U. z 1998 r., nr 91, poz. 578.

Przygotowanie logistyczne podmiotów realizujących pomoc humanitarną w Polsce

Streszczenie

Celem artykułu jest analiza przygotowania logistycznego podmiotów uczestniczących w działaniach niesienia pomocy humanitarnej. Część teoretyczna dotyczy znaczenia logistyki w pomocy humanitarnej. Część empiryczną stanowią przeprowadzone w 2021 r. badania na grupie podmiotów uczestniczących w działaniach pomocy humanitarnej.

Badania przeprowadzono metodą sondażu diagnostycznego, techniką ankietową PAPI (Papier and Pencil Interview) oraz CAPI (Computer-Assisted Personal Interview). Organizacje, które wzięły udział w badaniu, pozytywnie oceniły swój stan przygotowania do działań logistycznych w ramach niesienia pomocy humanitarnej. Okazuje się, że w badanych organizacjach pracują specjaliści odpowiedzialni za przedsięwzięcia logistyczne i zazwyczaj zajmują kierownicze stanowiska. Z badań wynika, że warto zwrócić uwagę na dostarczane środki pomocowe, ponieważ w wielu przypadkach są one niezgodne z potrzebami poszkodowanych.

Słowa kluczowe: logistyka humanitarna, pomoc humanitarna, zarządzanie kryzysowe, katastrofy

Logistic preparation of entities participating in humanitarian aid
Abstract

The goal of this paper is to analyze the logistic preparation of entities participating in humanitarian aid activities. The theoretical part looks at the importance of logistics in humanitarian aid. The empirical part of the paper consists of research with entities that participate in humanitarian aid activities in Poland. The research was conducted by means of a diagnostic poll method with the application of a survey techniques called Paper and Pencil Interview, and Computer-Assisted Personal Interview. The research was carried out in 2021. The organizations that took part in the research positively assess their state of logistic preparation for providing humanitarian aid. It turns out that the surveyed organizations employ specialists responsible for logistics and usually those specialists hold managerial positions. The research shows that it is worth paying attention to the proper distribution of relief items, because it happens that relief items are incompatible with the needs of the victims.

Keywords: humanitarian logistics, humanitarian aid, crisis management, disasters

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
No. 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-002
Received: 20.06.2023
Accepted: 21.09.2023

Mirosław Laszczak
PhD, University of Economics and Humanities in Bielsko-Biała
https://orcid.org/0000-0001-6060-4285

A critical link in the cybersecurity system

Introduction

Cybersecurity is a huge business, and at the same time one of the biggest challenges of our time. Any negligence in this area limits the economic development of companies, states and societies. According to forecasts, the annual costs associated with cybercrime will grow at a rate of 15% and reach the value of USD 10 trillion in 2025. 85% of small and medium-sized enterprises, especially in recent years, have taken the issue of digital security seriously, admitting that they stop saving on digital security and increase spending on IT network protection from year to year.[1]

Data theft and information leakage are a fact. And although blame is usually seen on the side of program weakness, in reality the weakest, and at the same time the key component of security is always the human being.

There is a popular saying that a safe computer is a turned off computer. But that's only partially true. The art of extracting information is also the ability to persuade someone to go to the office, turn the device on to the network and transfer the information.[2] Socio-technical tricks, manipulation, knowledge of the psyche turn out to be effective tools for obtaining classified material. Hackers and spies are already favored by the process of upbringing, which values such features as trust, empathy and

[1] *Cybersecurity trends: Looking over the horizon*, McKinsey & Company, 10.03.2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon#/ [accessed: 23.05.2023].

[2] K. Mitnick, W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, transl. by J. Dobrzański, Helion, Gliwice 2003, p. 19.

willingness to help. Hence, it is only a step to not deal with pushy requests or the inability to recognize signs of fraud. Computer scientists who perform penetration tests on behalf of companies reveal that hacking into security systems using social engineering tricks is almost one hundred percent effective.[3] Some character and personality dysfunctions push employees to commit crimes and reveal secrets.

The purpose of this article is to indicate which personality traits or which characterological dysfunctions are responsible for an employee's predilection to disclose secret data. What makes it so that, despite excellent security measures, phishing and leakage of important files still take place. In turn, the hypothesis that this text undertakes to verify is the conviction that the weakest, yet most important link in the cyber security system is the human being. At the same time, the article points to the development of security features and discusses how attempts are made to make it more difficult to conduct criminal activities inside an organization.

The study is based on an analytical and diagnostic approach. The primary research method to achieve the stated objectives is the method of analysis and critique of the literature on the subject and the analysis of review papers describing security breaches in cyberspace when the source of these breaches is the exploitation of human personality vulnerabilities.

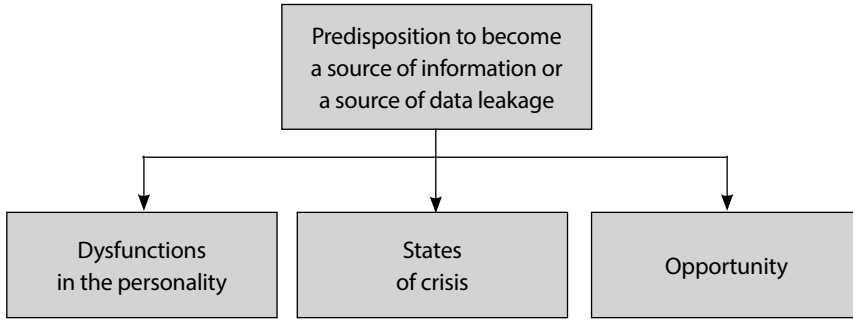
Whistleblower or traitor

Handling important and classified material is intriguing: it is combined with the illusion of being an insider, there is an impression of greater self-worth, one has access to knowledge that is guarded and therefore valuable, which in itself forces caution and self-control. Such people find themselves targeted by the intelligence services and are persuaded to cooperate in various ways. This is not always successful. A sense of patriotism, high morale, reluctance to get involved in dangerous situations, and fear of punishment stand in the way. At the same time, the inspiration to commit a crime turns out to be: the desire for excitement, the desire to experience adventure or the way to earn money. Bored with their previous jobs, the officials get involved in risky arrangements in which the stakes are really high. For some, maintaining a dual identity is an interesting and welcome adventure, for others it is exhausting and beyond stressful. There are prerequisites to help pick out the right person and make them a source of information.

In order to obtain a whistleblower and make him/her own agent, there should be special circumstances, namely with a deficit of responsibility, the encouragement for betrayal could be the experienced state of solstice in personal and professional life, and also a chance for high earnings or hope for global publicity and fame (Figure 1).

[3] *Ibidem*, p. 267.

Figure 1. Basic factors for involvement in espionage activities



Source: Author's own elaboration based on: U.M. Wilder, *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, p. 20.

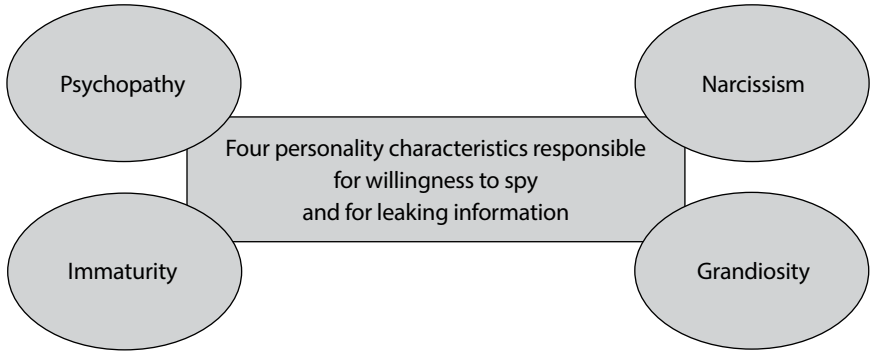
The dysfunctional personality takes many forms. Spies usually become thrill-seekers, struggling to hide their desire for power and seeking to take control of their surroundings. They are largely selfish, sometimes betraying a mania for greatness, in other cases trying to compensate for their own problems by taking revenge on the whole world.[4]

The domino principle works here: people with a dysfunctional personality fall into a state of crisis, look for a way out in activities associated with a higher risk and offering an effective escape from everyday troubles. Some emotions are covered by others, more expressive, stronger. Hence only a step to trading secrets; sometimes without thinking, sometimes out of desperation, which distorts the vision of the world and changes the understanding of the word "reason", sometimes in search of a particular thrill of emotions. Intelligence services are well aware of this, so they often initiate crisis situations themselves; there are no shortages of ways, it is enough to escalate debts, get involved in a risky sexual relationship or in a romantic relationship with a person controlled by the services. It is difficult to get out of such a system, and in addition, crises can easily be exacerbated, introducing an additional element of risk and exacerbating the state of mental enslavement.

There are at least four types of dysfunctional personality that are conducive to engaging in the activity of revealing secrets (Figure 2). Of course, it is impossible to say which of these personalities is most susceptible to being recruited by competing intelligence forces, but enumeration always begins with the psychopathic personality.

[4] U.M. Wilder, *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, p. 20.

Figure 2. The four personality components that lead people to steal information and espionage



Source: Author's own elaboration based on: U.M. Wilder, *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, pp. 20–28.

Psychopaths by nature are predators forever chasing risks. They are strangers to remorse, and experience limited feelings of guilt, shame, or regret. They easily mislead others. At first contact, they make a good impression. They at the beginning easy make friends, create an atmosphere of honest conversation, and slowly take control of the other person. At the same time, they are born liars who take pleasure in cheating and seizing power over others.[5] Enchanted by their pretended kindness, their superiors allow them to do more and more. Their power expands, their subordinates fear them, and their co-workers see merciless persecutors who, without hesitation, will use every means at their disposal to take revenge for their superiority.

Seeing how easy it is for them to take control of others, they want more and more until they overdo it. Mainly because they don't learn from their mistakes, can't plan for the long term, don't understand other people. Immersed in the present, they seek short-term excitement.

Psychopaths are not the only group of potential intelligence sources. Equally good sources of intelligence are narcissistic personalities, i.e., employees convinced of their uniqueness, who see themselves almost as organizational superstars that no one appreciates. So they fantasize about themselves and look for people who would attest to their uniqueness.

Skills, charisma, beauty, wisdom, prospects for the future – these features make up the inner image of a narcissistic person, it is enough that they find someone who will convince them that they are exactly like that, and they will be happy to share their opinion about co-workers and the uniqueness of the work they do. When a co-worker does not share their opinion, narcissists become malicious and vindictive. The possibilities of taking revenge on the organization, on superiors, even on the whole country

[5] J. Gibas, *Psychopata w pracy, w rodzinie i wśród znajomych*, Helion, Gliwice 2021, pp. 41–42.

are found primarily in the network.[6] Access to important information builds in them a conviction of superiority over others, which is dangerous insofar as they, sometimes experiencing Promethean illusions, want to save the world, to introduce a new fantastic order. It is among them that the sources of information leaks are recruited. All it takes is for top-secret documents to be made available online, secret services to be disseminated, governments will be shaken, international relations will crumble and the heads of superiors who failed to see to their duties will be sprinkled. They, in turn, will quickly find supporters shouting paeans to their courage, praising their uncompromisingness and affirming any uniqueness they can think of. Those eager for affirmation become easy objects to be controlled by the services and by all those whose approval and admiration they seek.

In the case of the April 2023 leak of classified documents, the reason was to impress members of an online OG group that publishes confidential documents. While Snowden was a Russian agent, here vanity came into play. "I had the impression that I was at the top of Mount Everest. I was special person and above everyone else. [...] I knew things that others had no idea about" – said one of the members of the group responsible for the data leak.[7]

The third group of people used in intelligence activities are people with immature personalities, treating the world as a great sandbox, life for them is the accumulation of adventures. They don't take their responsibilities seriously. They treat the entrusted secrets as toys that shine in front of the other participants of the game. Immaturity manifests itself in the inability to reliably assess the consequences of actions. They want to have fun and have an adventure, to see what it's like, regardless of the fact that the fun of being a spy is like riding on a slide. With each second you gain speed and even if you initially considered resignation, it turns out quite quickly that it is impossible to leave the game. People with an immature personality do not cope with difficult situations, difficulties at work, disagreements in personal life are enough to start looking for new activities, most often marked by an emotion similar to that remembered from the preschool game of policemen and thieves. Rapid boredom with routine work, leads to the search for stimulation and at the end lead to betrayal of secrets. Thanks to this, they are again in the center of attention, like a child who needs attention from adults.

Perhaps the most characteristic feature of the immature personality in adults is excessive fantasy, it seems to them that the world is to fulfill their desires.

The fourth group includes people with grandiosity, men with exaggerated ego. Having access to kept secrets, they gain the power to influence the future of their own organization, sometimes of the entire country, which gives them a sense of importance, which – it happens – they want to verify. When looking for a way to be at

---

6 U.M. Wilder, *The Psychology of Espionage and Leaking in the Digital Age*, *op. cit.*, s. 4.

7 M. Budzisz, *Wyciek tajnych dokumentów*, „Sieci" 2023, nr 16, pp. 45–47.

the center of events, they agree to break the law and share information they have access to.[8]

Internet – tool and tube

Cyberspace is an environment in which people with low self-esteem, low morale or poorly tolerating crisis situations feel especially good. Here they fall into uncontrollable gambling, break away from everyday affairs, play computer games, find an outlet for their addictions or compulsions. It is not for nothing that we talk about a global network, because it is actually a network into which psychologically sensitive and weaker individuals fall like insects into a trap set by a spider.

The Internet additionally suggests how to anonymously cause a data leak, it also promises to publicize the crime, global dissemination of stolen secrets and promises fame. Information that goes to the Internet is immediately reproduced and sent to other Internet users. The more sensational, the more legally protected information in them, the greater the chance that the stollen dates will gain a wider reach.

A study conducted in Canada found that online trolls are "prototype daily sadists" and there is a connection between "trolling" and those what psychologists call a "dark tetrad" of personality traits: narcissism, a tendency to manipulate others, psychopathy, and sadism.[9]

In assessing attitudes, the researchers used a Likert scale, allowing respondents to mark answers along the lines of: "The more beautiful and pure a thing is, the more satisfying it is to corrupt it," and "Hurting people is exciting".[10]

It is worth noting, however, that not all trolls are pathological characters, only some part shows signs of pathology and sadism,[11] most are ordinary people giving vent to anger, their daily frustrations and jealousies. The Internet additionally provides arguments convincing that betrayal or data leakage is no great wickedness. After all, one need only visit the Dark Web to see things far worse and more horrific. In view of the violations of decency on the Dark Web – data theft seem to be a trivial crime.[12]

---

8 U.M. Wilder, *The Psychology of Espionage*, *op. cit.*, p. 28.

9 Eadem, *The Psychology of Espionage and Leaking in the Digital Age*, „Studies in Intelligence" 2017, vol. 61, no. 2, p. 4.

10 C. Mooney, *Internet Trolls Really Are Horrible People: Narcissistic, Machiavellian, psychopathic, and sadistic*, Slate, 14.02.2014, http://www.slate.com/articles/health_and_science/climate_desk/2014/02/internet_troll_personality_study_machiavellianism_narcissism_psychopathy.html [accessed: 20.05.2023].

11 P.W. Singer, E.T. Brooking, *Nowy rodzaj wojny. Media społecznościowe jako broń*, transl. by S. Baranowski, Vis-á-vis Etiuda, Kraków 2019, p. 212.

12 K. Finklea, *Dark Web*, Congressional Research Service Report R44101, 10.03.2017, National Security Archive, https://nsarchive.gwu.edu/media/22737/ocr [accessed: 26.05.2023].

Growing danger

The development of IT networks takes place in a geometric progression. In highly developed countries, employees work on-line three to five days a week. They are relentlessly downloading information and uploading new information. It is assumed that the hosting industry will grow from $108.54 billion in 2023 to nearly $400 billion in 2030,[13] and there are perhaps no other industry that will grow at such a rate. Online service networks are expanding and the types of online activity and mobile platforms are multiplying. Demand for wider and more convenient access to online resources is emerging, while at the same time confidential data sets are swelling and natural security gaps are appearing. In 2020, each person generated an average of 1.7 megabytes of data per second.[14] All this information was aggregated, analyzed, passed through various filters, and then synthesized into conclusions of interest to everyone from large corporations to government agencies and foreign intelligence, to commercial organizations and small businesses. A hacker is no longer an introverted computer science student struggling with existential problems. Cybercrime is a multi-billion-dollar industry, with an elaborate organizational structure and massive research and development budgets. The attack cycle: from reconnaissance to data extraction is accelerating, no longer measured in weeks, but in days or even hours. The number of ransomware attacks doubles every year, starting in 2019. Phishing attacks saw an increase of 510% from January to February 2020.[15]

These numbers alone make it clear how much the information stored in the cloud is at risk. This is partly because risk management in the digital space has not kept pace with the multitude of transactions taking place. It is also not very clear what standard of protection should be set for data protection, so as not to block some services on the one hand, and on the other not to expose them to criminal activity. It is a constant maneuvering between the Scylla of convenience and the Charybdis of caution.

When constructing security, newer and newer technological solutions are used. Integrated programs to fight Internet espionage are being created, which combine artificial intelligence and machine learning. However, they also do not guarantee that human error will be noticed or predicted and that it will preventively block access to important data in time.

That is why multi-layer security is emerging (Figure 3).

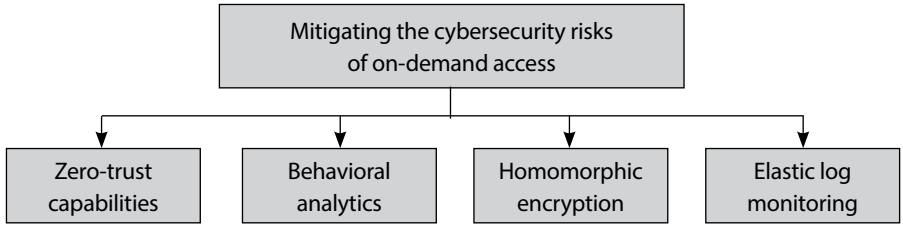
---

[13] *Web Hosting Services Market Size, Share, Growth Report, 2030*, https://www.fortunebusinessinsights.com/industry-reports/web-hosting-services-market-100863 [accessed: 26.05.2023].

[14] *Data Takes a Quantum Leap*, https://quantium.com/wp-content/uploads/2016/08/BFM_Quantium.pdf [accessed: 26.05.2023].

[15] *Cybersecurity trends: Looking over the horizon*, *op. cit.*

Figure 3. Contemporary trends of mitigating the cybersecurity risks



Source: Author's own elaboration based on *Cybersecurity trends: Looking over the horizon*, McKinsey & Company, 10.03.2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon# [accessed: 23.05.2023].

At the forefront is the principle of zero trust. Access to confidential data must be particularly strictly protected, and since it is well known how eager employees are to share confidential data with others, behavioural analysis is another layer of security, aimed at identifying and 'screening' employee behaviour. Each access request, the state and type of devices used are assessed for possible crime and, in the case of suspicious movements on the network or unusual forms of behaviour, deviating from the habits of a person using IT resources on a daily basis, access protection tools prevent such a person from logging in and enforce new authorisation methods.

Another form of security is login monitoring based on several open-source platforms. Each connection is analysed in real time, thus identifying potential threats.

Finally, homomorphic encryption comes to the rescue. With this technology, users can work with encrypted data without decrypting it first. In this way, strict data privacy requirements can be maintained and the significant increase in computing power allows this form of security to be used more widely.

Machine learning technologies, in conjunction with artificial intelligence, can further identify extraneous patterns and the impact of incompatible systems. They can automatically patch the holes in the system and detect an attack. It is just that cyber security services cannot keep up with the creativity of hackers. Even the best-organised and most secure system will not be able to withstand the bad will of a person who suddenly wants to make amends for imaginary grievances or who, with a Herostrates complex, longs for fame. Then the system's safeguards won't even have a chance to work and data leakage will become a reality.

Control

The fact that a person has become the source of a leak, and that after all it was easy to foresee, is usually known after the incident. However, the possibility of singling out a potentially dangerous person is no so difficult as earlier. In organisations

handling confidential data, there is continuous monitoring of employees. Machine learning and cognitive programmes conduct continuous digital surveillance. Network users are assessed, their personality is profiled and future activity is predicted based on current behaviour. Anything can be important, which is why cognitive technologies analyse the footprints, which are used to refer to as digital exhaust, i.e. the digital fumes left by employees during normal on- and off-duty activities. This huge body of information is analysed first by artificial intelligence and then by the organisation's safety officers. Of course, therein lies the danger of intruding into the intimate sphere of the lives of those being observed, but this is the price that is paid for protecting confidential and valuable information. There are other disadvantages of this type of employee surveillance.

Working in an atmosphere of constant suspicion, the awareness that one is being observed, and on different levels: from the general to the very intimate, affect the atmosphere at work. This manifests itself in employee behaviour such as:[16]

- resentment towards the employer and implicit contestation of work,
- deterioration of morale among employees,
- reduced productivity,
- erosion of loyalty to the organisation,
- and last but not the east the undermining of creativity cannot be forgotten either.

Constant supervision is always a burden. It becomes a clear signal sent in the direction of the employees, informing them of limited trust. For some, suspicion and scrutiny is an understandable part of the organisational culture, typical when dealing with valuable information, but for others, it is something unbearable that hinders the performance of professional duties. In the first instance, it discourages creative individuals – who usually have a strong need for autonomy – from continuing to work and staying with the company. The most prominent ones leave, leaving the teams they previously worked in without substantive support and without interesting ideas.

And what after a data leak?

Just as the weak part of security is the human being, with all character weaknesses and biases, so too he is the strong part of dealing with crisis situations after a data leak. What counts above all is creativity, which no artificial intelligence can currently afford.

The modus operandi does not resemble typical crisis management – no apologies, no abasing in front of the media and explaining everything to the public. Instead, a game resembling a hare and hounds in the house of mirrors begins. There are contradictory reports in the media and on the web, either that the leak was

[16] U.M. Wilder, *The Psychology of Espionage and Leaking in the Digital Age*, *op. cit.*, s. 9.

controlled, or that the information leaked is false and intended to mislead or target the hacker network, or that only what was supposed to see the light of day was leaked and instead much more valuable information was obtained. In addition, explanations and contradictory suggestions come from a variety of sources, most often unrelated to the site of the data leak. The public is misled and conspiracy theories are circulated by the mass media and coloured by social media.

This is well illustrated by the case of the leaked US intelligence documents, which became notorious after April 6th 2023. First, it was reported that the documents had previously been altered and differed from the originals. In the United States, serious losses of the secret service were written about, while on Russian news platforms the view was propagated that the whole leak was an intelligence operation prepared in fine detail and planned.[17]

Hair of the dog that bit you. Once a leak becomes a fact, the Internet proves to be a convenient tool for diluting the importance of the information revealed. Two patterns in particular prove helpful. The first is that anger is the emotion that travels fastest and reaches furthest on the web;[18] the second is that made-up stories spread six times faster on the internet than real ones.[19] Thus, an emotionally wrapped lie with the presentation of a new narrative is likely to re-format the thinking of Internet users. All the more so because anger is exciting and addictive at the same time.[20]

Along with disinformation activities, the source of the leak is identified and forms of security are modified. Additional knowledge about the characteristics and behaviour of those responsible for the disclosure of data is emerging, new safeguards are arriving, including methods of behavioural analysis to more effectively identify the personality traits of the perpetrator of the leak. Only that all these activities resemble a cat-and-mouse game and seem to have no end.

Conclusions

The risks associated with the disclosure of confidential and classified information are increasing year by year. Network intrusions are on the rise, data leaks are occurring, information trafficking is intensifying. But the data collected is also becoming more valuable every year. Everything is there: shopping behaviour, political and religious preferences, illnesses and treatments, new discoveries, ideas, business strategies, citizens' savings – everything is of interest to market players. And, of course, anything directly related to security – this is of particular interest to intelligence

[17] M. Budzisz, *op. cit.*
[18] P.W. Singer, E.T. Brooking, *op. cit.*, p. 209.
[19] *Ibidem*, p. 178.
[20] *Ibidem*, p. 213.

services. And since there are always weaknesses in the system, endless attempts are made to penetrate the security.

The opportunities for penetration are numerous. One that springs to mind is underdeveloped software, but more often than not, the main weakness is in the employees, whose carelessness, perhaps overload of duties and fatigue, but above all character flaws, provide a gateway through which important data leaks out.

According to the ancient Romans, whenever one wants to solve a difficult case, one must find the woman in it and understand her will.[21] Nowadays, when trying to find the place of the leak, the first place to look at is the people using the network. Second place is bugs in the programme itself and faulty system design. Attention is drawn to personality flaws: egotism, narcissism, psychopathic behaviour. Behavioural analysis looks for deviations from the usual behaviour of each employee, because perhaps behind such deviation lies a personality crisis.

The peculiarities of the Internet are capable of making a breach even in the case of healthy personalities, creating many opportunities for pathological traits to emerge.

Today, it is already known that the impulse to break the law, to spy and to take important data outside the organisation comes out of the human psyche and will never disappear, just as the personal tragedies experienced or the desire to improve one's own ego by showing the world how important information one has dealt with will never disappear. Of course, behavioural analysis attempts to detect human weaknesses, and machine learning and artificial intelligence also come into the picture. However, they are at least one step behind the cleverness of a human thinking about committing a crime. Thus, there is a never-ending procession of betrayals, leaks and new security features, and this will continue at least as long as humans are in charge of the most important secrets and have access to information so valuable that it already seems to have no upper bound.

In addition to security systems, the educational layer cannot, of course, be overlooked. Employees not only need to be monitored and their behaviour analysed, they should also be taught to distrust and be cautious. They need to know what sociological trickery will be used to penetrate beyond the security barrier.

References

Budzisz M., *Wyciek tajnych dokumentów*, „Sieci" 2023, nr 16, pp. 45–47.

Cybersecurity trends: Looking over the horizon, McKinsey & Company, 10.03.2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon# [accessed: 23.05.2023].

[21] W. Suworow, *Szpieg, czyli podstawy szpiegowskiego fachu*, transl. by A. Pawłowska, Dom Wydawniczy REBIS, Poznań 2017, p. 116.

Data Takes a Quantum Leap, https://quantium.com/wp-content/uploads/2016/08/BFM_Quantium.pdf [accessed: 26.05.2023].

Finklea K., *Dark Web*, Congressional Research Service Report R44101, 10.03.2017, National Security Archive, https://nsarchive.gwu.edu/media/22737/ocr [accessed: 26.05.2023].

Gibas J., *Psychopata w pracy, w rodzinie i wśród znajomych*, Helion, Gliwice 2021.

Mitnick K., Simon W., *Sztuka podstępu. Łamałem ludzi, nie hasła*, transl. by J. Dobrzański, Helion, Gliwice 2003.

Mooney C., *Internet Trolls Really Are Horrible People: Narcissistic, Machiavellian, psychopathic, and sadistic*, Slate, 14.02.2014, http://www.slate.com/articles/health_and_science/climate_desk/2014/02/internet_troll_personality_study_machiavellianism_narcissism_psychopathy.html [accessed: 20.05.2023].

Piekałkiewicz J., *Dzieje szpiegostwa*, Czytelnik, Warszawa 1999.

Singer P.W., Brooking E.T., *Nowy rodzaj wojny. Media społecznościowe jako broń*, transl. by S. Baranowski, Vis-á-vis Etiuda, *Kraków 2019*.

Suworow W., *Szpieg, czyli podstawy szpiegowskiego fachu*, transl. by A. Pawłowska, Dom Wydawniczy REBIS, Poznań 2017.

Web Hosting Services Market Size, Share, Growth Report, 2030, https://www.fortunebusinessinsights.com/industry-reports/web-hosting-services-market-100863 [accessed: 26.05.2023].

Wilder U.M., *The Psychology of Espionage*, „Studies in Intelligence" 2017, vol. 61, no. 2, pp. 19–36.

Wilder U.M., *The Psychology of Espionage and Leaking in the Digital Age*, „Studies in Intelligence" 2017, vol. 61, no. 2, pp. 1–17.

A critical link in the cybersecurity system

Abstract

The aim of this article is to identify human traits that are responsible for the propensity to betray and take secrets outside the organisation. For this purpose, an analytical-diagnostic approach has been used. The primary research method to achieve the stated objectives is the method of analysis and critique of the literature on the subject and the analysis of review papers describing security breaches in cyberspace, when the source of these breaches is the exploitation of human personality weaknesses.

First of all, personality and character traits leading to taking information outside the organisation or selling important data are identified. Psychopathic tendencies are identified, in addition to the immature, narcissistic and egotistical personality. The reasons for disclosing sensitive data are discussed. In this way, the article shows a different side of the problem of information system security and helps to understand the mechanism of theft or leakage of important information.

Since security weaknesses are attributed to personality traits, the article points to the possibility of anticipatory threat recognition and security enhancement. This is achieved through the use of machine learning, artificial intelligence and behavioural analysis. This succeeds in identifying potentially dangerous individuals who are not coping with their own problems.

Keywords: cyber security, personality, dysfunction, behavioural learning, artificial intelligence, data leakage

Kluczowe ogniwo w systemie cyberbezpieczeństwa
Streszczenie

Artykuł omawia rolę człowieka w systemie zapewnienia bezpieczeństwa cyfrowego. Podjęte na potrzeby artykułu badania wynikają z podejścia analityczno-diagnostycznego. Podstawową metodą badawczą służącą osiągnięciu wyznaczonych celów jest metoda analizy i krytyki literatury przedmiotu oraz analizy prac przeglądowych opisujących naruszenia bezpieczeństwa w cyberprzestrzeni wykorzystujące słabości ludzkiej osobowości.

Przede wszystkim identyfikowane są cechy osobowościowe i charakterologiczne prowadzące do wynoszenia informacji poza organizację lub sprzedawanie ważnych danych. Wskazano na skłonności psychopatyczne, a prócz nich wyróżniono jeszcze osobowość niedojrzałą, narcystyczną i egotyczną. Omówione zostały przyczyny ujawniania danych wrażliwych. W ten sposób artykuł ukazuje problem zabezpieczeń systemów informatycznych od innej strony oraz pomaga zrozumieć mechanizm kradzieży lub wycieku ważnych informacji.

Skoro słabości zabezpieczeń upatruje się w cechach osobowościowych – artykuł wskazuje na możliwość uprzedzającego rozpoznania zagrożeń i wzmocnienia bezpieczeństwa. Droga do niego wiedzie przez zastosowanie maszynowego uczenia się, wykorzystanie sztucznej inteligencji i analizy behawioralnej. Dzięki temu udaje się zidentyfikować potencjalnie niebezpieczne osoby, nie radzące sobie z własnymi problemami.

Słowa kluczowe: cyberbezpieczeństwo, osobowość, dysfunkcje, uczenie behawioralne, sztuczna inteligencja, wyciek danych

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-003
Data wpłynięcia: 29.05.2023
Data akceptacji: 26.09.2023

Jadwiga Mazur

dr hab., prof. WSB, Wyższa Szkoła Bezpieczeństwa z siedzibą w Poznaniu
https://orcid.org/0000-0001-7766-7864

Programy profilaktyczne na rzecz podnoszenia bezpieczeństwa hybrydowego

> We must confront bigotry by working to tackle the hate that spreads like wildfire across the internet[1].

Wprowadzenie

Współczesne zagrożenia są opisywane najczęściej jako hybrydowe. Ich złożoność odpowiada szybkiej zmianie, ta z kolei charakteryzuje się zmiennością systemów aksjonormatywnych. Zmiany wartości i norm oraz konsekwencje tych zmian widoczne są w ekonomii, działaniach wojennych, ale także w doniesieniach medialnych. Towarzyszą im emocje takie jak strach, lęk lub tylko obawa przed kolejnymi wydarzeniami.

Ten trudny okres anomii można próbować łagodzić różnymi narzędziami. Utworzone obronne i ochronne systemy bezpieczeństwa dają nadzieję na przetrwanie w sytuacjach trudnych, a usystematyzowane w dokumentach działania dają podstawę do wiary w to, że przyjęte założenia i wynikające z nich działania będą skuteczne. Oprócz tych systemów dobrze funkcjonują oddziaływania profilaktyczne, które choć nie przynoszą widocznych natychmiast, spektakularnych zmian, to w długofalowym działaniu są korzystne dla grup społecznych, do których są kierowane.

[1] António Guterres, United Nations Secretary-General, 2023, *What is hate speech?*, UN, https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech [dostęp: 23.05.2023].

Celem tego artykułu jest wykazanie roli i znaczenia ewaluacji programów profilaktycznych – na przykładzie ewaluacji pilotażowego programu zapobiegania radykalizacji i mowie nienawiści „Rozumiem=Szanuję" – oraz wykorzystania płynących z niej wniosków do dalszych działań.

Zagrożenia hybrydowe

W dyskursie publicystycznym, a także w rozważaniach naukowych od co najmniej dekady pojawia się termin „zagrożenia hybrydowe". Najczęściej zalicza się do nich rozprzestrzenianie nieprawdziwych informacji, podejmowanie prób manipulowania informacją wraz z dodaniem do niej komentarza, który wzmacnia przekaz strony próbującej wywierać wpływ na odbiorców. Głównym celem jest pozyskanie takiego audytorium, które zostanie przekonane o słuszności informacji i osiągnie masę krytyczną pozwalającą na dalsze rozpowszechnianie fake newsów i potwierdzanie ich wiarygodności. W dłuższej perspektywie umożliwia to podważenie zaufania zarówno do władzy, jak i innych znaczących instytucji państwa.

Nowe technologie pozwoliły na szybszy przekaz informacji oraz stworzyły możliwość różnorodnych, szerszych kontaktów międzyludzkich. Komunikowanie stało się szybsze, co wpływa na przyśpieszanie zachodzących zmian społecznych, a także wzmacnianie zagrożeń w cyberprzestrzeni[2]. Jednym z czynników przyśpieszających zachodzące zmiany jest globalizacja, dostęp do systemów informatycznych, a w związku z tym – do różnych sposobów interpretacji wydarzeń. Z jednej strony daje to możliwość wyboru źródła informacji, a z drugiej – powoduje otwarcie na wpływ wynikający ze sposobu jej interpretacji, od naukowej po teorie spiskowe.

Zagrożenia hybrydowe są definiowane głównie jako połączenie konwencjonalnych i niekonwencjonalnych (w tym pozamilitarnych), wielowymiarowych skoordynowanych przez główne podmioty działań skierowanych w krytyczne punkty, których celem jest podważenie zaufania i wiarygodności oraz pogłębianie podziałów społecznych przeciwnika[3]. W podobny sposób zagrożenia hybrydowe są wyjaśniane przez Davida Cattlera: łączą one środki wojskowe i pozamilitarne oraz tajne i jawne – obejmujące ataki cybernetyczne, presję ekonomiczną oraz dezinformację[4].

---

[2] K. Michalski, M. Jurgilewicz, *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Difin, Warszawa 2022, s. 11–21.

[3] P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych*, Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 18.05.2023].

[4] D. Cattler, Assistant Secretary General for Intelligence and Security, *What is NATO doing to address hybrid threats*?, 21.044.2021, https://www.nato.int/cps/en/natohq/news_183004.htm [dostęp: 18.05.2023].

Wizja społeczeństwa informacyjnego została już wielokrotnie opisana[5], niemniej wymaga dalszych badań dotyczących zmian w sposobach myślenia, otwarcia jednostek i grup na redefiniowanie się, zwłaszcza w sytuacji permanentnego lęku lub strachu powodowanego przez nieoczekiwane wydarzenia.

Rozwiązania informatyczne, których celem jest kreowanie informacji i jej odbiorców, pokazują, że tworzący się nowy paradygmat wymaga uwagi zarówno ze strony nauki, jak i inżynierii społecznej[6]. Ponadto, jak wskazywał Marian Golka już dwie dekady wcześniej, wzrasta znaczenie informacji i wiedzy[7], które jako towar są w tym kontekście szczególnie istotne. Podobnie stwierdza Tomasz Goban-Klas, uznając, że informacja została utowarowiona, coraz szybciej jest powielana, a uwaga odbiorców staje się dobrem rzadkim[8]. Ponadto na proces powstawania informacji i jej obiegu ma wpływ wiele czynników, takich jak fakty, opinie, doświadczenia odbiorcy, kontekst polityczny, społeczny, gospodarczy oraz emocje i zastosowane techniki wywierania wpływu. Pozwala to też zrozumieć znaczenie bezpieczeństwa informacyjnego, nie tylko na poziomie państwa, ale także na poziomie organizacji.

Wśród zagrożeń hybrydowych wymieniana jest dezinformacja, która jest jedną z metod naruszania zaufania do strategicznych podmiotów państwa, powoduje też wzrost poczucia zagrożenia i lęku w społeczeństwie. To skutkuje zacieraniem granic między wojną i pokojem, między informacją i dezinformacją, między działaniem świadomym a emocjonalnym.

Dezinformacja to proces prowadzony systematycznie, głównie za pośrednictwem mass mediów. Adresowana do opinii publicznej, jest lokowana pomiędzy wprowadzeniem odbiorcy w błąd a wpływaniem na niego. Dezinformacja jest uznana za skuteczną, gdy istnieje masa krytyczna zdezinformowanych, którzy skłonni są poddać się manipulacjom tzw. ekspertów „przywracających poczucie bezpieczeństwa"[9].

Jednym z warunków bezpieczeństwa jest budowanie odporności organizacji militarnych i pozamilitarnych. Zapobieganie dezinformacji, która może prowadzić do radykalizacji, jest jednym z wyzwań towarzyszących budowie odporności przez organizacje pozamilitarne. W ujęciu NATO odporność jest zdolnością społeczeństwa do przeciwstawiania się zagrożeniom, wstrząsom, która łączy w sobie gotowość cywilną i potencjał wojskowy. W takim rozumieniu gotowość cywilna jest głównym filarem

---

5 M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 138.

6 H. Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa*, Wydawnictwo Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2021, s. 7.

7 M. Golka *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 7.

8 T. Goban-Klas, *Tabloidyzacja mediów a neopopulizm*, [w:] *Media – Populizm – Demokracja. Zapis konferencji z dnia 5 listopada 2011 roku*, Ośrodek Myśli Społecznej im. Ferdynanda Lassalle'a, Wrocław 2011, s. 16.

9 V. Volkoff, *Przedmowa*, [w:] *Dezinformacja oręż wojny*, oprac. V. Volkoff, tłum. A. Arciuch, Wydawnictwo Delikon, Warszawa 1991, s. 8.

umożliwiającym zbiorową obronę i może służyć wzmacnianiu cywilnej gotowości do obrony[10].

Zapobieganie dezinformacji jest więc wyzwaniem dla wielu podmiotów, których zadaniem jest przekaz wiedzy, kształtowanie umiejętności i kompetencji. To również wyzwanie dla twórców programów profilaktycznych zapobiegających radykalizacji kierowanych do młodych ludzi.

Rola edukacji w kreowaniu bezpieczeństwa hybrydowego

Zdefiniowanie bezpieczeństwa hybrydowego jest dużym wyzwaniem. W literaturze przedmiotu próby takie odnoszą się głównie do bezpieczeństwa informacyjnego. Niemniej można poszukiwać odniesienia do budowy bezpieczeństwa hybrydowego w działaniach The Resilience Comittee (RC), który jest najwyższym organem doradczym NATO ds. odporności i gotowości cywilnej. Zgodnie z wytycznymi w tym zakresie każde państwo członkowskie NATO powinno być odporne na zagrożenia militarne i pozamilitarne, takie jak zakłócenia infrastruktury krytycznej, klęski żywiołowe, ataki zbrojne i hybrydowe. Odporność jest tutaj podkreślana jako zbiorowe zobowiązanie wynikające z artykułu 3 Traktatu Północnoatlantyckiego[11]. W całości tych wielowymiarowych działań można próbować przewidzieć także te z zakresu budowy bezpieczeństwa w obszarze zapobiegania dezinformacji. Wskazuje na to również Tomasz Nowak, który stwierdza, że istotą działań hybrydowych jest „użycie destrukcyjnych narzędzi pozamilitarnych na płaszczyźnie: politycznej, ekonomicznej (gospodarczej), społecznej, kulturowej, ideologicznej, humanitarnej"[12]. Zwraca też uwagę na to, że obecnie wśród działań hybrydowych Rosji i Białorusi prowadzone są procesy dezinformacyjne.

W ramach działań związanych z budową bezpieczeństwa hybrydowego można ująć wzmacnianie odporności polityczno-militarnej, energetycznej, społecznej i informacyjnej, potraktowane jako ciągły, wielowymiarowy proces.

W sytuacji zagrożeń hybrydowych istotna jest edukacja do bezpieczeństwa. To dość szerokie pojęcie obejmujące kwestie bezpieczeństwa indywidualnego, grup

---

[10] „Resilience is a society's ability to resist and recover from such shocks and combines both civil preparedness and military capacity. Civil preparedness is a central pillar of Allies' resilience and a critical enabler for the Alliance's collective defence, and NATO supports Allies in assessing and enhancing their civil preparedness". *Resilience, civil preparedness and Article 3*, NATO, https://www.nato.int/cps/en/natohq/topics_132722.htm [dostęp: 18.05.2023].

[11] *Tackling online disinformation*, European Commission, https://digital-strategy.ec.europa.eu/en/policies/online-disinformation [dostęp: 18.05.2023].

[12] T. Nowak, *Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski*, „Roczniki Nauk Społecznych" 2022, t. 14 (50), nr 4, s. 36, https://repozytorium.kul.pl/bitstream/20.500.12153/4217/1/Nowak_Tomasz_Budowa_odpornosci_na_obecne_i_przyszle_zagrozenia.pdf [dostęp: 18.05.2023].

społecznych, jak i całego państwa. Rozwiązania przyjęte w tego typu edukacji obejmują również oddziaływania o charakterze profilaktycznym. W ich realizację włączone są podmioty, które w zakres swojego działania mają wpisane bezpieczeństwo. To często specjalistyczne programy opracowywane przez specjalistów, dedykowane różnym grupom wiekowym i zawodowym, w zależności od potrzeby i zidentyfikowanych zagrożeń. Ponadto odnoszą się do specyfiki lokalnych społeczności, ich poczucia bezpieczeństwa, wraz z uwzględnieniem ich potrzeb. Jednym z ważnych elementów tych programów jest wzmacnianie więzi społecznych. Wymaga to od kreatorów działań profilaktycznych budowania programów opartych na wielowymiarowości wyzwań związanych z zagrożeniami oraz korzystania z interdyscyplinarności edukacji do bezpieczeństwa.

Na poziomie formalnej edukacji oznacza to przyjęcie obowiązku prowadzenia programów wychowawczo-profilaktycznych na różnych szczeblach kształcenia. Ich celem jest głównie transfer wiedzy o podstawowych zagrożeniach, kształtowanie umiejętności radzenia sobie z nimi oraz budowanie kompetencji, które pozwolą na ich wykorzystanie. Kolejny poziom edukacji do bezpieczeństwa (włączając profilaktykę o różnych strategiach i poziomach) to programy i aktywności edukacyjne prowadzone przez różne podmioty – w tej części mogą się mieścić programy dedykowane przeciwdziałaniu konkretnym zagrożeniom proponowane przez militarne, paramilitarne i cywilne grupy dyspozycyjne (policja, straże, służby ratownicze itp.), a także miejskie i gminne programy bezpieczeństwa. Kolejny etap to edukacja nieformalna wynikająca z procesu socjalizacji. Łączenie tych poziomów daje możliwość kumulacji i pogłębienia wiedzy o bezpieczeństwie.

W zakres tych przedsięwzięć, a zwłaszcza w zakres programów profilaktycznych, wchodzą też takie, które oprócz wyraźnie wskazanego celu (jak opisany poniżej program zapobiegający radykalizacji), włączają w proponowane moduły wiedzę pozwalającą na łączenie kilku elementów. Mogą one dotyczyć bezpieczeństwa kulturowego, kształtowania umiejętności rozwiązywania konfliktów, radzenia sobie z emocjami itp. – i łącznie mogą wzbogacać kapitał kulturowy odbiorców i wyposażać ich w nową wiedzę, umiejętności i kompetencje.

Profilaktyka – teoria i praktyka

Edukacja do bezpieczeństwa – jak wspomniano wcześniej – to dość szerokie pojęcie, w którym mieszczą się oddziaływania profilaktyczne. Profilaktyka to pojęcie również wielokrotnie definiowane, z podziałem na strategie i poziomy realizowane w obszarze zdrowia i zapobiegania działaniom niepożądanym. W jej definicjach najczęściej podaje się zapobieganie – poprzez działanie i stosowanie zespołu środków do tego służących – występowaniu zjawisk niepożądanych w życiu jednostek i grup. O potrzebie profilaktyki pisała już Helena Radlińska, ujmując ją jako

zapobieganie klęskom społecznym i wykolejeniu jednostek[13]. Po roku 1990 profilaktyką, jej opisem, poziomami i strategiami zajmują się Zbigniew Bronisław Gaś[14] i Barbara Woynarowska[15] oraz inni autorzy z różnych dyscyplin naukowych. Jedną z częściej przytaczanych jest dość ogólna i szeroka definicja sformułowana przez Brunona Hołysta, który opisuje profilaktykę jako system środków i metod, których zadaniem jest usunięcie przyczyn ujemnych zjawisk społecznych i stworzenie odpowiednich warunków dla prawidłowego rozwoju i funkcjonowania jednostek i grup[16]. Natomiast Z.B. Gaś wskazuje na proces wspomagania jednostki w trudnościach, które mogą jej zagrażać w prawidłowym rozwoju i dezorganizować życie, oraz na inicjowanie i wzmacnianie czynników chroniących[17]. Z przytoczonych definicji można wyłonić cele profilaktyki, którymi są zapobieganie, zmniejszanie ryzyka, promocja zdrowia, wspomaganie w dążeniu do nabycia wiedzy, umiejętności i kompetencji służących zdrowemu stylowi życia.

W planowaniu oddziaływań profilaktycznych oprócz wyznaczonego celu głównego i celów szczegółowych, przyjmuje się również założenia, zakłada spodziewane efekty, przyjmuje formy oddziaływania, czas i zakres działań i kontroli efektów – które przyjmują postać ewaluacji. W nowoczesnych modelach profilaktycznych widoczna jest dbałość o kontrolę efektów, która pozwala na bieżące dokonywanie zmian lub dostosowywanie programów do odbiorców.

W literaturze naukowej dotyczącej wyzwań z zakresu profilaktyki wymienia się jej poziomy i strategie. Najczęściej wyróżnia się trzy poziomy oddziaływań: profilaktykę pierwszo-, drugo- i trzeciorzędową, akcentując zakres jej oddziaływania i adresatów[18]. Nazwy tych poziomów mogą się różnic (np. profilaktyka uniwersalna, selektywna i wskazująca[19]), ale ich główny cel pozostaje taki sam. Wśród strategii profilaktycznych wymienia się strategię edukacji normatywnej, strategię edukacji rówieśniczej, przekazu informacji, kształtowania umiejętności życiowych, alternatyw, rozwijania umiejętności wychowawczych, rozwoju zasobów środowiskowych[20]. Każda z tych strategii w połączeniu z poziomem profilaktyki i grupą, do której jest adresowana w zależności od potrzeb, jest ważnym obszarem edukacji – dającym możliwości

---

13 T. Wiśniewski, *Profilaktyka pedagogiczna*, PWN, Warszawa 1989, s. 17.

14 Z.B. Gaś, *Profilaktyka w szkole*, WSiP, Warszawa 2006.

15 B. Woynarowska, *Edukacja zdrowotna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

16 B. Hołyst, *Kryminologia*, Wydawnictwo Naukowe PWN, Warszawa 1994, s. 525.

17 Z.B. Gaś, *Profilaktyka w szkole*, [w:] *Profilaktyka w szkole. Poradnik dla nauczycieli*, red. B. Kamińska-Buśko, J. Szymańska, Centrum Metodyczne Pomocy Psychologiczno-Pedagogicznej, Warszawa 2005, s. 14.

18 Z.B. Gaś, *Szkolny program profilaktyki. Istota, konstruowanie, ewaluacja*, Ministerstwo Edukacji Narodowej i Sportu, Warszawa 2003, s. 20–21.

19 Zob. K. Ostaszewski, *Nowe definicje poziomów profilaktyki*, „Remedium" 2005, nr 7–8, s. 40–41.

20 *Metody i strategie profilaktyczne*, 20.05.2010, Krajowe Biuro Do Spraw Przeciwdziałania Narkomanii, https://www.kbpn.gov.pl/portal?id=105808 [dostęp: 20.05.2023].

dalszego rozwoju i świadomego kształtowania życia. W podejściu teoretycznym odnoszącym się do działań profilaktycznych autorzy nawiązują do teorii społecznego uczenia się, teorii przywiązania, teorii zachowań problemowych i koncepcji resilience.

Głównym zadaniem profilaktyki – w ramach wymienionych celów, poziomów, strategii i podejść teoretycznych w opracowywaniu programów – jest transfer nowej wiedzy, kształtowanie umiejętności i kompetencji. To duże wyzwanie zwłaszcza w czasie zwiększających się zagrożeń hybrydowych, wzrastającego lęku i obaw przed zmianą. To również potrzeba ciągłej redefinicji samego siebie, żeby móc odnaleźć się w szybko zmieniającej się rzeczywistości.

Ewaluacja programu zapobiegania mowie nienawiści

W definicji mowy nienawiści proponowanej przez ONZ podkreśla się, że jest to komunikacja realizowana przez zachowanie, mowę, pismo, w której używa się dyskryminującego innych języka z powodu ich odmienności religijnej, etnicznej, rasowej, pochodzenia, płci lub innych czynników tożsamości[21]. Jednocześnie zaznacza się, że nie ma uniwersalnej definicji mowy nienawiści w prawie międzynarodowym dotyczącym praw człowieka. Jest to nadal przedmiotem dyskusji odnoszącej się do wolności wypowiedzi i opinii. Niemniej jest to termin szerszy niż podżeganie do dyskryminacji, wrogości lub przemocy, co z kolei jest już zabronione przez międzynarodowe prawo dotyczące praw człowieka. Mowa nienawiści może mieć trzy cechy: 1) rozpowszechnianie w dowolnej formie wypowiedzi (obrazów, przedmiotów, symboli, gestów itp.), online i offline; 2) stronniczość, nietolerancyjność połączona z uprzedzeniem, poniżanie osób lub grup; 3) odwoływanie się do elementów tożsamości i odmienności[22].

Mowa nienawiści szerząca się w internecie wpisana jest również w procesy dezinformacji, na którą pozwalają narzędzia cyfrowe. Wzmacnia ją anonimowość i umiejętność posługiwania się technikami wywierania wpływu. Taka informacja ma wielką moc, a także duży potencjał dotarcia do szerokiego i zróżnicowanego audytorium w czasie rzeczywistym.

Wzrastająca tolerancja mowy nienawiści w przestrzeni publicznej może sprzyjać utrwalaniu stereotypów i uprzedzeń, akceptacji zachowań o charakterze dyskryminacyjnym. Ponadto brak wiedzy lub niepełna wiedza dotycząca odmienności połączona z negatywnymi emocjami mogą stać się czynnikiem wyzwalającym dla mowy nienawiści połączonej z brakiem tolerancji. Stąd potrzeba nie tylko przestrzegania uregulowań prawnych dotyczących mowy nienawiści i dyskryminacji, ale także edukacji do bezpieczeństwa i opracowywania programów profilaktycznych, które w sposób spójny i przemyślany będą edukować i wzmacniać akceptację dla odmienności.

---

[21] *What is hate speech?*, UN, https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech [dostęp: 23.05.2023].

[22] *Ibidem*.

Wyniki badań wskazują na związek dopuszczalności mowy nienawiści u badanej młodzieży z deklarowanymi poglądami politycznymi. Młodzież deklarująca poglądy lewicowe częściej domagała się zakazania mowy nienawiści niż osoby deklarujące poglądy prawicowe[23]. Autorzy przytoczonych badań podkreślają, że młodzież części niż dorośli styka się z sytuacjami, gdzie pojawiają się przykłady mowy nienawiści. Wskazują też, że „ekspozycja na mowę nienawiści jest istotnie skorelowana z agresją słowną. Osoby częściej narażone na kontakt z mową nienawiści deklarują wyższy poziom słownej agresji aniżeli osoby mające mniejszy kontakt z mową nienawiści. Związek ten jest silniejszy wśród młodzieży niż wśród dorosłych"[24]. Wyróżniają też dwie kategorie mowy nienawiści: tradycyjną i racjonalizującą. Pierwsza dotyczący wulgaryzmów i obraźliwych określeń wyrażających nienawiść bezpośrednio, natomiast druga odnosi się do stwarzania pozorów racjonalnego argumentowania, która przez adresatów tych argumentacji również określana jest jako obraźliwa[25].

W raporcie z 2017 r. ta sama grupa badaczy wskazuje, w jakim stopniu wydarzenia z lat 2014 i 2016 odbiły się na postawach Polaków. Podkreślają, że w kampaniach wyborczych (prezydenckiej i parlamentarnej) w roku 2015 często przywoływano zagrożenia związane z migracją, wzbudzano lęk społeczny przed uchodźcami, wyznawcami islamu, odwoływano się do resentymentów antysemickich i antyukraińskich. W tym czasie Europa również stanęła przed dużym wyzwaniem dotyczącym narastającej fali imigracji i powiązanych z nią procesów integracyjnych[26]. Autorzy raportu wskazują też na uwarunkowania kulturowe i czynniki takie jak autorytaryzm i werbalna agresja, które pozwalają zrozumieć, jakie osoby częściej przejawiają uprzedzenia, a w konsekwencji – stosują mowę nienawiści.

Z kolei Agnieszka Pazderska we wnioskach ze swoich badań wskazuje, że częsty kontakt młodych dorosłych z informacjami dotyczącymi mowy nienawiści i hejtu w internecie może obniżać wrażliwość na tego typu treści, a w efekcie powodować obojętność, bezsilność, ale i „brak wiedzy na temat narzędzi niezbędnych

---

[23] M. Bilewicz *et al.*, *Mowa nienawiści. Raport z badań sondażowych*, Fundacja im. Stefana Batorego, Warszawa 2014, s. 103, https://www.researchgate.net/profile/Mikolaj-Winiewski/publication/317318302_Mowa_nienawisci_Raport_z_badan_sondazowych/links/5931ba72a6fdcc89e7a631bc/Mowa-nienawisci-Raport-z-badan-sondazowych.pdf [dostęp: 24.05.2023].

[24] *Ibidem*, s. 106.

[25] *Ibidem*, s. 109.

[26] M. Wiśniewski *et al.*, *Mowa nienawiści, mowa pogardy. Raport z badania przemocy werbalnej wobec grup mniejszościowych*, Fundacja im. Stefana Batorego, Warszawa 2017, s. 4, https://www.researchgate.net/profile/Mikolaj-Winiewski/publication/317318364_Mowa_nienawisci_mowa_pogardy_Raport_z_badania_przemocy_werbalnej_wobec_grup_mniejszosciowych/links/5931b5dba6fdcc89e7a59de7/Mowa-nienawisci-mowa-pogardy-Raport-z-badania-przemocy-werbalnej-wobec-grup-mniejszosciowych.pdf [dostęp: 24.05.2023].

do reagowania na ten problem"[27]. Widać więc palącą potrzebę nowej wiedzy dotyczącej radykalizacji, mowy nienawiści i hejtu.

Poniżej zostanie zaprezentowany profilaktyczny program edukacyjny zapobiegający radykalizacji wiodącej do dyskryminacji i mowy nienawiści „Rozumiem=Szanuję", autorstwa Marzeny Kordaczuk-Wąs i realizowany przez jej zespół z Polskiej Platformy Bezpieczeństwa Wewnętrznego, wraz z ewaluacją jego pilotażu. Projekt został zrealizowany przez Polską Platformę Bezpieczeństwa Wewnętrznego we współpracy z I Liceum Ogólnokształcącym w Gorzowie Wielkopolskim[28] w okresie od grudnia 2021 do czerwca 2022 r.

Program „Rozumiem=Szanuję" w swoich celach proponuje transfer wiedzy, umiejętności i kompetencji, w które uczeń będzie wyposażony w trakcie realizacji poszczególnych modułów programu – co wpisuje się w zadania dotyczące mowy nienawiści w mediach rekomendowane przez Ministerstwo Edukacji i Nauki, tym bardziej że umożliwia to zapis w pkt. 7 dotyczący corocznego minimalnego zakresu zajęć profilaktycznych uświadamiających ten problem[29]. Ewaluacja to proces zbierania, opracowywania i udostępniania materiałów zawierających informacje dotyczące treści programu celem ich dalszego wykorzystania w przyszłych realizacjach, to również „systemowe badanie, prowadzone z użyciem zróżnicowanych metod, złożone ze zbierania danych, analizy, oceny, informowania o wynikach"[30].

Zaplanowane działania edukacyjne prowadzone były w formie warsztatów, dyskusji, dni tematycznych, ćwiczeń umiejętności życiowych (w tym psychologicznych i radzenia sobie ze stresem i agresją, budowania samokontroli) zgodnych z celami wychowawczo-edukacyjnymi szkoły.

Założono następujące rezultaty: wyposażenie beneficjentów programu w rzetelną wiedzę o polaryzacji społecznej i procesach radykalizacji prowadzących do dyskryminacji i mowy nienawiści oraz o skutkach prawnych i społecznych przestępstw motywowanych nienawiścią; wzmocnienie umiejętności psychospołecznych sprzyjających pozytywnej komunikacji w środowisku rówieśniczym, rodzinnym i szkolnym, w tym umiejętności konstruktywnej polemiki dotyczącej polaryzacji społecznej prowadzącej do braku tolerancji dla odmienności, rozwijanie hobby.

---

[27] A. Pazderska, *Tolerancja zachowań związanych z szerzeniem nienawiści w internecie w grupie młodych dorosłych: analiza empiryczna*, „Polityka i Społeczeństwo" 2023, t. 21, nr 1, s. 228, https://journals.ur.edu.pl/polispol/article/view/4492/4041 [dostęp: 24.05.2023].

[28] Projekt finansowany przez Islandię, Liechtenstein i Norwegię z Funduszy EOG w ramach Programu Aktywni Obywatele – Fundusz Regionalny.

[29] *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, wyd. 4 uaktualnione, Ministerstwo Edukacji Narodowej, Warszawa 2020, s. 66–67.

[30] *Ewaluacja. Poradnik dla pracowników administracji publicznej*, red. S. Bienias, P. Strzęboszewski, E. Opałka, Ministerstwo Rozwoju Regionalnego, Warszawa 2012, s. 12, https://www.ewaluacja.gov.pl/media/11102/Poradnik_ewaluacji.pdf [dostęp: 20.10.2023].

W procesie ewaluacji starano się uwzględnić interesy i cele stron uczestniczących w programie. Rola ewaluatora wymagała pośredniczenia w wymianie informacji w celu wypracowania modelu odpowiadającego wszystkim przygotowującym ostateczną wersję programu (autor, zespół realizujący, uczniowie, nauczyciele, rodzice). W takim procesie ważne są funkcje prowadzonej ewaluacji takie jak:

- konkluzywna – podsumowanie efektów działań, ustalenie związków przyczynowo-skutkowych pomiędzy działaniami a zakładanymi efektami;
- formatywna – dążenie poprzez wdrożenie wypracowanych rekomendacji do poprawy jakości przedsięwzięć podejmowanych w programie (skuteczność, efektywność, użyteczność);
- społeczna – zwiększenie poziomu uspołecznienia, zwiększenie mobilizacji społecznej i poparcia społecznego, motywacji do działania i współodpowiedzialności[31].

Elementy ewaluacji programu „Rozumiem=Szanuję" zostaną przedstawione z dwóch powodów. Pierwszy to wskazanie, jak bardzo ważna jest ewaluacja programów w czasie zagrożeń hybrydowych, zwłaszcza w zakresie przeciwdziałania polaryzacji społecznej i mowie nienawiści prowadzącej do radykalizacji. Drugi to zwrócenie uwagi na istotne potrzeby młodego pokolenia w zakresie wsparcia psychologicznego, zwłaszcza radzenia sobie z trudnymi emocjami, umiejętności rozwiązywania problemów, komunikowania się, tolerancji dla odmienności.

Ewaluację zewnętrzną przygotowała osoba niebędąca autorem programu (ewaluacja ex-ante realizowana przed przyjęciem jego ostatecznej wersji) na wniosek autorki programu i jej zespołu. Badaniu podlegało pilotażowe przeprowadzenie programu i jego wpływ na podniesienie poziomu wiedzy w zakresie mowy nienawiści i jej rozpoznawania, reagowania i zapobiegania. Ewaluację wykonano w celu sformułowania wniosków i rekomendacji do wykorzystania w kolejnych realizacjach programu. Ewaluację przeprowadzono w trakcie pilotażowej realizacji programu w Gorzowie Wielkopolskim w I semestrze roku szkolnego 2021 i II semestrze roku szkolnego 2022.

W ewaluacji ocenie ex-ante podlegały następujące zagadnienia:

1) zasadność diagnozy (czy problemy są dalej aktualne, zmniejszyły się / zwiększyły się);
2) analiza zidentyfikowanych problemów;
3) jakie czynniki mogą wpływać na szanse powodzenia programu;
4) wewnętrzna spójność programu z programem profilaktyczno-wychowawczym szkoły (na ile cele są spójne z zdefiniowanymi priorytetami szkoły w jej programach);
5) ustalenie powiązań między celami programu a jego efektami (w tym wypadku celami i zawartością programu),

[31] *Ibidem*, s. 15.

6) przewidywany wpływ programu na pożądane założone zmiany w obszarze zapobiegania mowie nienawiści;
7) analiza planowanego systemu wdrażania.

Źródłami danych do badań ewaluacyjnych były: diagnoza młodzieży, dla której przeznaczono pilotaż programu, ministerialne zalecane przedsięwzięcia w zakresie profilaktyki, szkolny program profilaktyczny, wyniki badań ewaluacyjnych uczniów, rodziców, nauczycieli i realizatorów programu. Złożoność badania wymagała zastosowania triangulacji metod, technik, narzędzi badawczych i analiz.

Istotnym elementem badań było zastosowanie tych samych technik po realizacji poszczególnych segmentów programu. Badania ewaluacyjne dotyczyły materiałów, dowodów empirycznych, dzięki którym uzyskano odpowiedzi na pytania problemowe dotyczące adekwatności przyjętych celów i metod do zdiagnozowanych wyzwań, skuteczności zastosowanych metod i profesjonalizmu osób prowadzących zajęcia, relacji pomiędzy poniesionymi nakładami a osiągniętymi efektami, oceny uzyskanych efektów w odniesieniu do wyzwań, spójności programu „Rozumiem=Szanuję" i strategii wychowawczo-profilaktycznej szkoły, pozytywnych efektów programu wśród jego beneficjentów.

Przeprowadzenie pilotażu programu zostało poprzedzone przez jego autorkę dogłębną diagnozą dotycząca podejmowanej tematyki, a sam program został przygotowany na podwalinach teorii naukowej i przy zastosowaniu nowoczesnych metod jego realizacji.

Zaplanowane działania edukacyjne obejmowały warsztaty, dyskusje, dni tematyczne, ćwiczenia umiejętności życiowych psychologicznych i społecznych (radzenia sobie ze stresem i agresją, budowania samokontroli) oraz zajęcia wolnoczasowe wzbogacające ofertę profilaktyczną szkoły (partnera programu).

Zakładane rezultaty to wyposażenie uczestników w wiedzę o polaryzacji społecznej i procesach radykalizacji prowadzących do dyskryminacji i mowy nienawiści – zaplanowano zajęcia o wiodącym temacie „Radykalizacja – mit czy fakt" dla 90 uczniów, 30 rodziców i 50 nauczycieli, w tym:

- zajęcia dla 90 uczniów „Dyskryminacja i mowa nienawiści",
- zajęcia dla 90 uczniów „Żywa biblioteka" oraz trzy spotkania z przedstawicielami mniejszości i ćwiczenie „Goście",
- trzy spotkania dla 90 uczniów – moderowana dyskusja „Tydzień różnorodności kulturowej",
- projekcja trzech filmów z debatą po filmie w ramach „Dyskusyjnego Klubu Filmowego – Piękno i wyzwania wielokulturowego świata" dla 90 uczniów.

W ramach wzmacniania umiejętności psychospołecznych:

- jeden warsztat dla 90 uczniów, w trzech modułach:
  1. „Kształtowanie myślenia rozwojowego",
  2. „Emocje i stres a uważność na siebie i innych",

3. „W jaki sposób uprzedzenia i dyskryminację można przekształcić w zrozumienie i akceptację?"

- jeden wykład dla 90 rodziców „Zrozumieć Nastolatka",

W ramach rozwijania hobby:

- konkurs fotograficzny dla 90 uczniów: „Ja–Ty. My–Oni. Oblicza różnorodności")[32].

W procesie ewaluacji zapoznano się w wynikami diagnozy uczniów, poddano analizie program wychowawczo-profilaktyczny szkoły z uwzględnieniem jego spójności z zaleceniami ministerialnymi, a następnie przy pomocy wyżej opisanych narzędzi systematycznie prowadzono badania wśród beneficjentów programu (włączając w to również nauczycieli i zespól realizujący program).

Wyniki procesów ewaluacyjnych wskazują, że działania wyznaczone do realizacji programu odbyły się zgodnie z przyjętym kalendarium. Biorąc pod uwagę ich złożoność i wyzwania organizacyjne, należy je ocenić bardzo dobrze, ponieważ założone cele, pozwalające na zrozumienie mechanizmów wielokulturowości, różnic i wynikających z nich nieporozumień, zostały zrealizowane. Wnioski z badań uprawniały też do stwierdzenia, że program uruchomił transfer wiedzy oddolnej. Założono, że uczniowie dzięki przekazanej w ramach programu wiedzy mogą uruchomić pozytywne mechanizmy w lokalnych społecznościach, w czasie zachodzących zmian związanych z nagłą i dużą migracją (zagrożenie polaryzacją międzykulturową). Wiedza ta oparta na module prawnym, socjologicznym i psychologicznym (z uwzględnieniem komunikacji międzykulturowej), daje realną możliwość dalszego transferu i praktycznego wykorzystania w komunikacji międzykulturowej.

W szerszym wymiarze program uznano za ważny i potrzebny w kontekście dużej fali uchodźców z Ukrainy. Pozwala na uruchomienie czynników wyzwalających w zapobieganiu radykalizacji, a w przyszłości – polaryzacji wynikającej z odmienności kulturowych, konkurencji na rynku pracy, pamięci historycznej itp.

Wyniki badań ewaluacyjnych w obszarze przygotowywania treści zajęć wskazują, że można, a nawet należy podjąć aktywność w celu zredefiniowania wiedzy o pokoleniu Z i Alfa. Ważne jest korzystanie z najnowszych badań, które umożliwiają odczytanie rzeczywistości z perspektywy najmłodszych generacji, co z kolei może, ale nie musi pomóc w zmodyfikowaniu treści zajęć.

W wymiarze organizacyjnym poddano do przemyślenia zmniejszenie jednostek czasowych zajęć, zaprojektowanie zajęć stacjonarnych w mniejszych grupach oraz wcześniejsze ustalenie z dyrekcją szkoły powołania zespołu (pedagog, wychowawcy) zajmującego się organizacją i wsparciem zajęć realizowanych w ramach programu.

[32] Pełny opis programu, wraz z informacjami o jego autorce Marzenie Kordaczuk-Wąs, zespole realizującym i ewaluatorze Jadwidze Mazur zob. *Rozumiem=Szanuję*, Polska Platforma Bezpieczeństwa Wewnętrznego, https://ppbw.pl/pl/programprofilaktyczny [dostęp: 25.05.2023].

Moduły programu zostały zrealizowane w całości, a pilotaż i jego ewaluacja pozwoliła na wypracowanie wniosków, które mogą być uwzględnione w kolejnych edycjach programu. Należy również w tym miejscu zaznaczyć, jak ważny jest program, który w swoich celach i treściach odpowiada wymogom aktualnych wydarzeń związanych z migracją i uchodźctwem. Dlatego dużą wagę powinno się również przywiązać do jego marketingu.

Podsumowanie

Podjęte cele programu i związane z nimi zamierzenia oraz przyjęte metody ich realizacji są adekwatne do wyzwań zdiagnozowanych w badaniu uczniów przeprowadzonym zarówno przez autorkę programu, jak i szkołę.

Metody zastosowane w programie są skuteczne, a osoby realizujące treści programu wykazały profesjonalizm, zaangażowanie i uważność w kontakcie z beneficjentami. Warunkami niezależnymi wewnętrznymi były wyzwania organizacyjne, które opisano w raporcie i wskazano we wnioskach i zaleceniach. Warunkami niezależnymi zewnętrznymi był okres pandemii i wymóg w prowadzenia zajęć online w większości modułów.

Relację pomiędzy nakładami (ludzkimi, administracyjnymi czasowymi, finansowymi i lokalowymi) a osiągniętymi efektami programu można uznać za dobrą. Wyzwania organizacyjne opisane we wnioskach i zaleceniach programu można wziąć pod uwagę przy jego kolejnych edycjach. Warto wspomnieć, że efekty planowane: wzrost wiedzy, umiejętności i kompetencji beneficjentów programu w zakresie zapobiegania radykalizacji wiodącej do dyskryminacji i mowy nienawiści można przełożyć w warstwie oddolnej na pozytywny odbiór migracji i uchodźctwa w lokalnej społeczności.

Pozytywne efekty przeprowadzonego programu wśród uczniów, nauczycieli, rodziców i lokalnej społeczności obejmują wzrost wiedzy, umiejętności i kompetencji w odczytywaniu wielokulturowości i w komunikacji międzykulturowej.

Realizacja programu profilaktycznego to duże wyzwanie, które dotyczy zarówno osadzenia go w wymagającej rzeczywistości, uwzględnienia perspektywy generacji Alfa oraz wyboru wiedzy niezbędnej do jego realizacji. W sytuacji zagrożeń hybrydowych zmienia się też treść przekazu, gdzie warto wskazać w wyzwaniach komunikacyjnych na mowę nienawiści, która może prowadzić do radykalizacji, a w efekcie do polaryzacji różnych środowisk. To także wyzwanie dla autorów programów, jak w kolejnych edycjach uzupełnić je o takie elementy jak umiejętność odczytania dezinformacji, działanie mechanizmów społecznych w sytuacji zagrożenia (np. panika moralna), czy wpływ zagrożeń hybrydowych na zachowania społeczne.

W trakcie omawianych badań ewaluacyjnych powstało również kilka nowych obszarów do objęcia programami profilaktycznymi. Dotyczą kwestii zgłaszanych przez uczniów biorących udział w programie, a przede wszystkim wskazywanej przez nich

potrzeby większej liczby spotkań z psychologiem, których tematami mogą być: radzenie sobie z emocjami, z sytuacjami uznanymi za trudne (potrzeba osobnej diagnozy psychologicznej i socjologicznej), postępowanie negocjacyjne w sytuacjach trudnych, potrzeba zrozumienia niektórych mechanizmów społecznych i psychologicznych. Tematem, który powracał, była też różnego rodzaju odmienność – nie tylko w wymiarze międzykulturowym dotyczącym migracji. Wiele odpowiedzi uczniów wskazywało także na poczucie osamotnienia lub samotności, co wymagałoby zarówno osobnych badań, jak i programu profilaktycznego.

Z diagnozy i badań ewaluacyjnych obok tematu wiodącego i realizacji celów z nim związanych wyłania się obraz pokolenia Alfa: delikatnego, kruchego, nieradzącego sobie z emocjami lub radzącego sobie z nimi w sposób nieakceptowalny. Naturalny proces adolescencji w okresie zachodzących szybko zmian wymaga wsparcia i pomocniczości zarówno profilaktycznej, jak i psychologicznej. Wskazuje to też na potrzebę badań nowej generacji, żeby móc sprostać wyzwaniom profilaktycznym. To wyzwanie dla profesjonalnych profilaktyków, szkoły, ale również dla rodziców.

Nadto programy profilaktyczne wpisują się w modelowanie bezpieczeństwa hybrydowego, które jest odpowiedzią na zagrożenia hybrydowe. To szczególnie ważne w odniesieniu do młodego pokolenia, które może być poddane procesom dezinformacji dotyczącym ważnych dla państwa obszarów funkcjonowania – i być również podatne na radykalizację, prowadzącą w efekcie również do nieufności wobec instytucji państwa.

Bibliografia

Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów, wyd. 4 uaktualnione, Ministerstwo Edukacji Narodowej, Warszawa 2020.

Bilewicz M., Marchlewska M., Soral W., Wiśniewski M., *Mowa nienawiści. Raport z badań sondażowych*, Fundacja im. Stefana Batorego, Warszawa 2014, https://www.researchgate.net/profile/Mikolaj-Winiewski/publication/317318302_Mowa_nienawisci_Raport_z_badan_sondazowych/links/5931ba72a6fdcc89e7a631bc/Mowa-nienawisci-Raport-z-badan-sondazowych.pdf [dostęp: 24.05.2023].

Cattler D., Assistant Secretary General for Intelligence and Security, *What is NATO doing to address hybrid threats*?, 21.044.2021, https://www.nato.int/cps/en/natohq/news_183004.htm [dostęp: 18.05.2023].

Ewaluacja. Poradnik dla pracowników administracji publicznej, red. S. Bienias, P. Strzęboszewski, E. Opałka, Ministerstwo Rozwoju Regionalnego, Warszawa 2012, https://www.ewaluacja.gov.pl/media/11102/Poradnik_ewaluacji.pdf [dostęp: 20.10.2023].

Gaś Z.B., *Profilaktyka w szkole*, WSiP, Warszawa 2006.

Gaś Z.B., *Profilaktyka w szkole*, [w:] *Profilaktyka w szkole. Poradnik dla nauczycieli*, red. B. Kamińska-Buśko, J. Szymańska, Centrum Metodyczne Pomocy Psychologiczno-Pedagogicznej, Warszawa 2005.

Gaś Z.B., *Szkolny program profilaktyki. Istota, konstruowanie, ewaluacja*, Ministerstwo Edukacji Narodowej i Sportu, Warszawa 2003.

Goban-Klas T., *Tabloidyzacja mediów a neopopulizm*, [w:] *Media – Populizm – Demokracja. Zapis konferencji z dnia 5 listopada 2011 roku*, Ośrodek Myśli Społecznej im. Ferdynanda Lassalle'a, Wrocław 2011, s. 13–25.

Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 125–139.

Hołyst B., *Kryminologia*, Wydawnictwo Naukowe PWN, Warszawa 1994.

Mazur J., *Ewaluacja programu „Rozumiem=Szanuję"*, niepublikowany raport, Gorzów Wielkopolski, 2022.

Metody i strategie profilaktyczne, 20.05.2010, Krajowe Biuro Do Spraw Przeciwdziałania Narkomanii, https://www.kbpn.gov.pl/portal?id=105808 [dostęp: 20.05.2023].

Michalski K., Jurgilewicz M., *Konflikty technologiczne. Nowa architektura zagrożeń w epoce wielkich wyzwań*, Difin, Warszawa 2022.

Nowak T., *Budowa odporności na obecne i przyszłe zagrożenia o charakterze hybrydowym. Rekomendacje dla Polski*, „Roczniki Nauk Społecznych" 2022, t. 14 (50), nr 4, s. 29–50, https://repozytorium.kul.pl/bitstream/20.500.12153/4217/1/Nowak_Tomasz_Budowa_odpornosci_na_obecne_i_przyszle_zagrozenia.pdf [dostęp: 18.05.2023].

Ostaszewski K., *Nowe definicje poziomów profilaktyki*, „Remedium" 2005, nr 7–8, s. 40–41.

Pazderska A., *Tolerancja zachowań związanych z szerzeniem nienawiści w internecie w grupie młodych dorosłych: analiza empiryczna*, „Polityka i Społeczeństwo" 2023, t. 21, nr 1, s. 215–229, https://journals.ur.edu.pl/polispol/article/view/4492/4041 [dostęp: 24.05.2023].

Resilience, civil preparedness and Article 3, NATO, https://www.nato.int/cps/en/natohq/topics_132722.htm [dostęp: 18.05.2023].

Rozumiem=Szanuję, Polska Platforma Bezpieczeństwa Wewnętrznego, https://ppbw.pl/pl/programprofilaktyczny [dostęp: 25.05.2023].

Szymański P., *NATO i Unia Europejska wobec zagrożeń hybrydowych*, Ośrodek Studiów Wschodnich, 24.04.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 18.05.2023].

Tackling online disinformation, European Commission, https://digital-strategy.ec.europa.eu/en/policies/online-disinformation [dostęp: 18.05.2023].

Volkoff V., *Przedmowa*, [w:] *Dezinformacja oręż wojny*, oprac. V. Volkoff, tłum. A. Arciuch, Wydawnictwo Delikon, Warszawa 1991.

What is hate speech?, UN, https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech [dostęp: 23.05.2023].

Wiśniewski M., Hansen K., Bilewicz M., Soral W., Świderska A., Bulska D., *Mowa nienawiści, mowa pogardy. Raport z badania przemocy werbalnej wobec grup mniejszościowych*, Fundacja im. Stefana Batorego, Warszawa 2017, https://www.researchgate.net/profile/Mikolaj-Winiewski/publication/317318364_Mowa_nienawisci_mowa_pogardy_Raport_z_badania_przemocy_werbalnej_wobec_grup_mniejszosciowych/links/5931b5dba6fdcc89e7a59de7/Mowa-nienawisci-mowa-pogardy-Raport-z-badania-przemocy-werbalnej-wobec-grup-mniejszosciowych.pdf [dostęp: 24.05.2023].

Wiśniewski T., *Profilaktyka pedagogiczna*, PWN, Warszawa 1989.

Woynarowska B., *Edukacja zdrowotna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Wyrębek H., *Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa*, Wydawnictwo Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2021.

Programy profilaktyczne na rzecz podnoszenia bezpieczeństwa hybrydowego
Streszczenie

Współczesne zagrożenia hybrydowe są wyzwaniem dla kreatorów bezpieczeństwa i wymagają nowych rozwiązań w celu ich zapobiegania. Jednym z takich rozwiązań jest tworzenie programów profilaktycznych zapobiegających radykalizacji i mowie nienawiści. Programy te powinny być oparte na naukowych podstawach, dobrze zaprojektowane i uwzględniające wiedzę z psychologii, socjologii, prawa i bezpieczeństwa. Programy kierowane do młodzieży powinny uwzględniać też wyzwania związane z adolescencją i być prowadzone przez specjalistów z najnowszą wiedzą, umiejętnościami i kompetencjami.
Celem prezentowanego badania ewaluacyjnego programu profilaktycznego było sprawdzenie skuteczności programu edukacyjnego „Rozumiem=Szanuję", zapobiegającego radykalizacji wiodącej do dyskryminacji i mowy nienawiści. Badanie pozwoliło stwierdzić, że założone cele programu zostały zrealizowane. W celu wszechstronnego ujęcia oceny skuteczności programu zostały przeprowadzone analizy źródeł zastanych i wywołanych oraz badania jakościowe (wywiady) i ilościowe (technika ankiety), dokonywane po realizacji poszczególnych modułów programu.

Słowa kluczowe: zagrożenia hybrydowe, bezpieczeństwo, profilaktyka, radykalizacja, mowa nienawiści

Prevention programs to improve hybrid security
Abstract

Contemporary hybrid threats are a challenge for security creators and require new solutions in their prevention. One of such solution is the construction of prevention programs to prevent radicalization and hate speech. These programs should be science-based, well-designed, and include knowledge of psychology, sociology, law, and security. Programs addressed to young people should also take into account the challenges of adolescence and should be run by specialists with up-to-date knowledge, skills and competences.
The aim of the presented evaluation study of the preventive program was to check the effectiveness of the educational program preventing radicalization leading to discrimination and hate speech „Rozumiem=Szanuję" (Polish for "I Understand = I Respect"). The study shows that the assumed goals of the program were achieved. In order to comprehensively evaluate the effectiveness of the program, analyzes of existing and induced sources were carried out as well as qualitative research (interviews) and quantitative research (survey technique), conducted after the implementation of individual program modules.

Keywords: hybrid threats, security, prevention, radicalization, hate speech

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-004
Data wpłynięcia: 23.05.2023
Data akceptacji: 25.09.2023

Michał Adam Leśniewski

dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-2411-8911

Menedżer bezpieczeństwa organizacji w otoczeniu kulturowo zmiennym. Studium teoretyczno-koncepcyjne

Wprowadzenie

Bezpieczeństwo to problem istotny dla każdego człowieka i każdej organizacji chcącej funkcjonować na rynku[1]. Pojęcie bezpieczeństwa przyjmuje różne formy: od ochrony obiektu poprzez kontrolę policji drogowej, bezpieczeństwo ekonomiczne klientów, po bezpieczeństwo państwa w szerokim tego słowa znaczeniu. Jedną z form bezpieczeństwa jest bezpieczeństwo organizacji, obejmujące kwestię menedżera bezpieczeństwa. Bezpieczna organizacja rozwija się lepiej niż organizacja działająca w warunkach podwyższonego ryzyka. „Bezpieczeństwo organizacji" można zdefiniować jako proces, stan względnie gwarantujący poczucie pewności niezakłóconego funkcjonowania organizacji w zmiennym otoczeniu[2]. Bezpieczeństwo to czynnik, element organizacji, który nie może funkcjonować bez udziału czynnika ludzkiego[3]. Menedżer jest osobą zarządzającą, która ma wpływ na kształtowanie bezpieczeństwa organizacji, z uwzględnieniem realiów danej kultury

[1] A. Chodyński, *Using ambidexterity in the ecological security management of organisations*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 49–59.

[2] M.A. Leśniewski, *The manager and the safety culture of the organisation: a conceptual model*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 103–104.

[3] B. Dash, M.F. Ansari, *An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy*, „International Research Journal of Engineering and Technology" 2022, vol. 9, nr 4, s. 1–6.

organizacyjnej. Kultura organizacyjna jest czynnikiem miękkim, umożliwiającym menedżerowi kształtowanie bezpieczeństwa organizacji (kultury bezpieczeństwa).

Niniejsze opracowanie powstało w oparciu o autorską analizę interpretacyjną literatury przedmiotu i ma charakter teoretyczno-koncepcyjny. Celem jest przedstawienie autorskiego kulturowego modelu menedżera bezpieczeństwa. Poruszany problem wpisuje się w obszar zainteresowań praktyki gospodarczej i nauk o zarządzaniu i jakości.

Otoczenie zmienne kulturowo

Każda organizacja – w szerokim tego słowa znaczeniu – działa w otoczeniu[4] zmiennym, któremu musi sprostać i dostosowywać się do zmian, czyli musi charakteryzować się elastycznością[5]. Jednym z elementów otoczenia zewnętrznego jest kultura narodowa danego państwa, będąca znaczącym elementem kształtowania kultury organizacyjnej. Można stwierdzić, że kultura narodowa ma wpływ na kształtowanie kultury organizacyjnej. Każdy pracownik wywodzi się nie tylko z kultury narodowej, ale także z kultury swojego środowiska (rodziny, znajomych itp.), co z kolei przekłada się na kulturę danej organizacji. Biorąc pod uwagę globalizację, kultura narodowa państwa charakteryzuje się dużą zmiennością, czego wyrazistym przykładem jest np. kultura narodowa państw UE, w tym Polski, Francji czy Niemiec. Państwa uczestniczące w procesie globalizacji są bardziej podatne na zmiany kultury narodowej niż państwa w ograniczony sposób uwikłane w globalizację, np. Korea Północna.

Kultura narodowa przenika do kultury poszczególnych organizacji[6]. To, co stanowi wartość w kulturze narodowej, wpływa na wartość kultury organizacyjnej. Występuje tutaj swoista zależność. Każda organizacja w procesie globalizacji musi zdawać

---

[4] Pojęcie „otoczenie" jest w literaturze przedmiotu stosowane zamiennie z pojęciem „środowisko" (z zachowaniem podziału na środowisko wewnętrzne i zewnętrzne organizacji). Zob. E. Mączyńska, E. Okoń-Horodyńska, *Przedsiębiorstwo i jego otoczenie w obliczu czwartej rewolucji przemysłowej – wyzwania, szanse i zagrożenia*, „Przegląd Organizacji" 2020, nr 1, s. 9–21; A. Kowalczuk, *Otoczenie przedsiębiorstwa jako determinanta konkurencyjności*, „Przedsiębiorstwo i Region" 2015, nr 7, s. 38–52.

[5] Pojęcie „elastyczność" w pierwszym ujęciu oznacza stopień wrażliwości organizacji na zmiany zachodzące w otoczeniu. Im szybciej organizacja reaguje na zmiany zachodzące w otoczeniu, tym bardziej staje się elastyczna i na odwrót. Elastyczność w drugim ujęciu oznacza brak wyraźnych, wyodrębnionych granic między czynnikami konkurencyjności organizacji – to ujęcie elastyczności jest powszechnie stosowane w konkurencyjności miękkiej czy zarządzaniu miękkim. Zob. J. Grześ-Bukłaho, *Elastyczność jako atrybut współczesnej organizacji*, Politechnika Białostocka, Białystok 2022; M. Andrałojć, M. Ławrynowicz, *Elastyczny system wynagrodzenia w motywowaniu pokolenia Y*, „Zarządzanie Zasobami Ludzkimi" 2012, nr 5(88), s. 49–62.

[6] M.A. Leśniewski, *Konkurencyjność kulturowa przedsiębiorstw. Studium teoretyczno-empiryczne*, Uniwersytet Jana Kochanowskiego w Kielcach, Kielce 2020; Ł. Sułkowski, *Kulturowe procesy zarządzania*, Difin, Warszawa 2012.

sobie sprawę z dużej zmienności swojej kultury organizacyjnej. Zmienność otoczenia zewnętrznego to zmienność samej organizacji. Kultura organizacyjna zmienia się nie tylko poprzez napływ nowych pracowników, ale także poprzez zmianę wyznawanych wartości czy stylu życia pracowników danej organizacji. Część pracowników będzie bardziej cenić sobie czas wolny niż wysokość wynagrodzenia lub na odwrót itp. Zmiana (w tym zmiana kulturowa) i elastyczność to podstawowe cechy organizacji chcącej osiągnąć i utrzymać przewagę konkurencyjną na rynku.

Elastyczność zatrudnienia pracowników a elastyczność kultury organizacyjnej

Jednym z istotnych czynników wpływających na sukces organizacji (przedsiębiorstw) jest elastyczność[7], czyli zdolność do szybkiego reagowania na zmiany zachodzące w otoczeniu[8]. Elastyczność może przejawiać się w różnych formach, np. w zatrudnieniu i utrzymaniu pracowników w organizacji, w formie pracy zdalnej, w czasie pracy czy w formie motywowania pracowników. Elastyczność (w znaczeniu stosowanym w naukach o zarządzaniu i jakości) jest cechą podejmowanych działań i struktur budowanych dla ich realizacji. Elastyczność systemu organizacyjnego wyraża się więc w jego zdolności do inicjowania i dokonywania zmian celem dostosowania do nowej sytuacji, w której będzie realizowana strategia organizacji. Termin „elastyczność" jest często używany do opisu pojęć o innym znaczeniu, więc jego istota nie zawsze jest jasna[9].

Jedną z form elastyczności organizacji, która jest bezpośrednio związana z kulturą organizacyjną, są pracownicy. John Atkinson zaproponował model elastycznej organizacji, który pokazuje, jak organizacje mogą kierować systemem zatrudnienia w odniesieniu do różnych grup siły roboczej, aby zminimalizować koszty i stać się bardziej wrażliwymi na zmiany w otoczeniu rynkowym. W procesie kadrowym chodzi nie tylko o pozyskanie, ale również o utrzymanie pracownika w organizacji, dlatego reorganizacja systemów zatrudnieniowych ma iść w kierunku osiągnięcia kombinacji elastyczności organizacji[10]. Atkinson proponuje stosowanie różnych systemów zatrudnienia dla dwóch odmiennych segmentów, tj.: „rdzenia" i „części peryferyjnej". „Rdzeń" to pracownicy o wszechstronnych kompetencjach szkoleni w zakresie specyficznych umiejętności przydatnych organizacji, a „cześć peryferyjna" dotyczy

---

7 J. Grześ-Bukłaho, *op. cit*.

8 A. Hilarowicz, *Niestandardowe formy zatrudnienia jako wyraz zmian w funkcjonowaniu przedsiębiorstw*, [w:] *Metody i obszary zarządzania*, red. A. Potocki, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2007, s. 22.

9 P. Soffer, *On the notion of flexibility in business processes*, „Proceedings of the CAiSE" 2005, vol. 5, s. 1–7.

10 A. Hilarowicz, *op. cit.*, s. 23.

pracowników, których kompetencje są bardziej uniwersalne (to najczęściej pracownicy wykonawczy)[11].

Model zaprezentowany przez Atkinsona dzieli kulturę organizacyjną na „kulturę organizacyjną pracowników rdzenia" oraz „kulturę organizacyjną pracowników części peryferyjnej". Do każdego obszaru elastyczności organizacji można podejść pod kątem kultury organizacyjnej, gdyż jest to zasób wszechobecny w organizacji. Koncepcja elastyczności kultury organizacyjnej ma stanowić filozofię funkcjonowania organizacji w zmiennym otoczeniu. Elastyczność kultury organizacyjnej i zmienność otoczenia mają ze sobą współgrać. Menedżerowie muszą charakteryzować się elastycznością, która umożliwi im szybsze dostosowanie się do zmian zachodzących w otoczeniu wewnętrznym i zewnętrznym. Wychodząc z założenia, że zasób pierwotny to zasoby ludzkie – i człowiek stanowi podstawę każdej organizacji – to elastyczny pracownik to elastyczna kultura organizacyjna. Ta dwustronna elastyczność będzie tworzyć elastyczną organizację.

Menedżer zarządzający organizacją

Każda organizacja, aby prawidłowo funkcjonować, musi mieć menedżera. Menedżer decyduje nie tylko o teraźniejszości, ale również o przyszłości organizacji (przedsiębiorstwa). Menedżerem staje się osoba, która odpowiada za realizację procesu zarządzania organizacją – może to być odpowiednio dyrektor, kierownik, mistrz czy brygadzista[12].

Skuteczny menedżer to osoba o wielu cechach i umiejętnościach (*multifeatured*), które ułatwiają mu pełnienie funkcji zarządczych (kierowniczych) i wpływanie na innych. Umiejętności te muszą być kształtowane w zależności od zmian sytuacji, w jakiej znajduje się organizacja i sam menedżer. Nie ograniczają się tylko do podejmowania decyzji, ale obejmują też umiejętności dotyczące bezpieczeństwa – w obecnych czasach są bardzo ważne. Zmienność otoczenia generuje profil menedżera jako menedżera zmiennego, otwartego, permanentnie (ciągle) nastawionego na zmiany[13].

Menedżer organizacji to menedżer kultury organizacyjnej, która przyczynia się do kształtowania szeroko pojętego bezpieczeństwa organizacji[14]. Można stwierdzić, że kultura bezpieczeństwa jako „subkultura" stanowi składową kultury organizacyjnej, czyli kultury wiodącej.

---

11 *Ibidem*, s. 24.

12 U. Ornarowicz, *Menedżer XXI wieku. Definicja, identyfikacja, edukacja*, Szkoła Główna Handlowa – Oficyna Wydawnicza, Warszawa 2008, s. 18.

13 A. Gurba, J. Kowal, Z. Knecht, *Menedżer w procesie zarządzania zmianą we współczesnym przedsiębiorstwie*, „Gospodarka, Rynek, Edukacja" 2016, t. 17, nr 2, p. 14.

14 M. Choi, *Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing*, „Sustainability" 2016, vol. 8, nr 7, 638.

Kultura bezpieczeństwa organizacji

Zmiany zachodzące w otoczeniu zewnętrznym przyczyniają się do tego, że organizacje nieustannie poszukują nowych metod osiągnięcia przewagi konkurencyjnej[15]. Istotną rolę odgrywa tu oryginalność organizacji i jej pracowników czy sposób percepcji potencjalnych klientów przez dany podmiot gospodarczy. Bardzo ważna jest percepcja odmienności i podobieństw między danym podmiotem gospodarczym a przedsiębiorstwami konkurencyjnymi.

Kultura organizacyjna to szczególny byt społeczny, element (czynnik), zasób, który rozwija organizację i podlega ciągłym zmianom[16]. Menedżerowie względnie często nie podejmują decyzji o modyfikacji kultury organizacyjnej, lecz czerpią z niej wzorce, symbole, wartości czy sposoby komunikowania się. Otoczenie zewnętrzne ma charakter aktywny, zmiany w organizacji, modyfikacje kultury organizacyjnej są procesami trudnymi, ale możliwymi do realizacji[17]. Zmiany kultury organizacyjnej winny zachodzić z konieczności zmian otoczenia egzogenicznego i endogenicznego. Zmiana kultury organizacyjnej przyczynia się do zmiany kultury bezpieczeństwa[18].

Zaistnienie kultury bezpieczeństwa w dyskusjach, publikacjach czy badaniach naukowo-praktycznych jest charakterystyczne dla nauk o zarządzaniu i jakości, gdzie wiele problemów ma swoje uwarunkowania w praktyce gospodarczej. Doświadczanie kultury bezpieczeństwa wymagało jej uwzględnienia w prowadzonych badaniach teoretyczno-empirycznych, ze szczególnym uwypukleniem kultury organizacyjnej[19].

Kultura bezpieczeństwa może być weryfikowana w trzech głównych wymiarach[20]:

1) wymiar mentalny – to normy, wartości, idee i itp.,
2) wymiar społeczny i racjonalny – to interakcje społeczno-kulturowe, prawno-organizacyjne czy innowacyjno-wdrożeniowe,
3) wymiar materialny – to rzeczowe cechy istnienia i funkcjonowania człowieka.

Ukształtowanie i utrwalenie kultury bezpieczeństwa[21] wymaga holistycznego podejścia do trychotomii jej wymiarów. Przewaga podejścia specjalistycznego, które

---

[15] I.S.N. Arzahan, Z. Ismail, S.M. Yasin, *Safety culture, safety climate, and safety performance in healthcare facilities: a systematic review*, „Safety Science" 2022, nr 147, 105624.

[16] M. Drzewiecka, A. Stasiuk, *Charakterystyka kultury organizacyjnej przedsiębiorstwa produkcyjnego*, „Edukacja Ekonomistów i Menedżerów" 2012, t. 26, nr 4, s. 123–139.

[17] K. Skurjat, *Kultura bezpieczeństwa pracy w organizacji*, „Logistyka" 2014, nr 5, s. 1368–1374.

[18] M.A. Leśniewski, *Decyzyjność i decyzja a bezpieczeństwo pracy menedżera w organizacji – studium teoretyczne problemu badawczego*, „Bezpieczeństwo. Teoria i Praktyka" 2021, nr 4, s. 155–168.

[19] C.B. Frazier *et al.*, *A hierarchical factor analysis of a safety culture survey*, „Journal of Safety Research" 2013, nr 45, s. 15–28.

[20] A. Kłoskowska, *Socjologia kultury*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 103; A.L. Kroeber, *Istota kultury*, tłum. P. Sztompka, PWN, Warszawa 2002, s. 195.

[21] J. Czaja, *Kulturowy wymiar bezpieczeństwa. Aspekty teoretyczne i praktyczne*, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2013.

pomija konieczność powrotu do syntezy lub porównawczego ujmowania wyników badań naukowych, może skutkować brakiem poznania kultury bezpieczeństwa i spadkiem jej poziomu[22]. Jednostką monitorującą jest menedżer kultury bezpieczeństwa, który swoje działania powinien opierać na modelach adekwatnych do zaistniałej sytuacji w danej organizacji i w jej otoczeniu zewnętrznym.

Menedżer bezpieczeństwa organizacji w środowisku kulturowo zmiennym

Problem bezpieczeństwa jest obecny w każdej organizacji, niezależnie od jej wielkości. Menedżer jest odpowiedzialny nie tylko za realizację misji i wizji przedsiębiorstwa czy zachowanie norm i wartości, ale także za kształtowanie kultury bezpieczeństwa organizacji pracy. Pracownicy organizacji mają czuć się bezpiecznie podczas wykonywania swojej pracy. Zapewnienie przez menedżera bezpiecznych warunków pracy stanowi o trwałości i spójności organizacji.

Menedżer bezpieczeństwa (menedżer kultury bezpieczeństwa) to osoba odpowiedzialna za proces zarządzania w kierunku kształtowania kultury organizacyjnej tworzącej warunki, w których organizacja będzie realizować swoje cele mimo zagrożenia zewnętrznego[23]. Menedżer bezpieczeństwa (menedżer kultury bezpieczeństwa) w koncepcji Michała A. Leśniewskiego ma podłoże kulturowe, czyli kultury osobistej menedżera (kultura pozaorganizacyjna) oraz kultury miejsca pracy menedżera (kultura organizacyjna).

Menedżer bezpieczeństwa jest odpowiedzialny za warunki pracy w organizacji (przedsiębiorstwie), prowadzi permanentną kontrolę stanowisk pracy oraz utrzymuje stan aktywności poszczególnych maszyn i urządzeń[24]. Najważniejszym aspektem menedżera bezpieczeństwa jest jego wiedza, umiejętności, postawy, przekonania oraz intuicja w obszarze bezpieczeństwa. Zasady bezpieczeństwa i otwarta komunikacja to komponenty kultury bezpieczeństwa organizacji[25]. Otwarta komunikacja opiera się na porozumiewaniu się z innymi pracownikami organizacji, uczeniu, słuchaniu, mówieniu, dochodzeniu do kompromisu czy konsensusu. Komunikacja powinna być permanentna wśród pracowników wszystkich szczebli zarządzania. W przypadku bezpieczeństwa i higieny pracy komunikacja winna obejmować rzetelne i systematyczne

---

[22] M. Cieślarczyk, *Fenomen bezpieczeństwa i zjawisko kryzysów postrzegane w perspektywie kulturowej*, [w:] *Jedność i różnorodność. Kultura vs. kultury*, red. E. Rekłajtis, R. Wiśniewski, J. Zdanowski, Wydawnictwo ASPRA-JR, Warszawa 2010, s. 96.

[23] M.A. Leśniewski, *The manager and the safety culture…*, *op. cit.*, s. 103–112.

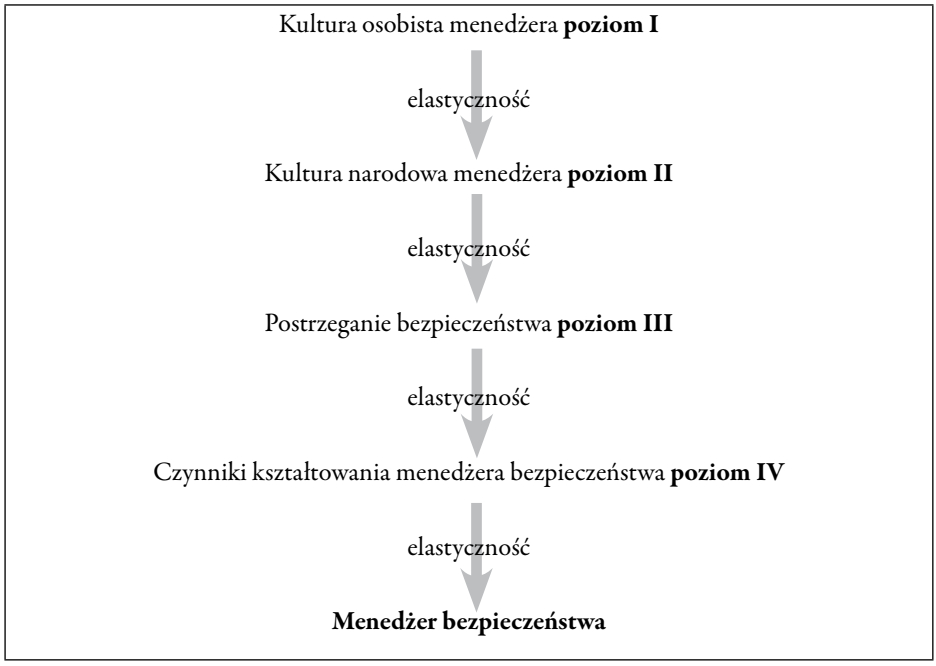
[24] M. Chan, I. Woon, A. Kankanhalli, *Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior*, „Journal of Information Privacy and Security" 2005, vol. 1, nr 3, s. 18–41.

[25] L. Kozioł, *Koncepcja systemu oceny kultury bezpieczeństwa pracy w przedsiębiorstwie*, „Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie" 2021, t. 52, nr 4, s. 67–80.

informowanie o występujących zagrożeniach, środkach ochrony technicznej, a także o pożądanych zachowaniach, które umożliwią zmniejszenie potencjalnego ryzyka[26].

Menedżer bezpieczeństwa, aby mógł skutecznie zabezpieczać organizację przed zagrożeniami z otoczenia zewnętrznego, powinien mieć wypracowany model kultury bezpieczeństwa i umieć go wdrożyć w danym podmiocie gospodarczym. W opracowanie takiego modelu powinni być zaangażowani menedżerowie wszystkich szczebli zarządzania wraz z podwładnymi. Rysunek 1 przedstawia kulturowy model menedżera bezpieczeństwa.

Rysunek 1. Kulturowy model menedżera bezpieczeństwa



Źródło: opracowanie własne na podstawie: M.A. Leśniewski, *The manager and the safety culture of the organisation: a conceptual model*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 108; idem, *Konkurencyjność miękka przedsiębiorstw*, Difin, Warszawa 2015; idem, *Konkurencyjność kulturowa przedsiębiorstw. Studium teoretyczno-empiryczne*, Uniwersytet Jana Kochanowskiego w Kielcach, Kielce 2020.

Powyższy model można określić jako model poziomowy – oznacza to, że zachodzi hierarchiczna zależność między poziomami, czyli kolejność poziomów ma znaczenie. Punktem wyjścia kulturowego modelu menedżera bezpieczeństwa zaprezentowanego na rysunku 1 jest kultura osobista menedżera (poziom I). Kultura osobista menedżera stanowi o jego możliwościach funkcjonowania w organizacji. Rodzina, grupa odniesienia menedżera będzie stanowić o podejściu do problemu bezpieczeństwa. Kultura

[26] K. Lis, *Kultura i klimat bezpieczeństwa pracy*, „Studia Oeconomica Posnaniensia" 2013, t. 1, nr 7, s. 7–16.

narodowa (poziom II) tworzy zestawy norm i wartości reprezentowanych przez dany naród i tym samym wpływa na kształtowanie zachowań menedżera bezpieczeństwa. Kultura osobista i kultura narodowa tworzą postrzeganie (percepcję) bezpieczeństwa (poziom III) przez menedżera organizacji. Postrzeganie bezpieczeństwa przyczynia się do jego kształtowania w ramach danej organizacji. Czynniki kształtowania menedżera bezpieczeństwa (poziom IV) to zestaw różnych elementów związanych z bezpieczeństwem organizacji, do których można zaliczyć: relacje międzyludzkie, behawioralność (zachowanie) pracowników (czyli ich reakcje na zmiany zachodzące w organizacji, codzienne rozmowy z innymi pracownikami czy wspólne wyjazdy integracyjne itp.), przepisy i zasady BHP czy konformizm i nonkonformizm pracowników organizacji. Przejście z poziomu I na poziom II i kolejno III i IV wsparte jest czynnikiem elastyczności, który w zmiennym otoczeniu jest niezbędny dla funkcjonowania organizacji. Uwzględnienie w powyższym modelu czynnika elastyczności stwarza silne podstawy do stwierdzenia, że bezpieczeństwo to elastyczne zachowanie między okresami spokoju i zagrożenia (konfliktów). Uwzględnienie w bezpieczeństwie czynnika elastyczności[27] wpisuje wówczas bezpieczeństwo w kategorię zarządzania miękkiego (jako bezpieczeństwo miękkie[28]).

Przedstawiony model jest otwarty na nowe czynniki i możliwy do stosowania w każdej organizacji (z dokonaniem określonej modyfikacji). Podłoże kulturowe menedżera bezpieczeństwa wpisuje ten model w problem zarządzania miękkiego i konkurencyjności miękkiej. Bezpieczeństwem i kulturą organizacyjną można zarządzać (zarządzanie miękkie) oraz można konkurować na rynku (konkurencyjność miękka).

Podsumowanie

Problem bezpieczeństwa ma charakter interdyscyplinarny – przejawia się w różnych formach i nierozerwalnie dotyczy człowieka i organizacji. W przypadku człowieka pojawia się każdego dnia w postaci bezpiecznego dojazdu do pracy, bezpiecznego użytkowania komputerów czy innych urządzeń multimedialnych, bezpiecznego lotu samolotem itp. W przypadku organizacji – w postaci przestrzegania przepisów i zasad BHP, bezpiecznej obsługi wózka widłowego w magazynie czy bezpiecznego picia kawy podczas lunchu firmowego.

Ważną rolę w formowaniu bezpieczeństwa odgrywają menedżerowie, którzy wraz z podwładnymi stanowią podstawę bezpieczeństwa organizacji. Bezpieczeństwo w organizacji może być wdrażane poprzez kulturę organizacyjną zwaną kulturą

[27] Elastyczność jest czynnikiem miękkim stanowiącym składową zarządzania miękkiego.

[28] Analogicznie do bezpieczeństwa miękkiego istnieje bezpieczeństwo twarde. Każdy z tych rodzajów bezpieczeństwa będzie przejawiać się w zależności od danej organizacji, np. bezpieczeństwo miękkie i bezpieczeństwo twarde państwa, bezpieczeństwo miękkie i bezpieczeństwo twarde szpitala czy szkoły itp.

bezpieczeństwa. To zadanie menedżera bezpieczeństwa, który wraz z organizacją funkcjonuje w otoczeniu zmiennym kulturowo. Ważnym czynnikiem kultury organizacyjnej (w tym kultury bezpieczeństwa) oraz menedżera bezpieczeństwa jest elastyczność – rozumiana jako szybkość, łatwość dokonywania w organizacji zmian wywołanych czynnikami otoczenia zewnętrznego. Elastyczność kultury organizacyjnej czy elastyczność menedżera bezpieczeństwa będzie stanowić o systemowym bezpieczeństwie organizacji.

Bibliografia

Andrałojć M., Ławrynowicz M., *Elastyczny system wynagrodzenia w motywowaniu pokolenia Y*, „Zarządzanie Zasobami Ludzkimi" 2012, nr 5(88), s. 49–62.

Arzahan I.S.N., Ismail Z., Yasin S.M., *Safety culture, safety climate, and safety performance in healthcare facilities: a systematic review*, „Safety Science" 2022, nr 147, 105624.

Cieślarczyk M., *Fenomen bezpieczeństwa i zjawisko kryzysów postrzegane w perspektywie kulturowej*, [w:] *Jedność i różnorodność. Kultura vs. kultury*, red. E. Rekłajtis, R. Wiśniewski, J. Zdanowski, Wydawnictwo ASPRA-JR, Warszawa 2010, s. 96–110.

Chan M., Woon I., Kankanhalli A., *Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior*, „Journal of Information Privacy and Security" 2005, vol. 1, nr 3, s. 18–41.

Chodyński A., *Using ambidexterity in the ecological security management of organisations*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 49–59.

Choi M., *Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing*, „Sustainability" 2016, vol. 8, nr 7, 638.

Czaja J., *Kulturowy wymiar bezpieczeństwa. Aspekty teoretyczne i praktyczne*, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2013.

Dash B., Ansari M.F., *An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy*, „International Research Journal of Engineering and Technology" 2022, vol. 9, nr 4, s. 1–6.

Drzewiecka M., Stasiuk A., *Charakterystyka kultury organizacyjnej przedsiębiorstwa produkcyjnego*, „Edukacja Ekonomistów i Menedżerów" 2012, t. 26, nr 4, s. 123–139.

Frazier C.B., Ludwig T.D., Whitaker B., Roberts D.S., *A hierarchical factor analysis of a safety culture survey*, „Journal of Safety Research" 2013, nr 45, s. 15–28.

Gurba A., Kowal J., Knecht Z., *Menedżer w procesie zarządzania zmianą we współczesnym przedsiębiorstwie*, „Gospodarka, Rynek, Edukacja" 2016, t. 17, nr 2, s. 11–18.

Grześ-Bukłaho J., *Elastyczność jako atrybut współczesnej organizacji*, Politechnika Białostocka, Białystok 2022.

Hilarowicz A., *Niestandardowe formy zatrudnienia jako wyraz zmian w funkcjonowaniu przedsiębiorstw*, [w:] *Metody i obszary zarządzania*, red. A. Potocki, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2007, s. 17–28.

Kłoskowska A., *Socjologia kultury*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Kowalczuk A., *Otoczenie przedsiębiorstwa jako determinanta konkurencyjności*, „Przedsiębiorstwo i Region" 2015, nr 7, s. 38–52.

Kozioł L., *Koncepcja systemu oceny kultury bezpieczeństwa pracy w przedsiębiorstwie*, „Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie" 2021, t. 52, nr 4, s. 67–80.

Kroeber A.L., *Istota kultury*, tłum. P. Sztompka, PWN, Warszawa 2002.
Leśniewski M.A, *Decyzyjność i decyzja a bezpieczeństwo pracy menedżera w organizacji – studium teoretyczne problemu badawczego*, „Bezpieczeństwo. Teoria i Praktyka" 2021, nr 4, s. 155–168.
Leśniewski M.A., *Konkurencyjność kulturowa przedsiębiorstw. Studium teoretyczno-empiryczne*, Uniwersytet Jana Kochanowskiego w Kielcach, Kielce 2020.
Leśniewski M. A., *Konkurencyjność miękka przedsiębiorstw*, Difin, Warszawa 2015.
Leśniewski M.A., *The manager and the safety culture of the organisation: a conceptual model*, „Bezpieczeństwo. Teoria i Praktyka" 2022, nr 2, s. 103–112.
Lis K., *Kultura i klimat bezpieczeństwa pracy*, „Studia Oeconomica Posnaniensia" 2013, t. 1, nr 7, s. 7–16.
Mączyńska E., Okoń-Horodyńska E., *Przedsiębiorstwo i jego otoczenie w obliczu czwartej rewolucji przemysłowej – wyzwania, szanse i zagrożenia*, „Przegląd Organizacji" 2020, nr 1, s. 9–21.
Ornarowicz U., *Menedżer XXI wieku. Definicja, identyfikacja, edukacja*, Szkoła Główna Handlowa – Oficyna Wydawnicza, Warszawa 2008.
Soffer P., *On the notion of flexibility in business processes*, „Proceedings of the CAiSE" 2005, vol. 5, s. 1–7.
Skurjat K., *Kultura bezpieczeństwa pracy w organizacji*, „Logistyka" 2014, nr 5, s. 1368–1374.
Sułkowski Ł., *Kulturowe procesy zarządzania*, Difin, Warszawa 2012.

Menedżer bezpieczeństwa organizacji w otoczeniu kulturowo zmiennym. Studium teoretyczno-koncepcyjne
Streszczenie

Zmienność otoczenia zewnętrznego wpływa na zamiany zachodzące w otoczeniu wewnętrznym organizacji (przedsiębiorstwa). Jednym w czynników, które muszą być brane pod uwagę w rozwoju organizacji, jest bezpieczeństwo. Zapewnienie bezpieczeństwa organizacji wymaga posiadania menedżera bezpieczeństwa, który będzie realizował proces permanentnego stabilnego funkcjonowania organizacji w zmiennym otoczeniu. Należy pamiętać, że bezpieczeństwo można rozpatrywać w różnych punktów widzenia, nie tylko jako stan wojny lub pokoju w danym państwie, ale także stan zagrożenia ze strony konkurentów itp. Celem opracowania jest przedstawienie kulturowego modelu menedżera bezpieczeństwa wraz z czynnikiem elastyczności. Model jest wynikiem badań teoretyczno-koncepcyjnych autora niniejszego opracowania, które wzbogaca dyscyplinę nauk o zarządzaniu i jakości.

Słowa kluczowe: menedżer bezpieczeństwa, otoczenie kulturowo zmienne, elastyczność, studium teoretyczno-koncepcyjne

Organization security manager in a culturally changing environment: a theoretical and conceptual study
Abstract

The variability of the external environment affects the changes taking place in the internal environment of the organization (enterprise). One of the factors that must be taken into account in the development of an organization is security. Ensuring the security of the organization requires having a security manager who will implement the process of a permanent stable functioning of the organization in a changing environment. It

should be remembered that security can be considered from various points of view, not only as a state of war or peace in a given country, but also as a state of threat from competitors, etc. The aim of the study is to present a cultural model of a security manager with a factor of flexibility. The model is the result of theoretical and conceptual research by the author of this study, which enriches the discipline of management and quality sciences.

Keywords: security manager, culturally variable environment, flexibility, theoretical and conceptual study

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-005
Data wpłynięcia: 18.05.2023
Data akceptacji: 26.09.2023

Piotr Komsta

dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0002-0162-5518

Uwarunkowania realizacji wdrożeń systemów informatycznych a bezpieczeństwo projektu

Wprowadzenie

Realizacja wdrożeń systemów informatycznych jest przedsięwzięciem złożonym i ryzykownym. Wiele projektów nie kończy się w założonym czasie i budżecie, a źle prowadzony projekt może skutkować brakiem osiągnięcia zamierzonych celów[1]. Rozpoznanie uwarunkowań, w których zamierzamy realizować projekt informatyczny, z jednej strony pozwala na rzetelne oszacowanie ryzyka podejmowanego przedsięwzięcia, a z drugiej – umożliwia podjęcie odpowiednich decyzji odnośnie do kształtu projektu. Szacowanie ryzyka projektu informatycznego jest bardzo istotnym elementem mogącym mieć wpływ na sprawność realizacji przedsięwzięć informatycznych[2]. Celem artykułu jest wskazanie istotnych uwarunkowań realizacji przedsięwzięć informatycznych, które powinny być brane pod uwagę przy szacowaniu ryzyka związanego z realizacją projektu. Artykuł składa się z czterech rozdziałów, w których Autor zwraca uwagę na tak istotne elementy jak: referencyjność rozwiązań informa-

[1] *Review Standish Group – CHAOS 2020: Beyond Infinity*, Henny Portman's Blog, 6.01.2021, https://hennyportman.wordpress.com/2021/01/06/review-standish-group-chaos-2020-beyond-infinity [dostęp: 12.05.2023]; A. Mersino, *Why Agile is Better than Waterfall (Based on Standish Group Chaos Report 2020)*, 25.05.2020, Medium.com, https://medium.com/leadership-and-agility/agile-project-success-rates-are-2x-higher-than-traditional-projects-376a05e590d4 [dostęp: 12.05.2023].

[2] D. Pimchangthong, V. Boonjing, *Effects of Risk Management Practices on IT Project Success*, „Management and Production Engineering Review" 2017, vol. 8, nr 1, s. 30.

tycznych, stabilność otoczenia implementacyjnego, motywacja i odpowiedzialność w projekcie oraz narzędzia zarządzania zmianą. Artykuł został napisany w oparciu o studium literatury przedmiotu oraz doświadczenie praktyczne Autora.

Referencyjność rozwiązań informatycznych

Wybór rozwiązania informatycznego, jak również firmy wdrożeniowej jest kluczowym elementem mającym bezpośredni wpływ na sprawność realizacji projektu informatycznego, zdolność osiągania celów projektu, a co za tym idzie – i jego bezpieczeństwo. Jednym z kluczowych kryteriów wyboru systemów informatycznych powinna być analiza zdolności oferowanego systemu do odwzorowania procesów zachodzących w firmie oraz poprawy ich sprawności. Rozwiązania referencyjne znacznie ułatwiają ocenę systemu w przedmiotowym zakresie, pozwalają unikać błędów w określeniu docelowego kształtu systemu, jak również pozwalają na zwiększenie wartości dodanej projektu. Jedną z przyczyn problemów ze sprawną realizacją projektów wdrożeń systemów informatycznych wspomagających zarządzanie są trudności w ustaleniu wspólnych stanowisk odnośnie do docelowego kształtu systemu pomiędzy firmą informatyczną a przedsiębiorstwem, w którym realizowany jest projekt[3].

Trudności takie często wynikają z braku posiadania przez firmę informatyczną rozwiązań referencyjnych. Referencyjność rozwiązań informatycznych jest również ważna z punktu widzenia budowy wartości firmy. Biorąc pod uwagę zmiany kapitałowe, przejęcia firm i fuzje, posiadanie rozwiązań referencyjnych znacznie ułatwia procesy integracyjne. W 2022 r. na rynku polskim zanotowano zwiększenie liczby transakcji (przejęć i fuzji) w porównaniu do roku 2021[4]. Na wybór rozwiązania informatycznego należy spojrzeć w szerszej perspektywie, uwzględniając nie tylko bieżące potrzeby firmy, ale również potrzeby, które pojawią się w dłuższej perspektywie czasowej, wynikające wprost z dynamiki rozwoju firmy. Firmy informatyczne, które mają duże doświadczenie w implementacji rozwiązań branżowych w firmach na różnym etapie ich rozwoju, zazwyczaj są w stanie oferować szeroki wachlarz dedykowanych rozwiązań dziedzinowych. Ma to istotne znaczenie z punktu widzenia procesów integracyjnych poszczególnych obszarów firmy, mających na celu zapewnienie swobodnego przepływu informacji. Duże doświadczenie firmy informatycznej w implementacji rozwiązań branżowych znacznie ułatwia i przyspiesza rozwiązywanie problemów

[3] 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. 82.

[4] *M&A Index Poland. Fuzje i przejęcia w 2022 roku*, Navigator Capital, FORDATA, styczeń 2023, https://fordata.pl/wp-content/uploads/2023/01/raport-mnaindexpoland-2022-pl.pdf [dostęp: 12.05.2023].

dotyczących kształtu funkcjonowania aplikacji i kierunków jej rozwoju, co ma istotny wpływ na ryzyka związane z realizacją projektu.

Nie da się całkowicie wyeliminować ryzyk związanych z realizacją projektów informatycznych, każdy projekt obarczony jest pewnym ryzykiem, jednak świadomość uwarunkowań związanych z jego realizacją i ich wpływu na przebieg projektu może skłaniać do refleksji na temat zasadności przystąpienia do jego realizacji i gotowości poniesienia ciężaru powyższego ryzyka. Należy tutaj brać pod uwagę nie tylko wątpliwości co do możliwości osiągnięcia założonych celów projektu, ale również wysokości kosztów, jakie ponosi firma przystępująca do realizacji ryzykownego projektu – będącego wynikiem niewłaściwego przygotowania pod względem strategicznym, merytorycznym czy koncepcyjnym.

Przystępując do realizacji projektów wdrożeń systemów informatycznych o charakterze procesowym, należy mieć świadomość konieczności dużych nakładów pracy zespołów wdrożeniowych po stronie firmy, w której wdrażany jest system, szczególnie w sytuacjach, kiedy uwarunkowania realizacyjne prac wskazują, że projekt może być bardzo ryzykowny. Biorąc pod uwagę fakt wysokiej pracochłonności i ograniczonej dostępności zasobów, podejmowanie decyzji odnośnie do przystąpienia do realizacji projektu obarczonego bardzo dużym ryzykiem może być dyskusyjne z punktu widzenia zagrożeń związanych z brakiem sprawności przy realizacji innych planowanych lub realizowanych projektów w firmie w tym samym czasie. Należy pamiętać, że pracownicy przedsiębiorstwa zaangażowani w realizację projektu informatycznego równolegle muszą realizować zadania wynikające z działalności operacyjnej firmy.

Brak rozwiązań referencyjnych, źle przygotowany projekt pod względem merytorycznym i koncepcyjnym zwiększa zaangażowanie zespołów wdrożeniowych i pracochłonność wdrożenia, co może mieć bezpośrednie przełożenie na termin realizacji projektu informatycznego, jak również jego budżet.

Jak już zostało wcześniej wspomniane, trudno jest całkowicie wyeliminować ryzyko z projektów informatycznych, niemniej jednak można to ryzyko znacznie ograniczyć, wybierając rozwiązania sprawdzone merytorycznie i koncepcyjnie, mocno osadzone w realiach dziedzinowych, w których projekt jest realizowany. Realizacja projektów obarczonych bardzo dużym ryzykiem może skutkować brakiem osiągnięcia celów projektów lub osiągnięciem celów nie do końca satysfakcjonujących, ponoszeniem nadmiernych (nieadekwatnych) kosztów związanych z projektem, a co za tym idzie – wydłużeniem czasu zwrotu z inwestycji. Wysoka pracochłonność przy ograniczonym dostępie do zasobów może mieć wpływ na zagrożenia przy realizacji innych projektów w firmie lub zagrożenia związane z brakiem osiągnięcia celów strategicznych czy operacyjnych firmy. Nieudane projekty informatyczne mogą nawet stanowić zagrożenie dla dalszego funkcjonowania firmy[5].

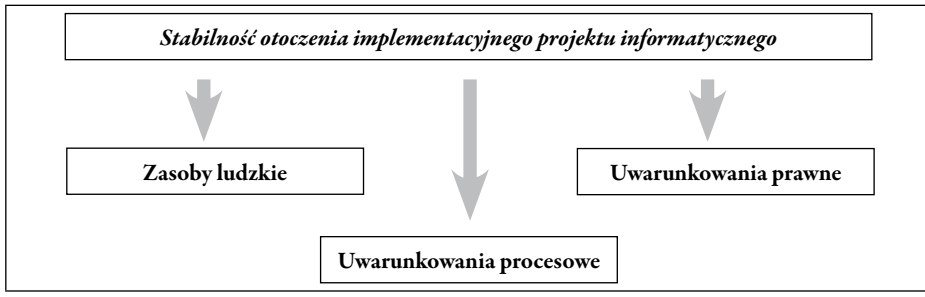
---

[5] M. Bloch, S. Blumberg, J. Laartz, *Delivering large-scale IT projects on time, on budget, and on value*, „McKinsey Quarterly" 2012, vol. 27, s. 2.

Stabilność otoczenia implementacyjnego

Na rysunku 1 zostały przedstawione elementy otoczenia implementacyjnego projektów informatycznych, które zdaniem Autora mają istotny wpływ na sprawność ich realizacji, tj. zasoby ludzkie, uwarunkowania procesowe oraz uwarunkowania prawne. W projektach wdrożeń systemów informatycznych biorą udział zarówno konsultanci firmy informatycznej, jak i pracownicy firmy, w której realizowany jest projekt. Dynamika i zmiany na rynku pracy niosą ze sobą ryzyka związane z destabilizacją zasobów ludzkich uczestniczących w realizowanym projekcie, co może negatywnie wpłynąć na sprawność realizowanych przedsięwzięć informatycznych. Jeśli problem zastępowalności zasobów ludzkich nie zostanie rozwiązany przed przystąpieniem do realizacji projektu, brak wystarczającej liczby wykwalifikowanych pracowników może stanowić poważny problem uniemożliwiający zakończenie projektu w zakładanym czasie.

Rysunek 1. Stabilność otoczenia implementacyjnego projektu informatycznego



Źródło: opracowanie własne.

Należy wziąć pod uwagę również to, że nowi pracownicy w projekcie (zarówno po stronie przedsiębiorstwa, jak i firmy informatycznej) potrzebują czasu, aby zapoznać się z zagadnieniami projektowymi, co może wpłynąć negatywnie na termin jego realizacji.

Innym istotnym zagadnieniem jest brak stabilizacji środowiska procesowego będącego przedmiotem implementacji systemu, jak również otoczenia prawnego, wymuszającego w niektórych przypadkach zmiany w realizacji procedur i procesów w systemie informatycznym. O ile zarządzanie zmianami o charakterze procesowym, które wynikają z przepisów wewnętrznych przedsiębiorstwa, jest łatwiejsze, o tyle zmiany wynikające wprost z niestabilności otoczenia prawnego funkcjonowania firmy i mające bezpośredni wpływ na sposób realizacji kluczowych procesów mogą stanowić poważne wyzwanie z punktu widzenia terminu realizacji projektu i jego budżetu. Przy określaniu skali projektu i szacowaniu czasu jego realizacji dobrą praktyką jest analiza ryzyka związanego z brakiem stabilności zasobów oraz zmienności środowiska procesowego czy zewnętrznych uwarunkowań prawnych funkcjonowania firmy mogących mieć wpływ na funkcjonalność systemu informatycznego.

Przedsięwzięcia informatyczne o dużej skali niosą większe ryzyko niepowodzeń niż przedsięwzięcia o mniejszej skali. W mniejszych projektach ze względu na krótki czas ich realizacji wpływ ryzyk związanych z destabilizacją środowiska implementacyjnego jest o wiele niższy. Umiejętność definiowania skali projektu w stopniu umożliwiającym precyzyjne planowanie ze względu na uwarunkowania środowiska implementacyjnego jest cechą bardzo pożądaną wśród kierowników projektów i decydentów. Przeskalowanie projektu informatycznego jest bardzo ryzykowne nie tylko ze względu na brak osiągnięcia zamierzonych celów projektu, ale również w kontekście dotrzymania terminów i zamknięcia projektu w złożonym budżecie.

Motywacja i odpowiedzialność w projekcie

Wdrożenie systemu informatycznego wspomagającego zarządzanie wiąże się z dużym zaangażowaniem pracowników przedsiębiorstwa. Jak już zostało wcześniej wspomniane, pracownicy poza pracą przy projekcie muszą wykonywać swoje codzienne obowiązki związane ze stanowiskiem w firmie. Brak adekwatnych narzędzi motywacyjnych może skutkować brakiem należytego zaangażowania pracowników przy realizacji projektu. Aspekt ten jest bardzo często pomijany i niedoceniany przy tworzeniu zespołów wdrożeniowych po stronie przedsiębiorstwa, w którym realizowany jest projekt informatyczny. Pracownicy obarczani są zazwyczaj dodatkowymi pracami w ramach swoich obowiązków zawodowych i nie otrzymują dodatkowego wynagrodzenia. Mówimy tutaj o niedoszacowaniu budżetu projektu informatycznego, o kosztach, które nie wynikają wprost z umowy projektowej.

Istotnym aspektem motywacyjnym jest również zauważalny brak należytego zaangażowania w projekt za strony kierownictwa firmy, co również może przełożyć się na brak należytej motywacji pracowników przedsiębiorstwa uczestniczących w projekcie. Przystępując do realizacji wdrożeń systemów informatycznych wspomagających zarządzanie, kadra menedżerska powinna być świadoma korzyści wynikających z implementacji oferowanych rozwiązań informatycznych w kontekście realizowanych celów strategicznych i operacyjnych firmy. Brak wyraźnego powiązania projektu informatycznego z celami firmy osłabia projekt pod względem motywacyjnym i podaje w wątpliwość zasadność jego realizacji.

Ważnym elementem negatywnie wpływającym na sprawność realizacji projektów informatycznych jest zła organizacja pracy po stronie firmy informatycznej. Podejście procesowe, które skupia odpowiedzialności poszczególnych zespołów dziedzinowo, nie jest w stanie sprostać współczesnym wymaganiom stawianym projektom informatycznym. Mówimy tutaj o sytuacji, w której każdy zespół odpowiedzialny jest za poszczególny obszar dziedzinowy projektu i nie poczuwa się do odpowiedzialności za jego całość. Sprawa komplikuje się, kiedy mamy do czynienia z nierzetelnym wykonywaniem swoich zadań czy popełnianiem błędów, np. na etapie tworzenia projektu systemu, i koniecznością dokonania zmian na późniejszych jego etapach. Podejście

procesowe w wielu przypadkach przy współczesnych projektach się nie sprawdza. Stopień skomplikowania projektów informatycznych i ich zmienność wymuszają nowe rozwiązania, które poprawiają sprawność ich realizacji.

Wiele firm świadomych współczesnych wyzwań stara się reorganizować swoje zespoły wdrożeniowe w kierunku podejścia DevOps. Podejście to wymusza na zespołach biorących w projekcie wzięcie odpowiedzialności za jego całość. Podejście takie wnosi wiele korzyści, do których można zaliczyć m.in: skupienie się pracowników na efekcie końcowym projektu, a nie jego wycinku, adekwatne dopasowanie narzędzi motywacyjnych uzależnionych od wyniku końcowego projektu, łatwiejsze zarządzanie zmianą w projekcie, łatwiejszy transfer wiedzy pomiędzy pracownikami, zwiększenie ich kompetencji i elastyczności[6].

Narzędzia zarządzania zmianą

Jedną z przyczyn problemów związanych z realizacją wdrożeń systemów informatycznych jest nieadekwatność metodyk implementacyjnych systemów informatycznych do skali projektu. Brak jasno zdefiniowanych narzędzi pozwalających na kontrolę projektu, słabo zdefiniowane ośrodki decyzyjne mogą mieć negatywny wpływ na jego jakość. Ośrodki decyzyjne powinny skupiać się nie tylko na aspektach dziedzinowych, ale brać również pod uwagę i stosować takie narzędzia jak priorytetyzacja w kontekście zarządzania zmianą w projekcie.

Zmiana w projekcie informatycznym jest nieodłącznym jego elementem i może wynikać z różnych przyczyn – np. zmiana koncepcji systemu wynikająca z wprowadzenia nowych przepisów prawnych mających wpływ na funkcjonowanie firmy, zmiana koncepcji funkcjonowania systemu wynikająca z procesów integracyjnych różnych aplikacji w obszarze przedsiębiorstwa i powiązań z aplikacjami zewnętrznymi. Zmiany mogą również wynikać z konieczności poprawy błędów, zmiany zakresu szczegółowości danych w raportach itp. Brak jasno sformułowanych narzędzi pozwalających na sprawne zarządzanie zmianą uniemożliwia budowanie jakości projektu. Jednym z narzędzi zarządzania zmianą jest priorytetyzacja.

Priorytetyzacja powinna się odbywać w kontekście oceny stopnia krytyczności zmiany z punktu widzenia realizacji procesu czy procedury będących przedmiotem implementacji. Często mamy do czynienia z nadmiarowością zgłaszanych zmian, które nie są poddawane ocenie z punktu widzenia ich krytyczności. Ocena krytyczności i dokonanie priorytetyzacji w zakresie wprowadzonych zmian jest właściwym narzędziem mającym wpływ na poprawę sprawności realizowanych projektów

[6] Szerzej zob. L. Banica, M. Radulescu, D. Rosca, A. Hagiu, *Is DevOps another Project Management Methodology?*, „Informatica Economică" 2017, vol. 21, nr 3, s. 39–51; R.T. Yarlagadda, *DevOps and Its Practices*, „International Journal of Creative Research Thoughts" 2021, vol. 9, nr 3, s. 111–119.

wdrożeń systemów informatycznych[7]. Problemy związane z zarządzaniem zmianą można często spotkać przy projektach informatycznych, w których nie zdefiniowano jednoznacznie zasad postępowania w przedmiotowym zakresie. Nadmiarowość zmian w projektach wdrożeń systemów informatycznych wspomagających zarządzanie jest często wynikiem złego przygotowana systemu do implementacji w poszczególnych obszarach dziedzinowych. System informatyczny źle przygotowany pod względem koncepcyjnym, merytorycznym wydłuża czas wypracowania właściwych rozwiązań pozwalających na sprawną realizację procesów biznesowych w firmie, co może mieć bezpośredni wpływ na termin zakończenia projektu i jego budżet. Zarządzanie zmianą jest przedsięwzięciem trudnym i powinno być realizowane zawsze w oparciu o kryteria jakości realizowanego projektu. Działania priorytetyzacyjne polegające na ocenie zmian pod kątem ich krytyczności z punktu widzenia realizowanego procesu biznesowego można przeprowadzić w oparciu o wiedzę dziedzinową – o wiele więcej problemów sprawia ocena kwalifikowalności budżetowej projektu. Dobrą praktyką jest uwzględnienie sposobu postępowania i sposobu wycen w przedmiotowym zakresie przed podpisaniem kontraktu.

Podsumowanie

Przedsiębiorstwa, przystępując do realizacji projektów wdrożeń systemów informatycznych wspomagających zarządzanie, powinny mieć świadomość uwarunkowań, w których przyjdzie im realizować projekt, i ryzyk z nich wynikających. Badanie tych uwarunkowań i szacowanie ryzyk w kontekście bezpieczeństwa projektu, jak również bezpieczeństwa funkcjonowania firmy przed przystąpieniem do projektu świadczy o właściwym przygotowaniu firmy, a co za tym idzie – jej dojrzałości do realizacji przedsięwzięć informatycznych.

Bibliografia

Banica L., Radulescu M., Rosca D., Hagiu A., *Is DevOps another Project Management Methodology?*, „Informatica Economică" 2017, vol. 21, nr 3, s. 39–51.

Bloch M., Blumberg S., Laartz J., *Delivering large-scale IT projects on time, on budget, and on value*, „McKinsey Quarterly" 2012, vol. 27, s. 2–9.

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. 79–84.

Komsta P., *Prioritizing areas of implementation within the dynamic modelling concept as regards implementation processes of integrated systems*, [w:] *Information management in the era of the*

[7] Szerzej zob. P. Komsta, *Prioritizing areas of implementation within the dynamic modelling concept as regards implementation processes of integrated systems*, [w:] *Information management in the era of the Internet. Selected Issues*, red. M. Pękala, M. Szepski, Towarzystwo Naukowe Societas Vistulana, Kraków 2020, s. 105–113.

Internet. Selected Issues, red. M. Pękala, M. Szepski, Towarzystwo Naukowe Societas Vistulana, Kraków 2020, s. 105–113.

M&A Index Poland. Fuzje i przejęcia w 2022 roku, Navigator Capital, FORDATA, styczeń 2023, https://fordata.pl/wp-content/uploads/2023/01/raport-mnaindexpoland-2022-pl.pdf [dostęp: 12.05.2023].

Mersino A., *Why Agile is Better than Waterfall (Based on Standish Group Chaos Report 2020)*, 25.05.2020, Medium.com, https://medium.com/leadership-and-agility/agile-project-success-rates-are-2x-higher-than-traditional-projects-376a05e590d4 [dostęp: 12.05.2023].

Pimchangthong D., Boonjing V., *Effects of Risk Management Practices on IT Project Success*, „Management and Production Engineering Review" 2017, vol. 8, nr 1, s. 30–37.

Review Standish Group – CHAOS 2020: Beyond Infinity, Henny Portman's Blog, 6.01.2021, https://hennyportman.wordpress.com/2021/01/06/review-standish-group-chaos-2020-beyond-infinity [dostęp: 12.05.2023].

Yarlagadda R.T., *DevOps and Its Practices*, „International Journal of Creative Research Thoughts" 2021, vol. 9, nr 3, s. 111–119.

Uwarunkowania realizacji wdrożeń systemów informatycznych a bezpieczeństwo projektu

Streszczenie

W artykule wskazano uwarunkowania realizacji przedsięwzięć informatycznych wspomagających zarządzanie, istotne z punktu widzenia bezpieczeństwa projektów. Zwrócono uwagę na tak ważne elementy jak: referencyjność oferowanych rozwiązań informatycznych, stabilność otoczenia implementacyjnego projektu, aspekty motywacyjne i odpowiedzialność w projekcie oraz narzędzia zarządzania zmianą. Autor wskazuje potrzebę przeprowadzenia analizy planowanych projektów informatycznych pod kątem ich uwarunkowań implementacyjnych w celu rzetelnego oszacowania ryzyk. Artykuł został napisany w oparciu o studium literatury przedmiotu oraz doświadczenie praktyczne Autora.

Słowa kluczowe: projekt informatyczny, bezpieczeństwo projektów informatycznych, system informatyczny wspomagający zarządzanie, wdrażanie systemów informatycznych

Implementation conditions of IT systems and project security

Abstract

The article indicates conditions for the implementation of IT projects supporting management, which are important from the point of view of project security. Attention was paid to such important elements as: the reference character of the offered IT solutions, the stability of the project's implementation environment, motivational aspects in the project and responsibility, as well as change management tools. The author indicates the need to analyze the planned IT projects in terms of their implementation conditions in order to reliably assess the risks. The article was written based on a study of the literature on the subject and the Author's practical experience in the subject area.

Key words: IT project, security of IT projects, IT management systems, implementation of IT systems

BEZPIECZEŃSTWO SECURITY
TEORIA I PRAKTYKA THEORY AND PRACTICE
e-ISSN 2451-0718 2023
ISSN 1899-6264 Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-006
Data wpłynięcia: 6.06.2023
Data akceptacji: 26.09.2023

Barbara Oliwkiewicz

dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0002-0752-2288

Godziwe wynagrodzenie jako element bezpieczeństwa społecznego młodych pracowników

Wprowadzenie

Bez względu na etap rozwoju cywilizacji i poziom osiągnięć technicznych ludziom zawsze potrzebne było poczucie bezpieczeństwa. W piramidzie potrzeb Maslowa bezpieczeństwo plasuje się nisko, czyli oprócz elementów niezbędnych do fizycznego przeżycia człowieka to właśnie bezpieczeństwo stanowi fundament, który zabezpiecza rozwój i umożliwia realizację kolejnych potrzeb wyższego rzędu[1]. Człowiek, by zaspokoić swoje potrzeby – niższego i wyższego rzędu – musi dysponować środkami pieniężnymi. W dzisiejszych czasach wiele się mówi o godziwym wynagrodzeniu, termin ten jest różnie interpretowany. Praca to podstawowe narzędzie, które dzięki płacy umożliwia realizację potrzeb życiowych człowieka, co kształtuje jego podstawowe bezpieczeństwo socjalne i społeczne. Wynagrodzenie za pracę powinno być ustalone adekwatnie do rodzaju wykonywanej pracy i kwalifikacji niezbędnych przy jej wykonaniu oraz powinno uwzględniać ilość i jakość świadczonej pracy. Pod pojęciem „wynagrodzenie" rozumieć należy wszystkie formy

[1] P. Goryń, *Bezpieczeństwo społeczne – jedno czy wiele?*, [w:] *Bezpieczeństwo i jego percepcja w dyskursie społecznym i militarnym*, red. D. Boćkowski, P. Goryń, K. Goryń, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2020, s. 48–49, https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/10699/1/P_Goryn_Bezpieczenstwo_spoleczne_jedno_czy_wiele.pdf [dostęp: 25.05.2023].

finansowych i niefinansowych korzyści otrzymywanych przez wynagradzanych w zamian za świadczenie stosunku pracy.

Celem niniejszego opracowania jest przedstawienie godziwego wynagrodzenia jako jednego z czynników kształtujących bezpieczeństwo społeczne młodego pracownika. Przedstawiono wyniki badań własnych dotyczących oczekiwań studentów studiów licencjackich co do wynagrodzenia, które daje im poczucie bezpieczeństwa, w kontekście teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń. W części teoretycznej artykułu przedstawiono pojęcie bezpieczeństwa społecznego, socjalnego i płacy minimalnej, następnie zaprezentowano model pomiaru kapitału ludzkiego oraz model płacy godziwej. Kolejna część opracowania prezentuje założenia, dane i wyniki empirycznych badań własnych przeprowadzonych wśród studentów jednej z krakowskich uczelni.

Pojęcie bezpieczeństwa i bezpieczeństwa społecznego

Etymologicznie słowo „bezpieczeństwo" pochodzi od zwrotu „bez pieczy" (łac. *sine cura*). Współcześnie wiele jest definicji i interpretacji tego pojęcia. Według Janusza Gierszewskiego „bezpieczeństwo postrzegane jest jako stan i proces, potrzeba oraz skomplikowany system wraz z licznym układem podsystemów, które mają na celu zapewnienie bezpieczeństwa rozwoju narodowi przy użyciu prawnie dostępnych środków (technicznych, organizacyjnych i prawnych)"[2]. Inna definicja przedstawia bezpieczeństwo jako „stan, który daje poczucie pewności i gwarancję jego zachowania oraz szanse na doskonalenie. Jedna z podstawowych potrzeb człowieka to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych"[3]. Potocznie mówi się o bezpieczeństwie globalnym, regionalnym, politycznym społecznym, psychicznym, socjalnym. Jednak kategorie te przenikają się między sobą i trudno wyznaczyć ich granice. Realnym źródłem wiedzy na temat poziomu bezpieczeństwa jest subiektywne odczucie podmiotu, który zostaje poddany badaniu. Należy pamiętać, że te subiektywne odczucia ulegają zmianie wraz z upływem czasu, są odmienne na różnych obszarach geograficznych i mogą się zmieniać ze względu na manipulację innych podmiotów.

Młody człowiek kończący studia marzy o tym, aby dostać pracę za odpowiednie wynagrodzenie. Bez godziwej płacy trudno przetrwać w dzisiejszym świecie, zatem pracownicy wchodzący na rynek pracy myślą przede wszystkim o wynagrodzeniu. Godziwa płaca to dla nich czynnik zapewniający bezpieczeństwo społeczne i chroniący przed wykluczeniem.

---

[2] J. Gierszewski, *Organizacja systemu bezpieczeństwa społecznego*, Difin, Warszawa 2013, s. 14.

[3] *Słownik terminów z zakresu bezpieczeństwa narodowego*, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Wydawnictwo AON, Warszawa 2009, s. 13.

Barry Buzan[4] przedstawia bezpieczeństwo społeczne jako termin tożsamości. „Bezpieczeństwo społeczne dotyczy utrzymywania, w zadowalających warunkach rozwoju, tradycyjnych wzorców języka, kultury i tożsamości religijnej i narodowej oraz zwyczajów"[5].

Ruchy nacjonalistyczne oraz naciski na ponowne wytyczanie granic skutkują napięciami w krajach ze społeczeństwem o zróżnicowanym pochodzeniu etnicznym. Bezpieczeństwo społeczne należy ściśle powiązać z bezpieczeństwem socjalnym, które dotyczy zagrożeń wywołanych przez analfabetyzm, dyskryminację, ubóstwo, choroby, narkotyki oraz przestępczość i terroryzm. Państwo demokratyczne powinno zadbać o bezpieczeństwo społeczne swoich obywateli niezależnie od ich statusu materialnego, aby mogli brać czynny udział w życiu społecznym. Ograniczenia ekonomiczne dużych grup społecznych negatywnie wpływają na funkcjonowanie demokracji w państwie[6]. Bezpieczeństwo socjalne traktowane jest jako ochrona podstaw życia ludzkiego, umożliwienie zaspokajania potrzeb duchowych i materialnych, a także realizacji życiowych celów poprzez tworzenie odpowiednich warunków do nauki i pracy, ochronę zdrowia i godnego życia w okresie emerytalnym[7].

Na bezpieczeństwo społeczne składa się całokształt działań prawnych, które są realizowane przez podmioty rządowe, pozarządowe i społeczeństwo w celu zapewnienia odpowiedniego poziomu życia jednostkom, rodzinom i grupom społecznym, jak również eliminacji marginalizacji i wykluczenia społecznego. Chodzi tu zarówno o pomoc dla osób czasowo lub trwale niezdolnych do pracy zawodowej z różnych przyczyn, jak i zachęcenie młodych ludzi wchodzących na rynek pracy do aktywnego w nim udziału. Główną zachętą jest tutaj wynagrodzenie, które umożliwia usamodzielnienie się i stworzenie nowego gospodarstwa domowego.

Wynagrodzenie za pracę to główne źródło, które gwarantuje zaspokojenie najważniejszych potrzeb pracownika. Płaca pracownika powinna być ustalona odpowiednio do rodzaju wykonywanej pracy, kwalifikacji pracownika, jak również w stosunku do ilości i jakości świadczonej pracy. Współczesna teoria pomiaru kapitału ludzkiego i godziwych wynagrodzeń, której autorem jest Mieczysław Dobija, wskazuje, że kapitał ludzki pracownika to potencjalna zdolność do wykonywania pracy, praca rozumiana jest jako transfer kapitału do obiektów pracy, a wynagrodzenie to należność za zrealizowany transfer kapitału. Za wykonaną pracę pracownikowi należy się godziwe wynagrodzenie, które powinno wzrastać wraz z kolejnym

---

4 B. Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, London 1991, s. 18–19

5 Cyt. za: M. Leszczyński, *Bezpieczeństwo społeczne a współczesne państwo*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2011, R. LII, nr 2 (185), s. 124.

6 *Ibidem*, s. 124–125.

7 A. Skrabacz, *Bezpieczeństwo społeczne*, [w:] *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, red. R. Jakubczak, J. Flis, Dom Wydawniczy Bellona, Warszawa 2006, s. 413.

przepracowanym okresem[8]. Pracownicy wchodzący na rynek pracy liczą, że ich wynagrodzenie zabezpieczy ich życie w społeczeństwie. Jednak często proponuje się im ustawowe płace minimalne, co dla wielu nie jest godziwym wynagrodzeniem, które daje poczucie bezpieczeństwa.

Płaca minimalna

Na temat płacy minimalnej jest wiele opinii. Jedni uważają, że istnienie płacy minimalnej to zło konieczne, i twierdzą, że powinna funkcjonować na jak najniższym poziomie. Natomiast Międzynarodowa Organizacja Pracy (MOP) sygnalizuje, aby płaca minimalna kształtowała się na poziomie 50% średniego wynagrodzenia. Komitet Niezależnych Ekspertów Rady Europy przedstawia odmienne rozwiązanie dotyczące kształtowania się płacy minimalnej[9]. Bazą do określenia jej wysokości powinna być płaca przeciętna. Eksperci twierdzą, że godziwe wynagrodzenie powinno kształtować się na poziomie 68% kwoty tzw. mediany płacowej w danym kraju.

W Polsce płaca minimalna została wprowadzona w 1956 r., a jej rola w systemie płac w ciągu lat uległa licznym zmianom. Na początku swojego istnienia płaca minimalna stanowiła zagwarantowany wszystkim pracownikom poziom łącznego uposażenia. W następnych latach poziom minimalnego wynagrodzenia wykorzystywano głównie do tworzenia tabel stawek wynagrodzenia i ustalany był on jako najmniejsza stawka wynagrodzenia zasadniczego w najniższej kategorii zaszeregowania. W latach 80. ubiegłego wieku wyznaczano poziom najniższego wynagrodzenia oraz wysokość najniższej stawki wynagrodzenia w najniższej kategorii zaszeregowania. W 1990 r. ustalano najniższe wynagrodzenie jako kwotę pełnego miesięcznego wynagrodzenia gwarantowanego pracownikom bez względu na posiadane przez nich kwalifikacje, jak również niezależnie od liczby i rodzaju stosowanych w zakładach pracy elementów wynagrodzenia. Do 1990 r. poziom najniższego wynagrodzenia ustalany był przez Radę Ministrów w drodze uchwały, następnie o wysokości najniższego wynagrodzenia stanowiły zarządzenia ministra pracy i polityki socjalnej. W latach 1998–2002 wysokość minimalnego wynagrodzenia określana była w rozporządzeniach ministra pracy, aż do dnia 10 października 2002 r., kiedy wprowadzona została ustawa o minimalnym wynagrodzeniu za pracę[10]. Tabele 1 i 2 prezentują polską płacę minimalną od początku jej funkcjonowania.

---

[8] B. Oliwkiewicz, *The impact of capital from experience on the value of an employee's fair remuneration*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2019, t. 63, nr 10, s. 208.

[9] A. Bojanowska-Sosnowska, C. Marzęda, *Regionalizacja płacy minimalnej w Polsce – rozważania*, Fundacja Republikańska, Biuro Rzecznika Małych i Średnich Przedsiębiorstw, Warszawa 2021, s. 10.

[10] M. Raczkowska, *Minimalne wynagrodzenie za pracę w Polsce i w wybranych krajach świata*, „Zeszyty Naukowe SGGW – Ekonomika i Organizacja Gospodarki Żywnościowej" 2007, nr 62, s. 42–44.

Tabela 1. Minimalne wynagrodzenie za pracę w Polsce w latach 1956–1994

Rok	Wysokość minimalnego wynagrodzenia (PLZ)	Rok	Wysokość minimalnego wynagrodzenia (PLZ)
1956	364–500	1982	3000–5400
1959	600	1986	5400
1961	700	1987	7000
1963	750	1988	9000
1966	850	1989	17 800 – 38 000
1970	1000	1990	120 000 – 440 000
1974	1200	1991	550 000 – 700 000
1977	1400	1992	875 000 – 1 350 000
1978	1600	1993	1 500 000 – 1 750 000
1979	1800	1994	1 950 000 – 2 400 000
1980	2000		

Źródło: B. Oliwkiewicz, *Historia polskiej płacy minimalnej na gruncie teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń*, „Nierówności Społeczne a Wzrost Gospodarczy" 2019, nr 57, s. 424.

Tabela 2 przedstawia płacę minimalną w Polsce w okresie po denominacji złotego, od 1996 do 2023 r.

Tabela 2. Minimalne wynagrodzenie za pracę w Polsce w latach 1995–2023

Rok	Wysokość minimalnego wynagrodzenia (PLN)	Rok	Wysokość minimalnego wynagrodzenia (PLN)
1995	260–305*	2010	1317
1996	325–370	2011	1386
1997	391–450	2012	1500
1998	500	2013	1600
1999	528–670	2014	1680
2000	700	2015	1750
2001	760	2016	1850
2003	800	2017	2000
2004	824	2018	2100
2005	849	2019	2250
2006	899,10	2020	2600
2007	936	2021	2800
2008	1126	2022	3010
2009	1276	2023	3490/3600**

* Zgodnie z ustawą z dnia 7 lipca 1994 r. o denominacji złotego (Dz.U. z 1994 r., nr 84, poz. 386) od 1 stycznia 1995 r. obowiązuje nowa jednostka pieniężna o nazwie „złoty" (PLN); 1 PLN = 10 000 PLZ.

** 3490 zł – wynagrodzenie minimalne obowiązujące od 01.01.2023 do 30.06.2023; 3600 zł – wynagrodzenie minimalne obowiązujące od 01.07.2023 do 31.12.2023.

Źródło: opracowanie własne na podstawie danych z roczników statystycznych GUS.

Współczesny polski system płacy minimalnej funkcjonuje według ustawy o minimalnym wynagrodzeniu za płacę[11]. W myśl przepisów poziom płacy minimalnej to efekt negocjacji partnerów społecznych w ramach Komisji Trójstronnej. Obowiązkiem Komisji jest ogłoszenia stawki płacy minimalnej na najbliższy rok kalendarzowy do dnia 15 lipca roku poprzedniego. W razie niezachowania tego terminu decyzję o wynagrodzeniu minimalnym podejmuje Rada Ministrów. Ogłoszenie decyzji o najniższym wynagrodzeniu musi nastąpić do dnia 15 września. Ustawa mówi, że płaca minimalna powinna zostać podwyższona o nie mniej niż prognozowany wskaźnik cen na dany rok. Dodatkowo w sytuacji, kiedy płaca minimalne nie przekracza 50% średniej krajowej, najniższą płacę należy zwiększyć o 2/3 przewidywanej dynamiki PKB. W trakcie ustalania poziomu płacy minimalnej należy również brać pod uwagę sytuację budżetową, poziom bezrobocia, produktywność pracy oraz potencjał przedsiębiorstw, a także koszty utrzymania[12].

Tabela 3. Relacja płacy minimalnej do płacy średniej w Polsce w latach 2008–2023

Rok	Minimalne wynagrodzenie brutto (PLN)	Przeciętne wynagrodzenie brutto w gospodarce narodowej (PLN)	Relacja wynagrodzenia minimalnego do wynagrodzenia przeciętnego
2008	1126	2944	38,25%
2009	1276	3103	41,12%
2010	1317	3225	40,84%
2011	1386	3400	40,76%
2012	1500	3521	42,60%
2013	1600	3650	43,84%
2014	1680	3783	44,41%
2015	1750	3900	44,87%
2016	1850	4047	45,71%
2017	2000	4272	46,82%
2018	2100	4585	45,80%
2019	2250	4918	45,75%
2020	2600	5167	50,32%
2021	2800	5663	49,44%
2022	3010	6346	47,43%
2023	3490/3600	7124 (I kwartał)	48,99%

Źródło: opracowanie własne na podstawie danych z roczników statystycznych GUS.

[11] Ustawa z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, tekst jedn. Dz.U. z 2020 r., poz. 2207.

[12] B. Oliwkiewicz, *Historia polskiej płacy minimalnej na gruncie teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń*, „Nierówności Społeczne a Wzrost Gospodarczy" 2019, nr 57, s. 424–426.

W Polsce system płacy minimalnej posiada więc trwałe podstawy prawne, ale jest zachowawczy i ostrożny. Analizując dane dotyczące relacji płacy minimalnej do płacy średniej w Polsce w latach 2008–2023, zawarte w tabeli 3, można stwierdzić, że między 2008 i 2009 r. relacja ta zwiększa się, jednak poziom jej nie spełnia zaleceń MOP i świadczy raczej o utrzymaniu status quo niż dążeniu do godziwego poziomu minimalnego wynagrodzenia. W latach 2010–2011 stosunek minimalnego wynagrodzenia do średniego uległ zmniejszeniu. Począwszy od 2012 r. zauważyć można tendencję wzrostową, a w 2017 r. stosunek ten wynosił prawie 47%. W latach 2018–2019 nastąpił nieznaczny spadek, a w 2020 r. po raz pierwszy przekroczony został poziom 50%. Jednak w kolejnych latach udział płacy minimalnej w średnim wynagrodzeniu w Polsce ponownie uległ obniżeniu. W 2023 r., biorąc pod uwagę dane za I kwartał, stosunek ten wynosił prawie 49%. Słabym punktem polskiego systemu płacy minimalnej jest jednolita stawka, co powoduje ograniczenia obszaru jej bezpośredniego oddziaływania do najsłabszych grup zawodowych.

Model pomiaru kapitału ludzkiego i godziwych wynagrodzeń

Współczesna teoria pomiaru kapitału ludzkiego i godziwych wynagrodzeń ma swoje początki w latach 90. ubiegłego wieku. Zapoczątkowana przez M. Dobiję, jest kontynuowana i rozwijana przez grupę krakowskich naukowców do dzisiaj. W ramach różnych badań między innymi: Mieczysława Dobii[13], Wojciecha Kozioła[14], Jurija Renkasa[15], Bartosza Kurka i Ireneusza Górowskiego[16] oraz Barbary Oliwkiewicz[17] została zidentyfikowana stała ekonomiczna potencjalnego wzrostu (p = 8%) oraz zdefiniowany model pomiaru kapitału ludzkiego i godziwych wynagrodzeń.

Jednym z wielu założeń w prezentowanym modelu jest konstatacja, że kapitał nie powstaje z niczego i ma swoje źródła umożliwiające jego wycenę w jednostkach pieniężnych. Należy zwrócić szczególną uwagę (za M. Dobiją) na różnice pomiędzy osobą pracownika a jego kapitałem ludzkim, który jest miarą zdolności człowieka do wykonywania pracy. Autor ten uważa, że człowiek stanowi triadę: ciała – umysłu – ducha.

---

13 M. Dobija, *Kapitał ludzki i intelektualny w aspekcie teorii rachunkowości*, „Przegląd Organizacji" 2002, nr 1 (744), s. 8–13.

14 W. Kozioł, *Pomiar kapitału ludzkiego jako podstawa kształtowania relacji płac w organizacji*, rozprawa doktorska, Uniwersytet Ekonomiczny w Krakowie, Kraków 2010.

15 J. Renkas, *Teoria pomiaru kapitału ludzkiego jako podstawa analizy wynagrodzeń w gospodarce Ukrainy*, rozprawa doktorska, Uniwersytet Ekonomiczny w Krakowie, Kraków 2014.

16 B. Kurek, I. Górowski, *Gender and Age as Determinants of Expected Rate of Return on Human Capital*, „Central European Management Journal" 2020, vol. 28, nr 4, s. 30–50, https://doi.org/10.7206/cemj.2658-0845.33.

17 B. Oliwkiewicz, *Oczekiwania płacowe a godziwe wynagrodzenie absolwentów studiów ekonomicznych*, [w:] *Zarządzanie zrównoważonym rozwojem organizacji. Wybrane aspekty*, red. D. Fatuła, Oficyna Wydawnicza AFM, Kraków 2020, s. 67–94.

Zatem kapitał ludzki ma swoje korzenie w skapitalizowanych nakładach koniecznych do stworzenia ekonomicznego zasobu w postaci jednostki ludzkiej. Ciało i umysł potrzebują nakładów wynikających z kosztów utrzymania, których poniesienie jest konieczne do prawidłowego przygotowania organizmu ludzkiego, czyli nośnika kapitału ludzkiego. Warunkiem niezbędnym do ujawnienia się i rozwoju wrodzonych umiejętności, zdolności i możliwości podczas nauki i pracy (umysł) jest odpowiednie ukonstytuowanie organizmu ludzkiego (ciało). Nakłady ponoszone są od momentu pojawienia się człowieka na świecie do chwili wejścia na rynek pracy. Wydatki te wprawdzie finansowane są przez rodzinę i społeczeństwo, ale właścicielem wytworzonego kapitału ludzkiego jest człowiek, na rzecz którego owe nakłady zostały poniesione[18]. Trzeci składnik triady – duch – ujawnia się w momencie kreatywnego działania ludzi i nie da się go zmierzyć jako strumienia nakładów. Zakładając zatem, że człowiek jest właścicielem swojego kapitału ludzkiego, można stworzyć formułę kapitału ludzkiego pracownika (H_t), który będzie zależał od nakładów początkowych (H_0), stałej ekonomicznej potencjalnego wzrostu *(p)* i czasu kapitalizacji *(t)*.

Wykorzystując wzór na procent składany i zasadę dualizmu wyprowadzony został model pomiaru kapitału ludzkiego[19]:

$$H_{(T)} = (K_{t,p} + E_{t,p}) \times (1 + Q_{(T)})$$

Tabela 4 prezentuje wzory, które przedstawiają powstanie kapitału ludzkiego z kosztów utrzymania i profesjonalnej edukacji.

Tabela 4. Formuły przedstawiające powstawanie kapitału ludzkiego

	Koszty utrzymania	Koszty edukacji
Kapitalizacja roczna	$K_t = k \times 12 \times \frac{(1+p)^t - 1}{p}$	$E_t = e \times 12 \times \frac{(1+p)^t - 1}{p}$
Kapitalizacja ciągła	$K_t = k \times 12 \times \frac{e^{pt} - 1}{p}$	$E_t = e \times 12 \times \frac{e^{pt} - 1}{p}$

$H_t(T,p)$ – wartość kapitału ludzkiego,
K_t – skapitalizowane koszty utrzymania,
E_t– skapitalizowane koszty edukacji,
$Q(T)$ – czynnik określający wzrost kapitału ludzkiego w wyniku pracy zawodowej wykonywanej przez okres T,
T – liczba lat pracy zawodowej,
k – miesięczne niezbędne koszty utrzymania,
e – miesięczne niezbędne koszty edukacji,
t – liczba lat kapitalizacji niezbędnych kosztów utrzymania lub niezbędnych kosztów profesjonalnej edukacji.

Źródło: opracowanie własne.

[18] W. Kozioł, *op. cit.*, s. 74–77.

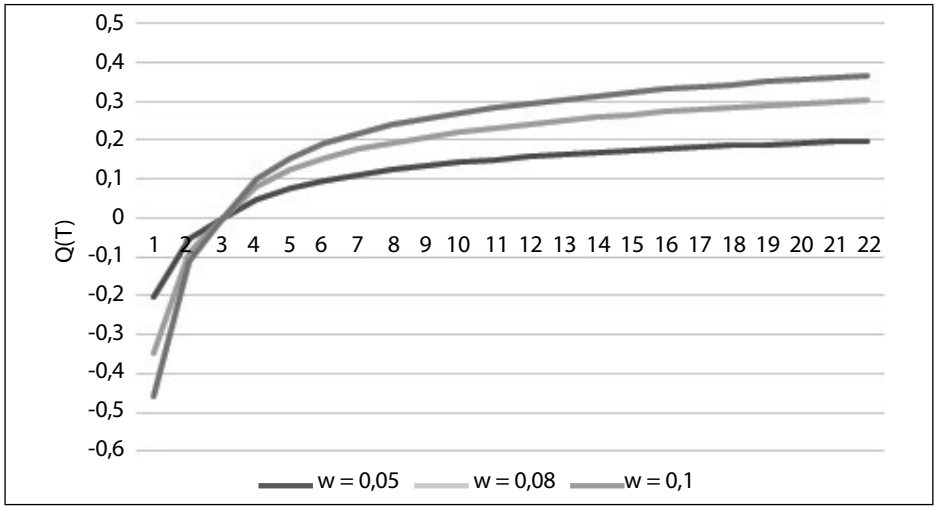
[19] M. Dobija, *Struktura i koszt kapitału ludzkiego*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2002, nr 562, s. 62.

W momencie rozpoczęcia pracy zawodowej pojawia się kapitał z doświadczenia, który jest wyliczany przy użyciu współczynnika doświadczenia $Q_{(T)}$, którego postać przedstawiono poniżej[20]:

$$Q_{(T)} = 1 - (T)^{\frac{\ln(1-w)}{\ln 2}}$$

Zmienna T prezentuje staż pracy, a zmienna w to współczynnik uczenia. Powiększanie kapitału z doświadczenia w trakcie wykonywania pracy można omówić w oparciu o koncepcję krzywej uczenia. Korzeni krzywej uczenia doszukać się można w przemyśle amerykańskim w latach 20. ubiegłego stulecia[21]. Na podstawie pomiarów udowodniono, że przy produkcji drugiego samolotu potrzeba o 20% mniej czasu pracy w stosunku do pierwszego, produkcja czwartego samolotu pochłania 20% mniej czasu pracy w stosunku do drugiego, a produkcja dziesiątego 20% mniej niż piątego. Efektem jest określony spadek czasu pracy pracowników bezpośrednich. W tym konkretnym przykładzie zmniejszenie wynosi 20% wraz z podwojeniem liczby egzemplarzy. Stwierdzić zatem można, że dzięki posiadanym zdolnościom intelektualnym pracownika następuje zjawisko zmniejszenia się czasu wykonywania danych czynności. Zauważalne nasilenie tego zjawiska pojawia się w początkowym etapie pracy zawodowej. W okresie tym, w pracowniku kryją się rezerwy doskonalenia wykonywanych czynności, które jeszcze nie zostały wykorzystane[22].

Wykres 1. Krzywa uczenia



Źródło: opracowanie własne.

[20] Idem, *Kapitał ludzki i intelektualny...*, *op. cit.*, s. 11.

[21] M. Ossowski, *Jak w praktyce korzystać z krzywej uczenia się*, „Controlling i Rachunkowość Zarządcza" 2006, nr 2, s. 18–20.

[22] B. Oliwkiewicz, *The impact of capital from experience...*, *op. cit.*, s. 214–215.

Wykres 1 prezentuje schemat graficzny krzywej uczenia dla różnych parametrów uczenia: $w = 0{,}05$, $w = 0{,}08$, w = 0,1. Parametr uczenia w ma wpływ na wzrost doświadczenia. Gdy jest on na przykład równy 0,1, oznacza to, że dany pracownik będzie wykonywał tę samą pracę w kolejnym roku o 10% łatwiej, taniej i krócej. We wszystkich trzech przypadkach, przedstawionych na wykresie 1, zauważalna jest duża tendencja wzrostowa w pierwszych latach zdobywania doświadczenia zawodowego, która z czasem zostaje spowolniona, co potwierdza tezę, że z biegiem lat maleje udział czynnika doświadczenia w wartości kapitału ludzkiego.

Analiza empiryczna oczekiwań płacowych studentów studiów licencjackich

Do analizy oczekiwanych wynagrodzeń wykorzystane zostały dane empiryczne zebrane w badaniu ankietowym studentów kierunków ekonomicznych. Zapytano, jakie wynagrodzenie wzbudzi u nich poczucie bezpieczeństwa społecznego. Badania prowadzone były od lutego do maja 2023 r. Ankietę wypełniło 123 studentów studiów licencjackich, stacjonarnych i niestacjonarnych jednej z krakowskich uczelni. Zebrany materiał empiryczny obejmował informacje na temat wieku, liczby lat kształcenia, kwot kosztów związanych z edukacją, a także kwot oczekiwanego wynagrodzenia. W celu uzyskania wiarygodnych wyników, dobór badanych był losowy. Przedmiotem badań i wniosków, na gruncie współczesnej teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń, były wynagrodzenia oczekiwane gwarantujące bezpieczeństwo społeczne. Ich określenie pozwoliło ocenić, czy oczekiwany stopień opłacenia pracy jest na poziomie 8% kapitału personalnego absolwenta.

Szacowanie poziomu wynagrodzeń godziwych studentów odbyło się na podstawie rachunku pomiaru kapitału ludzkiego. Do modelu przyjęto założenia odnoszące się do sytuacji ekonomicznej w Polsce na rok 2023. Wielkość kosztów utrzymania została oparta na rozmiarze kategorii minimum socjalnego publikowanego corocznie przez Instytut Pracy i Spraw Socjalnych (IPiSS). Minimum socjalne to kategoria, która obejmowała wielkość kosztów utrzymania niezamożnych gospodarstw domowych ustalonych na poziomie zabezpieczającym warunki, by w każdym momencie rozwoju człowieka umożliwić reprodukcję jego sił witalnych, posiadanie i wychowywanie dzieci oraz utrzymania więzi ze społeczeństwem[23]. Należy również zwrócić uwagę na to, że koszty te powinny być liczone jako koszt utrzymania jednej osoby w modelowej 4-osobowej rodzinie pracowniczej (warunek niezbędny, by

[23] L. Deniszczuk, *Wzorzec konsumpcji społecznie niezbędnej*, „Studia i Materiały IPiSS" 1977, nr 10.

kapitał ludzki mógł zostać odnowiony w długim okresie). Zatem miesięczne koszty utrzymania na poziomie minimum socjalnego w 2023 r. wyniosły 1230 zł[24].

Modelowy student, analizowany w tym opracowaniu, gromadził kapitał, ponosząc koszty utrzymania przez 21, 22 lub 23 lata (lata wczesnego dzieciństwa, przedszkola, szkoły podstawowej, gimnazjum, szkoły średniej (liceum lub technikum)). Koszty utrzymania studenta będą kapitalizowane przez 21, 22 lub 23 lata. Kolejnym ważnym składnikiem modelu płacy godziwej są koszty ponoszone na edukację. Koszty profesjonalnej edukacji ponoszone są przez okres studiów licencjackich (czyli 3 lata) i jest to okres kapitalizacji kosztów edukacji. Do kosztów edukacji zaliczymy wydatki na: czesne, materiały pomocnicze, książki, ksero, dojazdy itp. Z badania ankietowego przeprowadzonego wśród studentów wynika, że miesięczne koszty edukacji kształtują się średnio na poziomie 1900 zł. W obliczeniach wykorzystano stałą ekonomiczną potencjalnego wzrostu wynoszącą 8%. Współczynnik uczenia niezbędny do wyliczenia współczynnika Q symbolizującego doświadczenie zawodowe przyjęto na średnim poziomie $w = 0{,}05$. Absolwent kończący studia zwykle nie ma doświadczenia zawodowego, zatem wartość jego czynnika doświadczenia po pierwszym miesiącu pracy ($T = \frac{1}{12}$) jest ujemna:

$$Q_{(\frac{1}{12})} = 1 - (\frac{1}{12})^{\frac{\ln(1-0{,}05)}{ln2}} = -0{,}2019$$

Obliczenie wartości kapitału ludzkiego i godziwego minimalnego wynagrodzenia studenta studiów licencjackich uwzględnia następujące dane: $k = 1230$ zł miesięcznie, $e = 1900$ zł miesięcznie, $p = 8\%$, $w = 5\ \%$
Skapitalizowane koszty utrzymania:

$$K_{t,p} = k \times 12\ \frac{e^{pt} - 1}{p}$$

Koszty utrzymania kapitalizowane są przez 21 lat, zatem:

$$K_{21} = 1230 \times 12 \times \frac{e^{0{,}08 \times 21} - 1}{0{,}08} = 805\,445{,}08 \text{ zł}$$

Skapitalizowane koszty edukacji

$$E_{t,p} = e \times 12\ \frac{e^{pt} - 1}{p}$$

[24] *Wysokość minimum socjalnego*, IPiSS, https://www.ipiss.com.pl/pion-badawczy-polityki-spolecznej/wysokosc-minimum-socjalnego [stan na 31.03.2023].

Koszty profesjonalnej edukacji kapitalizowane są przez 3 lata studiów:

$$E_3 = 1900 \times 12 \times \frac{e^{0,08\times 3} - 1}{0,08} = 77\,306,01 \text{ zł}$$

Wartość kapitału ludzkiego $H_{(\frac{1}{12})}$:

$$H_{(\frac{1}{12})} = (K_{t,p} + E_{t,p}) \times (1 + Q_{(\frac{1}{12})})$$

Wartość kapitału ludzkiego dla 21-latka po pierwszym miesiącu pracy zawodowej wynosi $H_{(\frac{1}{12})}$:

$$H_{(\frac{1}{12})} = (805\,445,08 + 77\,306,01) \times (1 - 0,2019) = 704\,523,65 \text{ zł}$$

W analogiczny sposób obliczono wartość kapitału ludzkiego dla 22- i 23-latka.

W tabeli 5, ze względu na ograniczenia niniejszej pracy, zaprezentowano fragmenty wyników przeprowadzonych badań ankietowych.

Otrzymane wyniki oczekiwanej stopy zwrotu z kapitału ludzkiego absolwentów studiów licencjackich kolejny raz potwierdzają istnienie stałej ekonomicznej potencjalnego wzrostu (p = 8%). Średnia stopa zwrotu w przeprowadzonym badaniu to 8,40%, co oznacza, że wynagrodzenia oczekiwane przez respondentów są na poziomie godziwym i będą w stanie zagwarantować im bezpieczeństwo socjalne i społeczne.

Tabela 5. Wyniki pomiaru kapitału ludzkiego i poziomu oczekiwań płacowych studentów studiów licencjackich (wybrane pozycje)

Lp.	Oczekiwane wynagrodzenie (PLN)	Skapitalizowane koszty utrzymania (PLN)	Skapitalizowane koszty edukacji (PLN)	$Q_{(\frac{1}{12})}$	Kapitał absolwenta $H_{(0)}$ (PLN)	Roczna płaca oczekiwana zaraz po studiach (PLN)	Oczekiwana stopa zwrotu z kapitału ludzkiego
1	4500	887894,70	77306,01	–0,2019	770326,69	54000	7,01%
2	5000	887894,70	77306,01	–0,2019	770326,69	60000	7,79%
3	5000	887894,70	77306,01	–0,2019	770326,69	60000	7,79%
4	5500	977211,31	77306,01	–0,2019	841610,27	66000	7,84%
…	…	…	…	…	…	…	…
18	6500	887894,70	77306,01	–0,2019	770326,69	78000	10,13%
19	4500	887894,70	77306,01	–0,2019	770326,69	54000	7,01%
20	6000	887894,70	77306,01	–0,2019	770326,69	72000	9,35%
21	5000	887894,70	77306,01	–0,2019	770326,69	60000	7,79%
…	…	…	…	…	…	…	…
55	4500	887894,70	77306,01	–0,2019	770326,69	54000	7,01%
56	6000	887894,70	77306,01	–0,2019	770326,69	72000	9,35%

Lp.	Oczekiwane wynagrodzenie (PLN)	Skapitalizowane koszty utrzymania (PLN)	Skapitalizowane koszty edukacji (PLN)	$Q_{(\frac{1}{12})}$	Kapitał absolwenta $H_{(0)}$ (PLN)	Roczna płaca oczekiwana zaraz po studiach (PLN)	Oczekiwana stopa zwrotu z kapitału ludzkiego
57	5000	887894,70	77306,01	–0,2019	770326,69	60000	7,79%
…	…	…	…	…	…	…	…
74	5200	887894,70	77306,01	–0,2019	770326,69	62400	8,10%
75	6000	805445,08	77306,01	–0,2019	704523,64	72000	10,22%
76	5300	805445,08	77306,01	–0,2019	704523,64	63600	9,03%
…	…	…	…	…	…	…	…
90	5000	977211,31	77306,01	–0,2019	841610,27	60000	7,13%
91	6000	977211,31	77306,01	–0,2019	841610,27	72000	8,56%
92	5500	887894,70	77306,01	–0,2019	770326,69	66000	8,57%
93	5000	887894,70	77306,01	–0,2019	770326,69	60000	7,79%
…	…	…	…	…	…	…	…
121	4200	977211,31	77306,01	–0,2019	841610,27	50400	5,99%
122	5500	977211,31	77306,01	–0,2019	841610,27	66000	7,84%
123	4800	977211,31	77306,01	–0,2019	841610,27	57600	6,84%
średnia	5423				774695,08	65078	8,40%

Źródło: opracowanie własne.

Kolejnym etapem badania było wskazanie minimalnego godziwego wynagrodzenia dla ankietowanych w świetle współczesnej teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń.

Roczne koszty pracy wyznacza formuła $p \times H_{(\frac{1}{12})}$:

$$704\,523{,}65 \text{ zł} \times 0{,}08 = 56\,361{,}89 \text{ zł}$$

Wynagrodzenie miesięczne (koszty pracy):

$$\frac{56\,361{,}89 \text{ zł}}{12 \text{ miesięcy}} = 4696{,}82 \text{ zł miesięcznie}$$

Wyznaczona kwota 4696,82 zł jest kwotą wynagrodzenia całkowitego, zatem aby oszacować wynagrodzenie brutto, należy pomniejszyć tę kwotę o składki zapłacone przez pracodawcę (emerytalne: 9,76%; rentowe: 8,00%; wypadkowe: 1,67%; Fundusz Pracy: 2,45%; Fundusz Gwarantowanych Świadczeń Pracowniczych: 0,1% – co daje razem: 21,98%). Wobec powyższego, wynagrodzenie brutto będzie wynosić 3850 zł. Analogiczne obliczenia wynagrodzeń godziwych zostały przeprowadzone dla wieku 22 lata i 23 lata. Wyniki obliczeń prezentuje tabela 6.

Tabela 6. Wartość poszczególnych składników kapitału ludzkiego absolwenta licencjackich studiów ekonomicznych oraz jego godziwe wynagrodzenie ustalone w kontekście teorii kapitału ludzkiego (stan prawny na 2023 r.)

Pozycja na rynku pracy, wiek	Wartość kapitału ludzkiego		Całkowite wynagrodzenie roczne kapitału ludzkiego $H_{(T)} \times 8\%$ (PLN)	Całkowite miesięczne wynagrodzenie (koszty pracy)* (PLN)	Wynagrodzenie miesięczne brutto (PLN)
	Składowe wielkości	Wartość składowych wielkości			
Licencjat bez doświadczenia zawodowego; 21 lat	K_{21}	805 445,08	56 361,89	4696,82	3850
	E_3	77 306,01			
	$H_0 = K_{21} + E_3$	882 751,09			
	D_0	–178 227,45			
	$H_0 = K_{21} + E_3 + D_0$	704 523,64			
Licencjat bez doświadczenia zawodowego; 22 lata	K_{22}	887 894,70	61 626,14	5135,51	4210
	E_3	77 306,01			
	$H_0 = K_{22} + E_3$	965 200,71			
	D_0	–194 874,02			
	$H_0 = K_{22} + E_3 + D_0$	770 326,69			
Licencjat bez doświadczenia zawodowego; 23 lata	K_{23}	977 211,31	67 328,82	5610,74	4600
	E_3	77 306,01			
	$H_0 = K_{23} + E_3$	1 054 517,32			
	D_0	–212 907,05			
	$H_0 = K_{23} + E_3 + D_0$	841 610,27			

* Zawiera płacone składki przez pracodawcę.
Źródło: opracowanie własne.

Na podstawie uzyskanych wyników można stwierdzić, że absolwenci studiów licencjackich, dla poczucia bezpieczeństwa, oczekują wynagrodzeń na poziomie 8% wartości swojego kapitału ludzkiego. Zatem płaca minimalna aktualnie obowiązująca w Polsce nie jest dla nich odpowiednim wynagrodzeniem nawet na początku pracy zawodowej po ukończonych studiach licencjackich.

Podsumowanie

Młody pracownik, rozpoczynający swoje życie zawodowe, liczy na odpowiednie wynagrodzenie, dające poczucie bezpieczeństwa społecznego, umożliwiające realizację celów i zaspokajanie potrzeb. Z czasem oczekuje płacy, która pozwoli na założenie rodziny i zapewni tej rodzinie bezpieczeństwo. Gospodarstwo domowe jest jedynym dostawcą kapitału ludzkiego, a najważniejszym elementem jego współpracy z otoczeniem jest stosunek pracy. Za udostępnianie kapitału ludzkiego gospodarstwo otrzymuje wynagrodzenie, które przeznaczane jest w dużej mierze na pokrycie kosztów odtworzenia kapitału ludzkiego zarówno w krótkim, jak i w długim okresie.

Zbyt niskie płace powodują ograniczenie możliwości zaspokajania podstawowych potrzeb, zachwianie poczucia bezpieczeństwa społecznego i ryzyko wykluczenia z grupy społecznej, co prowadzi do niezadowolenia wśród pracowników. W przypadku młodych ludzi brak poczucia bezpieczeństwa wstrzymuje przed założeniem rodziny i posiadaniem dzieci, co w konsekwencji całego państwa prowadzi do starzenia się społeczeństwa i kłopotów z systemem emerytalnym.

Bibliografia

Bojanowska-Sosnowska A., Marzęda C., *Regionalizacja płacy minimalnej w Polsce – rozważania*, Fundacja Republikańska, Biuro Rzecznika Małych i Średnich Przedsiębiorstw, Warszawa 2021.

Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, London 1991.

Deniszczuk L., *Wzorzec konsumpcji społecznie niezbędnej*, „Studia i Materiały IPiSS" 1977, nr 10.

Dobija M., *Kapitał ludzki i intelektualny w aspekcie teorii rachunkowości*, „Przegląd Organizacji" 2002, nr 1 (744), s. 8–13.

Dobija M., *Struktura i koszt kapitału ludzkiego*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2002, nr 562, s. 59–67.

Gierszewski J., *Organizacja systemu bezpieczeństwa społecznego*, Difin, Warszawa 2013.

Goryń P., *Bezpieczeństwo społeczne – jedno czy wiele?*, [w:] *Bezpieczeństwo i jego percepcja w dyskursie społecznym i militarnym*, red. D. Boćkowski, P. Goryń, K. Goryń, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2020, s. 48–49, https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/10699/1/P_Goryn_Bezpieczenstwo_spoleczne_jedno_czy_wiele.pdf [dostęp: 25.05.2023].

Kozioł W., *Pomiar kapitału ludzkiego jako podstawa kształtowania relacji płac w organizacji*, rozprawa doktorska, Uniwersytet Ekonomiczny w Krakowie, Kraków 2010.

Kurek B., Górowski I., *Gender and Age as Determinants of Expected Rate of Return on Human Capital*, „Central European Management Journal" 2020, vol. 28, nr 4, s. 30–50, https://doi.org/10.7206/cemj.2658-0845.33.

Leszczyński M., *Bezpieczeństwo społeczne a współczesne państwo*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2011, R. LII, nr 2 (185), s. 123–132.

Oliwkiewicz B., *Historia polskiej płacy minimalnej na gruncie teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń*, „Nierówności Społeczne a Wzrost Gospodarczy" 2019, nr 57, s. 420–431.

Oliwkiewicz B., *The impact of capital from experience on the value of an employee's fair remuneration*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2019, t. 63, nr 10, s. 207–220.

Oliwkiewicz B., *Oczekiwania płacowe a godziwe wynagrodzenie absolwentów studiów ekonomicznych*, [w:] *Zarządzanie zrównoważonym rozwojem organizacji. Wybrane aspekty*, red. D. Fatuła, Oficyna Wydawnicza AFM, Kraków 2020, s. 67–94.

Ossowski M., *Jak w praktyce korzystać z krzywej uczenia się*, „Controlling i Rachunkowość Zarządcza" 2006, nr 2, , s. 18–20.

Raczkowska M., *Minimalne wynagrodzenie za pracę w Polsce i w wybranych krajach świata*, „Zeszyty Naukowe SGGW – Ekonomika i Organizacja Gospodarki Żywnościowej" 2007, nr 62, s. 41–53.

Renkas J., *Teoria pomiaru kapitału ludzkiego jako podstawa analizy wynagrodzeń w gospodarce Ukrainy*, rozprawa doktorska, Uniwersytet Ekonomiczny w Krakowie, Kraków 2014.

Skrabacz A., *Bezpieczeństwo społeczne*, [w:] *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, red. R. Jakubczak, J. Flis, Dom Wydawniczy Bellona, Warszawa 2006, s. 403–420.

Słownik terminów z zakresu bezpieczeństwa narodowego, red. J. Kaczmarek, W. Łepkowski, B. Zdrodowski, Wydawnictwo AON, Warszawa 2009.

Wysokość minimum socjalnego, IPiSS, https://www.ipiss.com.pl/pion-badawczy-polityki-spolecznej/wysokosc-minimum-socjalnego [stan na 31.03.2023].

Akty prawne

Ustawa z dnia 7 lipca 1994 r. o denominacji złotego, Dz.U. z 1994 r., nr 84, poz. 386.

Ustawa z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, tekst jedn. Dz.U. z 2020 r., poz. 2207.

Godziwe wynagrodzenie jako element bezpieczeństwa społecznego młodych pracowników

Streszczenie

Młody absolwent studiów, rozpoczynając swoją drogę zawodową, liczy na wynagrodzenie, które zagwarantuje mu bezpieczeństwo finansowe. W myśl współczesnej teorii pomiaru kapitału ludzkiego i godziwych wynagrodzeń, wynagrodzenie godziwe stanowi 8% wartości kapitału ludzkiego pracownika w skali roku.

Celem opracowania jest przedstawienie godziwego wynagrodzenia jako jednego z czynników kształtujących bezpieczeństwo społeczne młodego pracownika. Zaprezentowano wyniki badań własnych dotyczących oczekiwań studentów studiów licencjackich co do wynagrodzenia, które daje poczucie bezpieczeństwa. W badaniu wzięło udział 123 studentów. Otrzymane wyniki potwierdziły, że dla młodego pracownika godziwym wynagrodzeniem oczekiwanym jest kwota, która stanowi średnio 8,40% wartości jego kapitału ludzkiego.

Słowa kluczowe: wynagrodzenie godziwe, płaca minimalna, kapitał ludzki, bezpieczeństwo społeczne

Fair remuneration as an element of social security for young workers

Abstract

When starting his professional career, a young graduate counts on a salary that will guarantee him financial security. According to the modern theory of measuring human capital and fair remuneration, fair remuneration constitutes 8% of the value of an employee's human capital per year.

The aim of the study is to present fair remuneration as one of the factors shaping the social security of a young employee. The results of own research on the expectations of bachelor's degree students according to salary which gives a sense of security are presented. 123 students participated in the study. The results obtained confirmed that the expected fair remuneration for a young employee is an amount that constitutes an average of 8.40% of the value of his human capital.

Keywords: fair remuneration, minimum wage, human capital, social security

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-007
Data wpłynięcia: 4.05.2023
Data akceptacji: 14.09.2023

Wojciech Kozioł

dr, Uniwersytet Ekonomiczny w Krakowie
https://orcid.org/0000-0001-7920-760X

Paweł Łojek

mgr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-4049-4626

Praktyka bezpieczeństwa danych w systemie rachunkowości w świetle badań empirycznych

Wprowadzenie

Z prowadzeniem działalności gospodarczej wiąże się konieczność jej dokumentacji, ewidencji i okresowego rozliczania. Do tego celu służy system rachunkowości, który ma zapewnić wiarygodne i rzetelne źródło informacji o sytuacji ekonomiczno-finansowej podmiotów. Informacje te stanowią niezwykle wrażliwy obszar funkcjonowania organizacji, dlatego zarówno w krajowych, jak i międzynarodowych regulacjach z zakresu organizacji systemu rachunkowości wiele miejsca poświęcono właśnie problematyce bezpieczeństwa danych księgowych. Czwarta rewolucja przemysłowa sprawia, że otwierają się nowe perspektywy dla prowadzenia i rozwijania działalności gospodarczej – dzięki rozwiązaniom, jakie daje cyberprzestrzeń[1]. Jak powszechnie wiadomo, główny cel prowadzenia działalności gospodarczej to maksymalizacja zysków przy minimalnym zaangażowaniu kapitału. Cyfryzacja nie omija również systemu rachunkowości organizacji. Dzieje się tak z przyczyn organizacyjnych i prawnych. Cyfryzacja usprawnia bowiem proces przetwarzania informacji w organizacji

[1] E.I. Szczepankiewicz, *Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań*, „Zeszyty Teoretyczne Rachunkowości" 2018, t. 97, nr 153, s. 115–138.

i w jej otoczeniu gospodarczym. Obowiązkiem organizacji jest rzetelne rozliczenie się nie tylko z właścicielami, ale również z instytucjami państwowymi. Wprowadzone w ostatnich latach regulacje prawne nakładają na organizacje realizację kolejnych obowiązków sprawozdawczych w formie elektronicznej. Przykładem tego jest obowiązek okresowego przesyłania dokumentów elektronicznych: sprawozdań finansowych do Krajowego Rejestru Sądowego (KRS) i deklaracji podatkowych związanych z rozliczaniem podatków: podatku od towarów i usług (VAT), podatku dochodowego od osób prawnych (CIT) i innych (np. VAT-7 w formie tzw. jednolitego pliku kontrolnego (JPK)) – czy też ubezpieczeniowych, wynikających chociażby z ustawy o systemie ubezpieczeń społecznych[2]. Dokumenty te bazują na danych księgowych, co – niezależnie od aspektów organizacyjnych – wymusza na organizacjach digitalizację systemu finansowo-księgowego.

Ostatnie dwie dekady charakteryzuje powszechność systemów cyfrowych. Z punktu widzenia ewolucji społecznej jest to stosunkowo krótki okres. Powoduje to, że w porównaniu do systemów tradycyjnych, istnieje ograniczona świadomość istniejących zagrożeń. Ponadto reakcje ludzi na cyfrowe zagrożenia nie są tak intuicyjne, jak ma to miejsce w przypadku zagrożeń dla tradycyjnych rozwiązań.

Problematyka bezpieczeństwa danych stanowi szczególnie ważną kwestię w przypadku systemu rachunkowości, którego funkcją jest przetwarzanie szerokiego zakresu danych. Dane te zbierane są w trakcie roku obrotowego w następstwie procesu ewidencji wszystkich zdarzeń wywołujących skutki gospodarcze. Następnie w procesie odpowiedniej agregacji tych danych sporządzane są sprawozdania finansowe. Sprawozdania finansowe z założenia mają być wiarygodnym i rzetelnym źródłem informacji o sytuacji ekonomicznej jednostki, które znajdują zastosowanie w procesach decyzyjnych przebiegających wewnątrz jednostki, jak i w jej otoczeniu. Poza obowiązkowymi sprawozdaniami finansowymi, dane finansowe służą również do generowania raportów i zestawień przygotowywanych na potrzeby bieżącego i strategicznego zarządzania jednostką bądź jej poszczególnymi obszarami. Jak można zauważyć, utrata dostępu do tych danych może stanowić realne zagrożenie dla działania jednostki. Problem ten jest dodatkowo potęgowany przez rosnące zapotrzebowanie na informacje pochodzące z systemu rachunkowości, m.in. z powodu wzrostu złożoności powadzenia działalności gospodarczej, jak i pojawiających się nowych tendencji do poszerzania zakresu informacji sprawozdawczej o tzw. dane niefinansowe. Są to informacje środowiskowe i społeczne, które wchodzą w zakres społecznej odpowiedzialności jednostek.

Bezpieczeństwo systemu rachunkowości stanowi istotną kwestię organizacyjną. Uzasadnia to potrzebę identyfikacji zakresu znajomości tych zagrożeń oraz świadomego przeciwdziałania im poprzez stosowanie wymaganych prawem zaleceń. Celem

[2] Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, tekst jedn. Dz.U. z 2022 r., poz. 1009.

artykułu jest zdefiniowanie rozwiązań, jakie przewiduje podstawowy akt normatywny regulujący rachunkowość podmiotów gospodarczych: ustawa z dnia 29 września 1994 r. o rachunkowości[3] (dalej: UoR), oraz inne regulacje określone prawem polskim i niektórymi postanowieniami międzynarodowymi. Przedstawione badania mają odpowiedzieć na pytanie, czy podmioty gospodarcze z wybranej próby badawczej potrafią wskazać rozwiązania, jakie nakłada UoR czy też inne regulacje prawne w omawianym obszarze. Powstaje również pytanie, czy rozwiązania te są stosowane regularnie, czy też wybiórczo. Na próbę badawczą składają się podmioty sporządzające sprawozdania w oparciu o postanowienia UoR jak również Międzynarodowych Standardów Rachunkowości (MSR) zastąpionych od 2001 r. przez Międzynarodowe Standardy Sprawozdawczości Finansowej (MSSF)[4].

W artykule postawiono następujące hipotezy badawcze:

H1: Bezpieczeństwo danych w rachunkowości, w wybranej próbie badawczej wzrosło na przestrzeni analizowanego okresu.

H2: Podmioty poszukują nowych rozwiązań, wykraczających poza postanowienia UoR.

H3: Podmioty starają się zapobiegać ryzyku utraty danych poprzez rozbudowę sieci IT.

Niniejszy artykuł wykorzystuje metody badawcze takie jak analiza i krytyka piśmiennictwa i wyników badań naukowych oraz wnioskowanie statystyczne.

Bezpieczeństwo systemu rachunkowości w świetle uregulowań krajowych i międzynarodowych

Pojęcie bezpieczeństwa

Bezpieczeństwo jest pojęciem wieloznacznym i w zależności od obszaru analizy czy dziedziny wiedzy może być rozumiane w różny sposób. Dodatkowo występuje także w połączeniu z innymi pojęciami i w ten sposób uzyskuje kolejne konteksty znaczeniowe. W efekcie istnieje wielka różnorodność w rozumieniu tego pojęcia. W sytuacji, gdy te same pojęcia są stosowane w wielu obszarach wiedzy lub są pojęciami interdyscyplinarnymi, istnieje niebezpieczeństwo niewłaściwego rozumienia znaczenia specyficznego dla odrębnej specjalności naukowej czy dziedziny wiedzy[5].

Kwestia bezpieczeństwa jest ściśle związana ze stanem analizowanego obiektu. Bezpieczeństwo danego podmiotu to obszar jego aktywności, którego treścią jest

---

[3] Ustawa z dnia 29 września 1994 r. o rachunkowości, tekst jedn. Dz.U. z 2021 r., poz. 217.

[4] P. Łojek, *Wyzwania i odpowiedzialność biegłego rewidenta przy badaniu spółek giełdowych z WIG30*, [w:] *Wyzwania rewizji finansowej*, red. K. Chłapek, S. Krajewska, P. Zieniuk, Difin, Warszawa 2020, s. 129–148.

[5] R. Klamut, *Bezpieczeństwo jako pojęcie psychologiczne*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Ekonomia i Nauki Humanistyczne" 2012, z. 19, nr 4, s. 41–51.

zapewnianie możliwości przetrwania i dalszej egzystencji, a także swobody realizacji własnych interesów w niebezpiecznym środowisku, w szczególności poprzez wykorzystywanie szans, redukowanie ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów. U podstaw rozwiązywania najistotniejszych problemów bezpieczeństwa leży niewątpliwie ocena zagrożeń[6].

Z perspektywy każdego człowieka, bezpieczeństwo to przede wszystkim jedna z jego potrzeb, która została szeroko opisana na gruncie nauk psychologicznych. Jednak system finansowo-księgowy stanowi tzw. obiekt antropogeniczny, czyli obiekt techniczny stworzony celowo przez człowieka, przeznaczony dla realizacji różnorodnych jego potrzeb. Przeciwieństwem obiektu antropogenicznego jest obiekt naturalny, wytworzony przez przyrodę. W teorii zarządzania bezpieczeństwem ważne miejsce zajmuje nurt zarządzania bezpieczeństwem obiektu antropogenicznego, określany również mianem inżynierii bezpieczeństwa obiektów antropogenicznych. Obszarem jej zainteresowania są sposoby postępowania w procesach projektowania, wykonywania i eksploatacji obiektów antropogenicznych. Sposoby te mogą mieć charakter techniczny, ekonomiczny, prawny i organizacyjny i ukierunkowane są na:

- nadawanie tym obiektom cech umożliwiających przeciwstawienie się przewidywanym zagrożeniom (generowanym w samym obiekcie, a także w jego otoczeniu), które mogą wystąpić w czasie jego tworzenia, późniejszej eksploatacji i ewentualnej likwidacji,
- zmniejszanie przewidywanych zagrożeń generowanych w obiekcie, jak i w jego otoczeniu,
- utrzymanie określonego poziomu bezpieczeństwa obiektu przy założonym stopniu ryzyka[7].

Inżynieria bezpieczeństwa obiektów antropogenicznych dotyczy określenia i ciągłego doskonalenia metod postępowania oraz znajomości wymagań i zasad bezpieczeństwa, w tym umiejętności[8]:

- identyfikacji problemów i zadań w zakresie monitorowania, procesów decyzyjnych, eksploatacji i diagnostyki ww. obiektów oraz sposobów zarządzania nimi i inżynierią eksploatacji tych urządzeń,
- opracowywania strategii zarządzania bezpieczeństwem i działań wspierających niezawodność obiektów,
- identyfikacji potrzeb otoczenia gospodarczego i realizacji innowacyjnych działań,
- identyfikacji zagrożenia bezpieczeństwa osobistego, technologii komunikacji oraz metodyki badań inżynierskich.

---

6 S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 2 (18), s. 19–39.

7 A. Baryłka, *Podstawy inżynierii bezpieczeństwa obiektów antropogenicznych*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2015, nr 1, s. 10–16.

8 *Ibidem.*

Specyfika funkcjonowania cyfrowego systemu rachunkowości

Powszechna informatyzacja procesu wymiany informacji zachodząca w ramach systemu rachunkowości powoduje, że system ten funkcjonuje w warunkach określonych przez cyberprzestrzeń. Cyberprzestrzeń można zdefiniować jako kompleksową, automatyczną, złożoną sieć, oderwaną od realnego świata, zbudowaną z wykorzystaniem infrastruktury teleinformatycznej, w której funkcjonowanie człowieka staje się możliwe, a generowane w niej informacje są podstawą istnienia i stają się dobrem najwyższej jakości. Włączenie danego obszaru funkcjonowania organizacji do cyberprzestrzeni można określić mianem cyfryzacji. Cyfryzacja to działanie z wykorzystaniem narzędzi cyfrowych, mające na celu zwiększenie produktywności dzięki wprowadzeniu innowacyjnych produktów i usług, optymalizacji procesów organizacyjnych oraz bardziej efektywnemu wykorzystaniu zasobów takich jak zasoby techniczne, kapitał ludzki czy informacja[9].

Systemy informacyjne, takie jak systemy finansowo-księgowe, mają na celu gromadzenie danych, których ilość jest niemal nieograniczona, co daje im znaczną przewagę nad rozwiązaniami tradycyjnymi. Połączenie znacznej ilości danych z odpowiednim sposobem ich analizy ma przełożenie na rzetelność, wiarygodność oraz szybkość i łatwość pozyskania informacji finansowych. Z drugiej strony z procesem informatyzacji wiążą się też wady. Systemy wymagają czasochłonnych i kosztownych procesów wdrożeniowych i dostosowawczych oraz przeciwdziałania dezaktualizacji technologii. Dodatkowym zagrożeniem dla systemu jest aktywność w sieci, co rodzi ryzyko utraty lub kradzieży danych. Ponadto proces cyfryzacji, w tym cyfryzacji księgowości, wymaga zaangażowania odpowiednio wykwalifikowanych pracowników, których kompetencje są nieustannie aktualizowane. Wskazuje się również, że zmaterializowanie się wspomnianych zagrożeń może wypaczyć proces analizy danych, prowadząc do naruszenia zasady wiernego i rzetelnego obrazu[10].

Coraz szerszy zakres ujawnianych danych wymaga jednak nowych rozwiązań w rachunkowości, dlatego w coraz większym stopniu wykorzystuje się narzędzia informatyczne, takie jak[11]:

- big data,
- hurtownie danych,
- cloud computing (przetwarzanie w chmurze),
- blockchain.

---

[9] A. Kuczyńska-Cesarz, *Selected areas of threats to the security of accounting information system*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2021, nr 3, s. 37–49.

[10] D. Qin, *Designing an Accounting Information Management System Using Big Data and Cloud Technology*, „Scientific Programming" 2022, vol. 33, https://doi.org/10.1155/2022/7931328.

[11] T. Spychała, *Rozwój rachunkowości a cyberprzestrzeń w społeczeństwie sieci*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2019, nr 11, s. 109–118.

Nieco inną klasyfikację zagrożeń w systemie informatycznym przedsiębiorstwa przedstawia Kamila Schneider i Karol Schneider[12]:

1. Ze względu na źródło:
   a) zagrożenia wewnętrzne, na które jednostka ma wpływ:
   – organizacyjne, wynikające z nieprawidłowej organizacji jednostki,
   – technologiczne, będące następstwem błędów technologicznych,
   b) zewnętrzne, pochodzące z otoczenia jednostki gospodarczej.
2. Ze względu na celowość działania:
   a) przypadkowe (losowe),
   b) celowe (umyślne).
3. Ze względu na rodzaj zagrożenia:
   a) dotyczące oprogramowania,
   b) dotyczące sprzętu.
4. Ze względu na wynik – zagrożenia prowadzące do:
   a) całkowitej utraty danych,
   b) kradzieży informacji (wycieku danych),
   c) ingerencji w przetwarzane dane.

Bezpieczeństwo danych w systemach finansowo-księgowych

Ochrona danych w systemach informatycznych, audyty systemów informatycznych czy też bezpieczeństwo ich danych były przedmiotem rozważań wielu autorów[13]. Publikacje te wskazały rozwiązania, jakie należy przyjąć w zakresie ochrony danych rachunkowych w jednostkach gospodarczych. Postępująca informatyzacja podmiotów gospodarczych oraz liczne czynniki zewnętrzne i wewnętrzne powodują konieczność rozszerzania dotychczas stosowanej technologii, a także poszukiwanie nowych rozwiązań. Autorzy tych badań postulują rozwój w obszarze bezpieczeństwa danych w rachunkowości poprzez aspekty organizacyjne, kontrolę wewnętrzną, a także wdrażanie instrukcji, procedur czy też innych schematów mających na celu poprawę ogółu funkcjonowania jednostki w tym aspekcie.

---

[12] K. Schneider, K. Schneider, *Zagrożenia w funkcjonowaniu jednolitego pliku kontrolnego*, „Ekonomiczne Problemy Usług" 2018, nr 2 (131), t. 1, s. 323–330.

[13] T. Ciesielczyk, J. Stępniewski, *Ochrona danych w systemach informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 1994, nr 691: *Informatyka ekonomiczna*, s. 17–23; B. Galica, B. Tomczyk-Noga, *Atestacja systemów informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej w Katowicach", 1997: *Rachunkowość w gospodarce rynkowej: nauka i praktyka. Materiały konferencyjne. Ogólnopolski Zjazd Katedr Rachunkowości, Ustroń 17–19 września 1997*, t. 1, s. 121–124; J. Madej, K. Szymczyk-Madej, *Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach według kodeksu karnego, ustawy o rachunkowości i ustawy o ochronie danych osobowych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 770, s. 89–107; K. Szymczyk-Madej, J. Madej, *Bezpieczeństwo informatycznych systemów rachunkowości*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2000, nr 553, s. 161–177.

W przepisach art. 71–76 UoR zostały wprowadzone regulacje dotyczące ochrony danych w jednostkach podlegających postanowieniom tej ustawy, określonych w art. 2. Ustawodawca wskazał, że komputerowe prowadzenie ksiąg rachunkowych powinno opierać się na:

- stosowaniu nośników danych, które są odporne na wszelkie zagrożenia,
- doborze odpowiednich środków ochrony zewnętrznej,
- tworzeniu rezerwowych kopii zbiorów danych odpowiednio zabezpieczonych na nośnikach informatycznych zapewniających trwałość zapisu przez określony ustawą czas (art. 74 ust. 2 UoR),
- zapewnieniu ochrony programów komputerowych oraz danych systemowych poprzez zastosowanie odpowiednich rozwiązań informatycznych i organizacyjnych.

Z analizy przepisów wynika, że UoR nie wskazuje wprost rozwiązań, jakie powinna przyjąć jednostka gospodarcza stosująca jej postanowienia. Zatem każdy podmiot gospodarczy powinien dokonać osądu oraz wskazać właściwe rozwiązania w omawianych kwestiach. Przykładowe rozwiązania zostały przedstawione w tabeli 1 – jako interpretacja przepisów UoR według autorów.

Tabela 1. Przykładowe rozwiązania w zakresie ochrony danych rachunkowych zgodnej z UoR

Rodzaj ochrony	Przykładowe rozwiązania
Ochrona danych w systemie	niekorzystanie z systemu przez osoby nieupoważnione lub nieuprawnione, zabezpieczenie przed nieupoważnionym wtargnięciem do pomieszczeń – odpowiednie drzwi, środki identyfikacji użytkowników uruchamiających komputery – hasła,
Ochrona systemu przed uszkodzeniem	przeglądy i bieżąca konserwacja sprzętu komputerowego, konserwacja standardowego oprogramowania, ochrona przed wirusami komputerowymi, współpraca z zewnętrznym serwisantem, która wykluczy długotrwałe przerwy w pracy systemu,
Ochrona przechowywanych zbiorów i dowodów księgowych	przekazywanie zbiorów i dowodów do archiwum, tworzenie kopii zapasowych informacji księgowych na zewnętrznych nośnikach

Źródło: opracowanie własne na podstawie art. 71–76 ustawy z dnia 29 września 1994 r. o rachunkowości, tekst jedn. Dz.U. z 2021 r., poz. 217.

Jak wspomniano, pewne minimalne wymagania dla systemów informatycznych wspomagających rachunkowość przedsiębiorstwa zostały podane w UoR. Nie określono jednak procedur pozwalających na stwierdzenie, czy wymagania te są spełnione w stosowanych systemach informatycznych. Warto podkreślić, że Stowarzyszenie Księgowych w Polsce (SKwP), będące największą organizacją zawodową w obszarze

rachunkowości, prowadzi aktywność polegającą na weryfikacji produktów informatycznych wspierających procesy finansowo-księgowe w organizacjach. Lista rekomendowanych programów jest dostępna na stronie internetowej SKwP[14].

Ochrona danych w systemie polega głównie na zabezpieczeniu wszelkich informatycznych systemów oraz pomieszczeń przed osobami nieuprawnionymi. Najprostszą formą ochrony jest zastosowanie haseł zabezpieczających oraz odpowiednie wyposażenie pomieszczeń i budynków w drzwi posiadające funkcję zabezpieczenia systemów informatycznych. Stosowanie odpowiednich haseł zostało wypracowane jako jedna z metod zabezpieczeń przez praktyki rynkowe, a – co ciekawe – nie przez przepisy o ochronie danych osobowych (RODO)[15].

Każde przedsiębiorstwo powinno przeprowadzić analizę ryzyka, która rozpoznaje i wskazuje potencjalne zagrożenia. Należy wśród nich uwzględnić również zasady udzielania pracownikom dostępu do zasobów informatycznych jednostki gospodarczej[16]. Ciągły rozwój systemów informatycznych oraz nowe technologie wymuszają poszukiwanie coraz to nowych systemów, w których można przechowywać dane. W początkowym etapie informatyzacji były to dyskietki, następnie nośniki CD/DVD, pamięci masowe, a obecnie – archiwizacja danych w chmurze[17].

Metodyka badań własnych i prezentacja wyników

Zgodnie z postanowieniami art. 10 ust. 1 UoR w zakresie stosowania polityki rachunkowości podmioty gospodarcze powinny określić metody ochrony danych oraz wszelkich zbiorów, dowodów księgowych oraz tych stanowiących podstawy zapisów księgowych. Zaproszenie do udziału w badaniach zostało kierowane do podmiotów współpracujących z kilkoma biurami rachunkowymi oraz autorami artykułu. Z uwagi na cel badań, były to jednostki zobowiązane do stosowania prawa bilansowego (UoR lub MSR/MSSF). Chęć udziału zgłosiła zdecydowana większość z nich. W efekcie powstała próba badawcza licząca 379 podmiotów gospodarczych – przede wszystkim

[14] *Rekomendacje dla programów księgowych*, Stowarzyszenie Księgowych w Polsce, https://skwp.pl/o-skwp/uslugi [dostęp: 28.04.2023].

[15] Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (2016), Dz.U. UE L 119; zob. R. Stępniewski, *Polityka haseł w firmie*, Polityka Bezpieczeństwa, 27.06.2019, https://www.politykabezpieczenstwa.pl/pl/a/polityka-hasel-w-firmie [dostęp: 28.04.2023].

[16] M. Błażejowska, *Dostosowanie funkcjonowania spółdzielni socjalnych do RODO*, „Przedsiębiorczość i Zarządzanie" 2018, t. 19, z. 4, cz. 2: *Szanse i zagrożenia dla gospodarki europejskiej XXI wieku*, s. 39–51; M. Goddard, *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*, „International Journal of Market Research" 2017, vol. 59, nr 6, s. 703–705.

[17] P. Margol, P. Dymora, M. Mazurek, *Strategie archiwizacji i odtwarzania baz danych*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Elektrotechnika" 2017, z. 36, nr 3, s. 31–41.

stosujących postanowienia UoR w zakresie sporządzania sprawozdań finansowych (jedynie nieliczne podmioty obserwowane w latach 2019–2020 stosują MSR/MSSF) (tabela 2).

Tabela 2. Liczba podmiotów stosujących wybrane postanowienia prawa bilansowego w latach 2016–2022

Rok obserwacji	Sprawozdawczość UoR/MSR	Liczba obserwacji w danym roku
2016	100% UoR	27
2017	100% UoR	37
2018	100% UoR	21
2019	85% UoR 15% MSR	125
2020	95% UoR 5% MSR	137
2021	100% UoR	18
2022	100% UoR	14
suma		379

Źródło: opracowanie własne.

Zgodnie z hipotezami badawczymi zawartymi we wstępie niniejszego artykułu postawiono następujące pytania badawcze:

P1: Czy w latach 2016–2022 podmioty w próbie badawczej wdrażały nowe rozwiązania w zakresie bezpieczeństwa danych?

P2: Jakie nowe technologie zostały wdrożone w celu poprawy bezpieczeństwa danych wśród uczestników próby badawczej będących przedmiotem obserwacji w kolejnym roku?

P3: Czy podmioty starają się wdrażać nowsze technologie w celu zabezpieczenia zbiorów danych?

P4: Czy podmioty dokonują inwestycji w infrastrukturę sieci IT, aby zapobiegać ryzyku utraty danych?

P5: Jak duże nakłady finansowe poniesiono w celu ograniczania ryzyka utraty danych?

P6: Czy pracownicy działu finansowo-księgowego znają postanowienia UoR w zakresie ochrony danych księgowych oraz ich zbiorów?

Nowe technologie były i są przedmiotem badań wielu autorów[18]. Wszyscy zgodnie dochodzą do wniosku, że cyberbezpieczeństwo jest niezwykle ważnym elementem

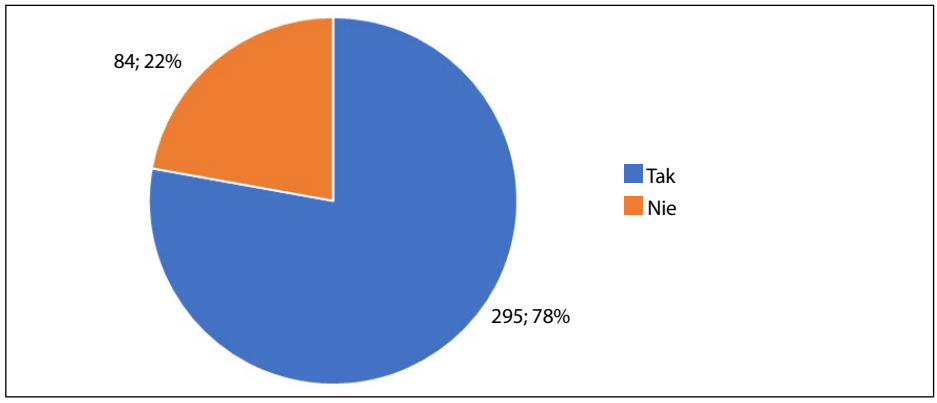
[18] T. Bąk, B. Łukaszewski, *Cyfrowe zagrożenia dla bezpieczeństwa wewnętrznego. Nowe subkultury sieciowe, wirtualna rzeczywistość, sztuczna inteligencja*, „Współczesne Problemy Zarządzania" 2020, t. 8, nr 1, s. 97–109; P. Domżał, A. Supel, P. Przybylski, *Nowoczesna technologia a wzrost cyberbezpieczeństwa – analiza zależności*, „Społeczeństwo, Kultura, Wartości. Studium społeczne" 2023, R. XIV, nr 23, s. 91–96; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1 (17), s. 15–28.

funkcjonowania każdej jednostki gospodarczej. Poszukiwanie oraz wdrażanie nowych rozwiązań powinno wiązać się z ich doskonaleniem w celu poprawy dotychczas funkcjonujących możliwości.

Niezwykle rzadkim zjawiskiem jest dziś brak posiadania jakichkolwiek zabezpieczeń przez funkcjonujące podmioty gospodarcze. Niekiedy właściciele firm decydują się również na zakup ubezpieczeń od włamań, ataków hakerskich oraz innych powiązanych zagrożeń.

Wydawać by się mogło, że w dobie postępującej cyfryzacji dbanie oraz rozwój dotychczas funkcjonującej infrastruktury IT w zakresie bezpieczeństwa danych księgowych powinno być kwestią priorytetową. Wykres nr 1 przedstawia liczbę podmiotów oraz ich udział procentowy w omawianym zakresie.

Wykres 1. Wdrożenie nowych rozwiązań w zakresie bezpieczeństwa danych księgowych w latach 2016–2022 w analizowanej próbie badawczej

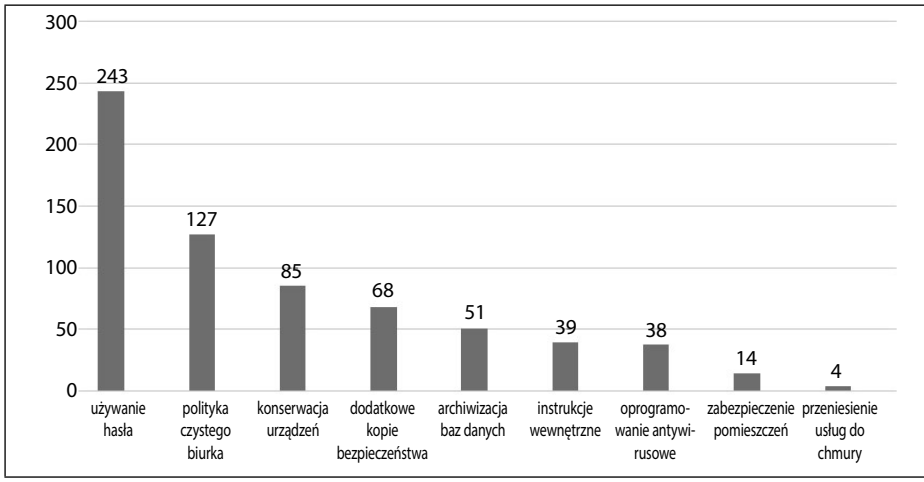


Źródło: opracowanie własne.

Przeprowadzone obserwacje wskazują, że w latach 2016–2022 w dobranej próbie badawczej 78% podmiotów dążyło do poszukiwania i wdrażania nowych rozwiązań w zakresie bezpieczeństwa danych księgowych. Niepokoić może fakt, że prawie co czwarte z badanych przedsiębiorstw w ciągu 7 lat nie dokonało żadnych uprawnień w tym obszarze. Jak wspomniano, trudno obecnie znaleźć podmiot, który nie posiada żadnych zabezpieczeń w obrębie cyberbezpieczeństwa. Można domniemywać, że takie zachowanie właścicieli i zarządzających firmami w analizowanej próbie badawczej wynika z niskiego poziomu świadomości potencjalnych zagrożeń.

Wśród podmiotów, które wdrożyły nowe technologie, postawiono pytanie, jakie konkretnie były to rozwiązania oraz którego obszaru dotyczyły. Podkreślić należy, że wybór ten nie był ograniczony do jednej możliwości, a co za tym idzie – występowały sytuacje (dość liczne) wskazań na kilka przyjętych rozwiązań.

Wykres 2. Wyszczególnienie nowych technologii wdrożonych w celu poprawy bezpieczeństwa danych w analizowanej próbie badawczej



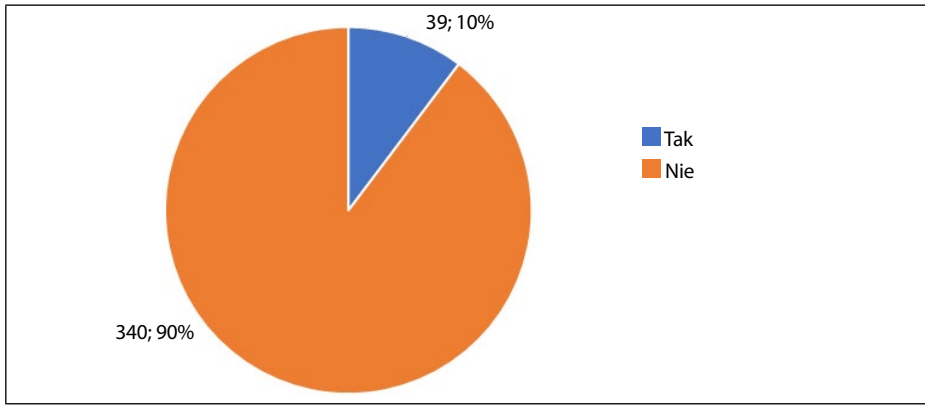
Źródło: opracowanie własne.

Jak można zaobserwować na wykresie 2, najwięcej wskazań dotyczyło używania hasła (lub wdrożenia tego rozwiązania), znaczna liczba odpowiedzi wskazywała też na wprowadzenie „polityki czystego biurka". Taki stan rzeczy może tłumaczyć obowiązywanie w Polsce od 25 maja 2018 r. rozporządzenia o ochronie danych osobowych (RODO) – obydwa ze wspomnianych powyżej rozwiązań są obligatoryjne od momentu wejścia w życie tego rozporządzenia.

Najmniej wskazań dotyczyło przeniesienia usług do tzw. chmury. Polega ono na migracji baz danych oraz całej infrastruktury na zewnątrz, co z kolei przenosi na dostawcę takich usług odpowiedzialność za wykonywanie kopii baz danych czy też innych nośników informatycznych. Jak pokazuje praktyka gospodarcza, rozwiązanie to jest dość drogie w dłuższej perspektywie, ale dla podmiotów rozpoczynających działalność może być korzystne ze względu na brak konieczności posiadania własnej, często rozbudowanej infrastruktury IT.

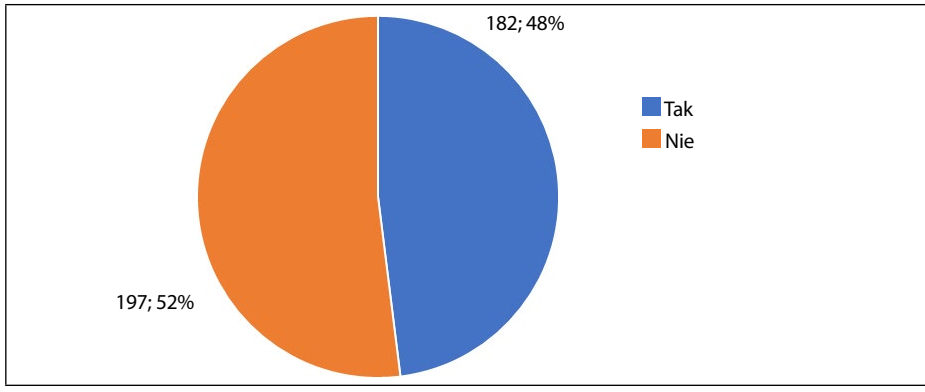
Kolejno postawiono pytanie, czy podmioty starają się wdrażać nowsze technologie w celu zabezpieczenia zbiorów danych. Co ciekawe, odpowiedź aż 340 uczestników badania, co stanowi 90% próby badawczej, można zakwalifikować jako pozytywną (wykres 3). Zjawisko to można rozpatrywać jako intrygujące: w dobie niepewności i gwałtownych wydarzeń mających miejsce na świecie (COVID-19, wojna w Ukrainie, inflacja oraz inne czynniki) podmioty starają się dążyć do zapewnienia sobie jeszcze wyższego poziomu bezpieczeństwa i do ograniczenia ryzyka utraty danych.

Wykres 3. Poszukiwanie nowych rozwiązań w zakresie poprawy bezpieczeństwa danych przez podmioty w analizowanej próbie badawczej



Źródło: opracowanie własne.

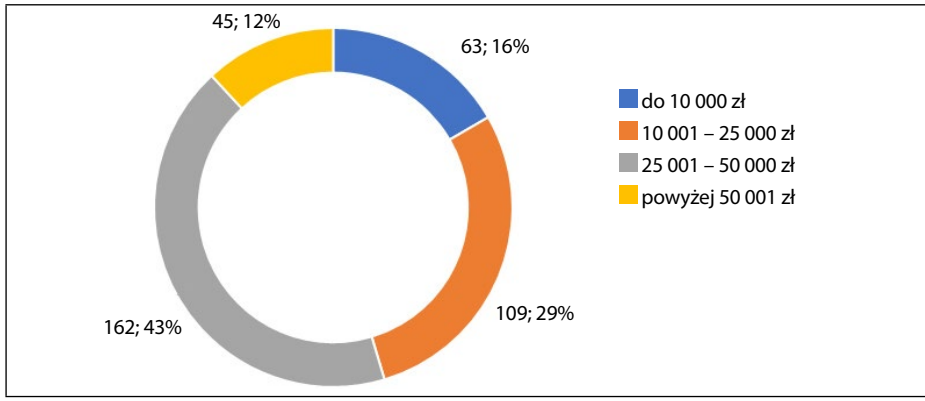
Wykres 4. Dokonywanie inwestycji w celu ograniczania ryzyka utraty danych wśród podmiotów w próbie badawczej



Źródło: opracowanie własne.

Spośród podmiotów, które udzieliły pozytywnej odpowiedzi na poprzednie pytanie, można wyszczególnić 182 jednostki, które ponadto ciągle inwestują nowe środki w rozwój infrastruktury IT związanej z poprawą zabezpieczeń zbiorów danych księgowych (wykres 4). Pozostałe 197 jednostek, co stanowi 52% podmiotów, wskazuje, że będzie bazować na rozwiązaniach, które już zostały wypracowane przez praktykę gospodarczą oraz nie są kosztowne. Obserwacji poddano również roczny poziom przewidywanych nakładów na inwestycje ograniczające ryzyko utraty danych (wykres 5).

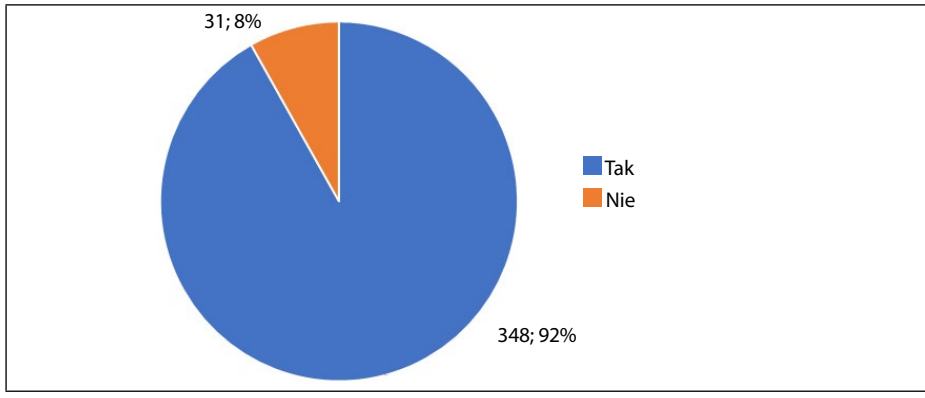
Wykres 5. Roczne nakłady finansowe na ograniczanie ryzyka utraty danych



Źródło: opracowanie własne.

Zgodnie z danymi przedstawionymi na wykresie 5, aż 43% podmiotów planujących nakłady pieniężne na poprawę bezpieczeństwa infrastruktury IT oraz ograniczanie ryzyka planuje rocznie przeznaczyć na te cele kwotę w przedziale 25 001 – 50 000 złotych. W analizowanej próbie badawczej znajdują się również podmioty (16% wszystkich obserwacji), które planują w ujęciu rocznym wygospodarować na te cele zaledwie kwotę poniżej 10 000 złotych. Zdaniem autorów artykułu kwota około 833 złote miesięcznie nie stanowi znaczącego obciążenia, patrząc przez pryzmat potencjalnych zagrożeń oraz konsekwencji wynikających z różnych aktów prawnych, szczególnie jeżeli podmiot planuje działanie w dłuższej perspektywie czasowej.

Wykres 6. Znajomość oraz świadomość stosowania rozwiązań przewidzianych w UoR w zakresie ochrony zbiorów księgowych



Źródło: opracowanie własne.

Pracownikom działów finansowo-księgowych zadano także pytanie o ich świadomość oraz umiejętność stosowania postanowień zawartych w UoR dotyczących ochrony danych zbiorów księgowych. Pozytywną odpowiedź można stwierdzić w przypadku 348 wskazań, co stanowi 92% obserwacji. Nominalnie to wysoki wynik, jednak pewnym zaskoczeniem jest fakt, że prawie co dziesiąty pracownik działu finansowo-księgowego nie zna zapisów UoR z zakresu zabezpieczenia danych księgowych, pomimo że jest to podstawowy akt normatywny regulujący prawo bilansowe w Polsce.

Podsumowanie

Problematyka zarządzania bezpieczeństwem danych, ze szczególnym uwzględnieniem danych o charakterze finansowo-księgowym, jest często podejmowanym tematem badawczym, co pozwala na bieżącą identyfikację nowo pojawiających się problemów. W efekcie liczne opracowania teoretyczne mogą być pomocne dla podniesienia poziomu bezpieczeństwa danych w organizacji.

Przeprowadzone badania wskazują, że wśród analizowanej próby badawczej stan infrastruktury IT w zakresie bezpieczeństwa oraz ochrony zbiorów księgowych znacząco się poprawił w latach 2016–2022. Po części zidentyfikowany wzrost zainteresowania kwestiami bezpieczeństwa danych księgowych był skutkiem wprowadzonego do obiegu prawnego w 2018 r. RODO. Rozporządzenie to zobowiązało wiele firm do systemowego podejścia do kwestii bezpieczeństwa danych, czego pośrednim efektem jest wzrost świadomości istnienia zagrożeń cyfrowych. Równie pozytywnie należy ocenić fakt, że mimo licznych zagrożeń, wiele podmiotów ciągle poszukuje nowych rozwiązań z zakresu bezpieczeństwa danych. Wzrost inflacji, pandemia, głębokie zmiany prawne w obszarze podatków, a w ostatnim z badanych lat – wybuch wojny, choć prowadzą do wyższego poziomu ryzyka towarzyszącego działalności gospodarczej, to jednak nie zniechęcają zarządzających do inwestycji i alokowania środków w obszar bezpieczeństwa.

Kontrowersyjną kwestią praktyczną jest przenoszenie danych do tzw. chmury, czyli środowisk wirtualnych. Z jednej strony rozwiązanie to ma swoje zalety, takie jak przeniesienie odpowiedzialności za infrastrukturę IT na zewnętrznego dostawcę, co ogranicza koszty w początkowej fazie działalności gospodarczej, z drugiej jednak – rozwiązanie to jest dość drogie jak na możliwości przedsiębiorców i realia ciągle zmieniającego się otoczenia gospodarczego.

Pomimo rosnącego dorobku nauki w tym obszarze, jak i jednoznacznie sformułowanych wymagań prawnych, część podmiotów nie wykazuje zainteresowania sprawami bezpieczeństwa danych. W praktyce gospodarczej nadal występują zarządzający przekonani o wystarczającym zabezpieczeniu zbiorów kierowanego

podmiotu. Takie przekonanie nie musi być zgodne z prawdą, a jego podstawą jest często brak wiedzy z zakresu bezpieczeństwa danych i niedostateczna świadomość istniejących zagrożeń.

Bibliografia

Baryłka A., *Podstawy inżynierii bezpieczeństwa obiektów antropogenicznych*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2015, nr 1, s. 10–16.

Bąk T., Łukaszewski B., *Cyfrowe zagrożenia dla bezpieczeństwa wewnętrznego. Nowe subkultury sieciowe, wirtualna rzeczywistość, sztuczna inteligencja*, „Współczesne Problemy Zarządzania" 2020, t. 8, nr 1, s. 97–109.

Błażejowska M., *Dostosowanie funkcjonowania spółdzielni socjalnych do RODO*, „Przedsiębiorczość i Zarządzanie" 2018, t. 19, z. 4, cz. 2: *Szanse i zagrożenia dla gospodarki europejskiej XXI wieku*, s. 39–51.

Ciesielczyk T., Stępniewski J., *Ochrona danych w systemach informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej we Wrocławiu" 1994, nr 691: *Informatyka ekonomiczna*, s. 17–23.

Domżał P., Supel A., Przybylski P., *Nowoczesna technologia a wzrost cyberbezpieczeństwa – analiza zależności*, „Społeczeństwo, Kultura, Wartości. Studium społeczne" 2023, R. XIV, nr 23, s. 91–96.

Galica B., Tomczyk-Noga B., *Atestacja systemów informatycznych rachunkowości*, „Prace Naukowe Akademii Ekonomicznej w Katowicach", 1997: *Rachunkowość w gospodarce rynkowej: nauka i praktyka. Materiały konferencyjne. Ogólnopolski Zjazd Katedr Rachunkowości, Ustroń 17–19 września 1997*, t. 1, s. 121–124.

Goddard M., *The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*, „International Journal of Market Research" 2017, vol. 59, nr 6, s. 703–705.

Klamut R., *Bezpieczeństwo jako pojęcie psychologiczne*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Ekonomia i Nauki Humanistyczne" 2012, z. 19, nr 4, s. 41–51.

Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 2 (18), s. 19–39.

Kuczyńska-Cesarz A., *Selected areas of threats to the security of accounting information system*, „Inżynieria Bezpieczeństwa Obiektów Antropogenicznych" 2021, nr 3, s. 37–49.

Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1 (17), s. 15–28.

Łojek P., *Wyzwania i odpowiedzialność biegłego rewidenta przy badaniu spółek giełdowych z WIG30*, [w:] *Wyzwania rewizji finansowej*, red. K. Chłapek, S. Krajewska, P. Zieniuk, Difin, Warszawa 2020.

Madej J., Szymczyk-Madej K., *Prawne wymogi bezpieczeństwa systemów informatycznych w polskich przedsiębiorstwach według kodeksu karnego, ustawy o rachunkowości i ustawy o ochronie danych osobowych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 770, s. 89–107.

Margol P., Dymora P., Mazurek M., *Strategie archiwizacji i odtwarzania baz danych*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Elektrotechnika" 2017, z. 36, nr 3, s. 31–41.

Qin D., *Designing an Accounting Information Management System Using Big Data and Cloud Technology*, „Scientific Programming" 2022, vol. 33, https://doi.org/10.1155/2022/7931328.

Rekomendacje dla programów księgowych, Stowarzyszenie Księgowych w Polsce, https://skwp.pl/o-skwp/uslugi [dostęp: 28.04.2023].

Schneider K., Schneider K., *Zagrożenia w funkcjonowaniu jednolitego pliku kontrolnego*, „Ekonomiczne Problemy Usług" 2018, nr 2 (131), t. 1, s. 323–330.

Spychała T., *Rozwój rachunkowości a cyberprzestrzeń w społeczeństwie sieci*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze" 2019, nr 11, s. 109–118.

Stępniewski R., *Polityka haseł w firmie*, Polityka Bezpieczeństwa, 27.06.2019, https://www.politykabezpieczenstwa.pl/pl/a/polityka-hasel-w-firmie [dostęp: 28.04.2023].

Szczepankiewicz E.I., *Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań*, „Zeszyty Teoretyczne Rachunkowości" 2018, t. 97, nr 153, s. 115–138.

Szymczyk-Madej K., Madej J., *Bezpieczeństwo informatycznych systemów rachunkowości*, „Zeszyty Naukowe Akademii Ekonomicznej w Krakowie" 2000, nr 553, s. 161–177.

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (2016), Dz.U. UE L 119.

Ustawa z dnia 29 września 1994 r. o rachunkowości, tekst jedn. Dz.U. z 2021 r., poz. 217.

Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, tekst jedn. Dz.U. z 2022 r., poz. 1009.

Praktyka bezpieczeństwa danych w systemie rachunkowości w świetle badań empirycznych
Streszczenie

Zmieniające się otoczenie gospodarcze podmiotów prowadzących działalność wymusza na ich właścicielach oraz osobach zarządzających ciągłe dbanie o bezpieczeństwo danych. O ile przepisy prawa bilansowego nie zmieniły się znacząco od momentu ich pierwotnego wprowadzenia do stosowania (w 1994 r.), to praktyka gospodarcza wypracowała różne metody mające na celu ochronę zbioru danych księgowych.

Niniejszy artykuł składa się z części teoretycznej oraz empirycznej, a jego głównym celem jest prezentacja badań przeprowadzonych wśród wybranych podmiotów gospodarczych w zakresie tego, jak w praktyce stosują one postanowienia ustawy o rachunkowości dotyczące ochrony danych księgowych.

Wykorzystano metody badawcze takie jak analiza i krytyka piśmiennictwa i wyników badań naukowych oraz wnioskowanie statystyczne.

Słowa kluczowe: ochrona danych księgowych, poprawa bezpieczeństwa, znajomość rozwiązań dotyczących bezpieczeństwa

Data security practice in the accounting system in the light of empirical research
Abstract

The changing economic environment of business entities forces owners and managers to constantly care about data security. While the provisions of the accounting law have not

changed significantly since their initial implementation (in 1994), economic practice has developed various methods to protect the set of accounting data.

This article consists of a theoretical and an empirical part, and its main goal is to present research conducted among selected business entities in terms of how they apply the provisions of data protection of the Act on Accounting in practice.

Research methods such as analysis and criticism of literature and research results, and statistical inference were used.

Keywords: protection of accounting data, improvement of security, knowledge of security solutions

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-008
Data wpłynięcia: 13.06.2023
Data akceptacji: 6.10.2023

Mariusz Grzyb

mgr inż., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0001-8439-9650

Marta Woźniak-Zapór

dr inż., Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0002-7773-2408

Bezpieczeństwo danych w małej firmie – wybór rozwiązań chmurowych

Wprowadzenie

W ostatnich latach widoczny jest efekt znacznej cyfryzacji procesów biznesowych. Dodatkowym mechanizmem powodującym przyspieszenie tego procesu była bezsprzecznie pandemia COVID-19 oraz wojna na Ukrainie. Cyfryzacja procesów biznesowych jest więc dziś jednym z aspektów zarządzania współczesną organizacją[1]. W związku z aktualnymi przepisami dotyczącymi ochrony danych, ważnym elementem zarządzania w organizacji staje się zarządzanie ochroną danych. Dlatego sposób przetwarzania danych w firmie się zmienia. Coraz częściej firmy wybierają rozwiązania chmurowe. Przy zarządzaniu ochroną danych w przedsiębiorstwie[2]

[1] A.E. Sawicka, *Cyberbezpieczeństwo jako współczesne wyzwanie w zarządzaniu małym i średnim przedsiębiorstwem*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie" 2022, nr 47, s. 43–59, https://znz.pcz.pl/fcp/uGBUKOQtTKlQhbx08SlkTUQJEUWRuHQwFDBoIVURNWHlBG1gnBVcoFW8SBDRKTxMWRxcBFyUJT1hLd1kIU0FYMA/_users/code_BEFIYKhdNJlY7HgMxDRFLAVVDMzgvF0MSBQ/znz/zeszyty/47/47_4.pdf [dostęp: 18.05.2023].

[2] W naukach o zarządzaniu pojęcia „firma" i „przedsiębiorstwo" są traktowane jak synonimy i stosowane zamiennie.

należy zwrócić uwagę na wybór odpowiedniego rozwiązania, które umożliwi bezpieczne funkcjonowanie i prowadzenie działalności.

Zarządzanie bezpieczeństwem. Pojęcie cyberbezpieczeństwa

Jedna z definicji bezpieczeństwa mówi, że jest ono „pewnym stanem obiektywnym, polegającym na braku zagrożenia, odczuwanym subiektywnie przez jednostki i grupy. Oznacza to, że bezpieczeństwo składa się z dwóch elementów, obiektywnego i subiektywnego. Pierwszy z nich, mający charakter obiektywny, jest zewnętrzny w stosunku do jednostki, grupy społecznej, zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa"[3]. Przeciwieństwem bezpieczeństwa jest stan, w którym występuje poczucie zagrożenia. Bezpieczeństwo ma dynamiczny charakter, zmienny w zależności od wieloczynnikowych zjawisk o charakterze obiektywnym i subiektywnym[4]. Inna definicja, bardziej ogólna, mówi, że bezpieczeństwo „obejmuje zaspokojenie takich potrzeb jak: istnienie, przetrwanie, całość, tożsamość (identyczność), niezależność, spokój, posiadanie i pewność rozwoju. Brak bezpieczeństwa powoduje niepokój i poczucie zagrożenia. Biorąc pod uwagę poczucie tego zagrożenia, w nauce wyróżnia się bezpieczeństwo wewnętrzne i bezpieczeństwo zewnętrzne. Bezpieczeństwo wewnętrzne oznacza stabilność i harmonijność danego organizmu lub podmiotu, natomiast bezpieczeństwo zewnętrzne – brak zagrożenia ze strony innych podmiotów lub czynników zewnętrznych"[5]. Bezpieczeństwo – zgodnie z innym podejściem – „jest to sytuacja odznaczająca się brakiem ryzyka, np. w inwestowaniu, planach strategicznych produktu itp., albo zasobach materialnych i ludzkich"[6].

W literaturze spotkać można także liczne definicje bezpieczeństwa informacji. Może ono być definiowane jako „obrona [...], która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych"[7]. Bezpieczeństwo definiowane jest też jako obrona informacyjna, w skład której wchodzą liczne przedsięwzięcia, w tym zapobieganie, odstraszanie,

---

3 H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, European Association for Security, Kraków 2004, s. 10.

4 J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, s. 166; K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2 (2), s. 7–23.

5 K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 9.

6 W. Šmid, *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000, s. 50.

7 L. Ciborowski, *Walka informacyjna*, Europejskie Centrum Edukacyjne, Wydawnictwo Adam Marszałek, Toruń 1999, s. 186.

wskazywanie i ostrzeganie, wykrywanie, przygotowanie się na sytuację awaryjną i reakcję na ewentualny atak[8]. Bezpieczeństwo informacji to także działanie zmierzające do zabezpieczenia zgromadzonych informacji poddawanych jakiemukolwiek przetwarzaniu, przechowywaniu czy udostępnianiu z wykorzystaniem komputerów w sieciach teleinformatycznych[9].

„Krajowe systemy teleinformatyczne wraz z przetwarzanymi w nich zasobami informacyjnymi, połączone rozległymi sieciami komputerowymi stanowią cyberprzestrzeń. W cyberprzestrzeni realizowane są usługi cyfrowe obywateli – jako społeczeństwa informacyjnego, podmiotów gospodarczych i różnych organizacji, usługi wspomagające działalność administracji i podmiotów realizujących zadania publiczne. Równolegle do realizowanych działań o charakterze rozwojowym, w cyberprzestrzeni realizowane są szkodliwe działania i działalność przestępcza, wywołująca ogromne szkody procesowe, finansowe, społeczne, w tym ograniczenie wzajemnego zaufania"[10]. Cyberbezpieczeństwo rozumiane może być jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"[11]. Cyberbezpieczeństwo jest także „ogółem technik, procesów oraz praktyk, które stosuje się w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami lub dostępem nieautoryzowanym. [...] Cyberbezpieczeństwo to także zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni"[12].

Zarządzanie bezpieczeństwem organizacji jest procesem złożonym, który powinien obejmować wszystkie sfery i kierunki działania i rozwoju organizacji[13]. „System bezpieczeństwa organizacji jest to celowo zaprojektowany i zorganizowany układ materialny, zespołów ludzkich i informacyjny (ideowy) eksploatowany przez człowieka, służący zachowaniu założonego poziomu oddziaływania zróżnicowanych zagrożeń (ryzyka) w celu zachowania bytu organizacji w postaci zapewnienia niezbędnych zasileń i samodzielnego kształtowania możliwości jej rozwoju w danych warunkach

---

8 M. Jabłoński, M. Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, red. M. Kwieciński, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2010, s. 25.

9 P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 71.

10 G. Mąkosa, *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, „Studia Bezpieczeństwa Narodowego" 2020, R.10, nr 17, s. 123, https://doi.org/10.37055/SBN/144283.

11 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560 ze zm., art. 2, pkt 4.

12 K. Wojciechowska, *Cyberbezpieczeństwo – definicja*, ISPortal, 3.01.2023, https://isportal.pl/cyberbezpieczenstwo-definicja [dostęp 12.05.2023].

13 M. Huczek, *Problematyka zarządzania bezpieczeństwem w organizacjach samorządu terytorialnego i szkołach wyższych*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie" 2010, nr 2, s. 96–102.

otoczenia"[14]. Zarządzanie bezpieczeństwem powinno pozwalać na utrzymanie poczucia bezpieczeństwa wśród interesariuszy procesów (również tych związanych z cyberbezpieczeństwem) w organizacji na wysokim poziomie.

Uwarunkowania prawne w zakresie cyberbezpieczeństwa

W strategii zarządzania cyberbezpieczeństwem należy uwzględnić wytyczne zawarte w obowiązujących ustawach, dyrektywach, rozporządzaniach oraz zasady i rekomendacje opracowywane przez organizacje zajmujące się cyberbezpieczeństwem[15]. Są to:

- Rozporządzenie o ochronie danych osobowych (RODO)[16],
- Ustawa o krajowym systemie cyberbezpieczeństwa[17],
- Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[18].

Dla firm prowadzących swoją działalność z uwzględnieniem powyższych wytycznych ważną informacją jest ogłoszenie nowej dyrektywy UE, skrótowo nazywanej NIS2[19]. Pierwsza dyrektywa NIS (Network and Information Systems Directive)[20] zawierała definicję założeń cyberbezpieczeństwa dla państw będących członkami Unii Europejskiej. Na jej podstawie 28 sierpnia 2018 r. wdrożona została zmiana Ustawy o krajowym systemie cyberbezpieczeństwa. Projekt dyrektywy NIS2 został

[14] M. Kwieciński, *Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki*, „Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie" 2016, nr 70, s. 154–155.

[15] M. Kibil, I. Piecuch, *Cyberbezpieczeństwo a praca zdalna*, „Monitor Prawniczy" 2020, nr 20, dodatek: *Prawo nowych technologii – dane osobowe i prywatność, cyberbezpieczeństwo, handel elektroniczny, innowacje, internet i media, prawo IT*, red. X. Konarski, https://iuscase.pl/cyberbezpieczenstwo-a-praca-zdalna [dostęp 12.05.2023].

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE L 119 z 4 maja 2016 r. ze zm. [dalej: RODO].

[17] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, *op. cit.*

[18] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, tekst jedn. Dz.U. z 2017 r., poz. 2247.

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz. UE L 333 z 27 grudnia 2022 r.

[20] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19 lipca 2016 r.

opublikowany 16 grudnia 2020 r., natomiast 27 grudnia 2022 r. dyrektywa NIS2 zastąpiła dyrektywę NIS.

Bezpieczeństwo danych w firmie – pierwsze kroki

W ramach prac nad zabezpieczeniem danych w małej firmie, zazwyczaj w pierwszej kolejności realizowane są zalecenia określone w RODO, wprowadzone Ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[21]. Ustawa weszła w życie 4 maja 2019 r.

W pierwszej kolejności należy dokonać analizy przetwarzanych w firmie danych. Na tej podstawie możliwe będzie wykonanie rejestru czynności przetwarzania. Zgodnie z artykułem 30 RODO[22] w rejestrze tym zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Ustęp 2 tego artykułu określa, co powinien zawierać rejestr kategorii czynności przetwarzania. Obydwa przypadki nie dotyczą jednak przedsiębiorstw zatrudniających mniej niż 250 osób, „chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10”[23].

---

[21] Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. z 2019 r., poz. 730.

[22] RODO, art. 30, ust. 1.

[23] RODO, art. 30, ust. 5.

Kolejnym krokiem jest analiza ryzyka oraz zaplanowanie środków mających na celu zapobieganie zagrożeniom. Następnie, na podstawie pełnej wiedzy na temat przetwarzanych danych, osobach odpowiedzialnych za przetwarzanie konkretnych danych na różnych etapach działalności firmy, sposobów przetwarzania, powierzania danych, a także możliwych ryzykach, stworzona może być polityka bezpieczeństwa. Jeżeli dane przetwarzane są w wersji cyfrowej, powinna powstać instrukcja zarządzania systemami informatycznymi do przetwarzania danych. W przypadku współpracy z innymi podmiotami, w ramach której dochodzi do możliwości przetwarzania danych, należy z taką firmą podpisać umowę powierzenia przetwarzania danych i informację o tym wprowadzić do rejestru powierzeń danych.

Bezpieczeństwo danych w chmurze – przykład wdrożenia w małej firmie

Jak już wspomniano – cyfryzacja procesów biznesowych doprowadziła do upowszechnienia rozwiązań chmurowych w zakresie przechowywania danych w firmach. Ważnym czynnikiem, który napędzał przejście z rozwiązań tradycyjnych do chmury, była w dużej mierze pandemia COVID-19. Obecnie – w okresie spowolnienia gospodarczego i wojny w Ukrainie – również widać wśród przedsiębiorców zainteresowanie rozwiązaniami chmurowymi. Ma na to wpływ zmieniający się rynek i przejście na pracę zdalną w okresie pandemii oraz ostatnie zmiany w polskim prawie. Pokazały to wyraźnie badania przeprowadzone od października do grudnia 2022 r. przez Deloitte[24]. Przechowywanie danych w chmurze staje się coraz popularniejsze ze względu na dużą oszczędność czasu i pieniędzy. Umieszczenie plików (zdjęć, filmów, muzyki, dokumentów) w chmurze zapewnia łatwy dostęp do danych praktycznie z dowolnego miejsca i urządzenia, które podłączone jest do Internetu.

W związku z tym przeanalizowano siedem oferowanych na polskim rynku rozwiązań chmurowych, wybranych z uwagi na dużą popularność, jaką cieszą się wśród użytkowników – głównie dzięki prostocie użytkowania. Dla przedsiębiorców korzystających z dysków chmurowych ogromną zaletą jest możliwość synchronizacji plików pomiędzy poszczególnymi urządzeniami czy pracownikami. Funkcja ta doskonale sprawdza się w przypadku korzystania z więcej niż jednego urządzenia. Wcześniej konieczne było przenoszenie danych – obecnie najczęściej robi się to automatycznie, a synchronizacja pozwala na aktualizację zawartości chmury w bardzo krótkich czasie. Przedstawione przez nas usługi przechowywania danych w chmurze posiadają opcje bezpłatnych pakietów oraz bardziej zaawansowane usługi płatne – producenci oferują różnego rodzaju pakiety z opcjami dodatkowymi. Na samym początku trzeba się

[24] *The CFO Programme. 2023 Central Europe CFO Survey*, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/cfo/CE_CFO_2023_Report.pdf [dostęp 12.05.2023].

jednak zastanowić, ile miejsca w chmurze tak naprawdę wykorzystamy. Przeciętnie pracownik, który zamierza przechowywać w sieci dane firmowe, powinien rozejrzeć się za opcją oferującą 100–200 GB. To przestrzeń, która powinna mu w zupełności wystarczyć. Osoby, które pracują na wielu dużych plikach, wybiorą pakiety o pojemności 1–2 TB.

Charakterystyka wybranych rozwiązań chmurowych

Dysk Google (Google Drive) – obecnie jedna z najpopularniejszych usług do przechowywania danych w chmurze. Bierze się to stąd, że wszyscy użytkownicy popularnej usługi pocztowej Gmail oraz systemu operacyjnego na urządzenia mobile Android muszą mieć aktywne konto Google. Posiadając konto Google, jesteśmy automatycznie posiadaczami Dysku Google i w wersji podstawowej mamy do dyspozycji 15 GB na dane. Użytkownicy najczęściej wykorzystują przyznaną im przestrzeń do tworzenia kopii zapasowych, przechowywania dokumentów, zdjęć, filmów, muzyki. Producent zadbał również o współdzielenie zasobów, wspólną pracę oraz synchronizację z różnego typu urządzeniami.

Microsoft OneDrive – jest doskonałym wyborem dla użytkowników pakietu Office 365. Otrzymują oni bezpłatnie 1 TB przestrzeni dyskowej z dodatkowymi funkcjami. Można też skorzystać z bardzo dobrej oferty na samą przestrzeń na dane przechowywane w chmurze. Współdzielenie zasobów, wspólna praca i synchronizacja danych to dopełnienie tego zestawu.

Dropbox – jedno z pierwszych rozwiązań dla klientów biznesowych. Dropbox oferuje świetną integracje z aplikacjami firm Microsoft i Adobe. Posiada również rozbudowane opcje zabezpieczeń przed utratą danych. W wersji bezpłatnej oferowana przestrzeń jest bardzo skromna w porównaniu z konkurencyjnymi rozwiązaniami: zaledwie 2 GB. Producent zdecydowanie jest tu nastawiony na klienta biznesowego.

Apple iCloud Drive – skierowany głównie do użytkowników innych produktów firmy Apple, ponieważ jest zaimplementowany zarówno w systemie macOS, jak i iOS. Oczywiście możemy go używać w innych środowiskach, ale jest to mało popularne rozwiązanie poza urządzeniami Apple.

Box – jest dyskiem oferującym przestrzeń chmurową do przechowywania plików dla osób indywidualnych i biznesu. Mimo dobrze działającej aplikacji do synchronizacji nie oferuje nic, czym mógłby się wyróżnić na tle konkurencyjnych rozwiązań.

Mega – oferta z korzystnymi rozwiązaniami chmurowymi. Najważniejszym atutem jest bezpieczeństwo. Szyfrowanie typu end-to-end chroni zasoby użytkowników nawet podczas przesyłania pomiędzy urządzeniem końcowym a serwerem. Mega udostępnia każdemu użytkownikowi klucze do szyfrowania, co chroni przed niepowołanym dostępem. Niestety utrata klucza uniemożliwia odzyskanie danych.

Sync – łatwe w użyciu i niedrogie rozwiązanie do przechowywania danych w chmurze. Sync oferuje bezpłatnie 5 GB miejsca oraz przesyłanie plików bez

ograniczenia. Zastosowane szyfrowanie zapewnia prywatność i nieograniczone plany przechowywania danych. Jednak użytkownicy mogą odczuwać spowolnienie kompleksowym szyfrowaniem i ograniczoną integracją aplikacji innych firm.

W tabeli 1 przedstawione zostało zestawienie najważniejszych parametrów rozwiązań chmurowych wybranych do analizy.

Tabela 1. Darmowa przestrzeń na dane w chmurze

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Darmowa przestrzeń	15 GB	5 GB	2 GB	5 GB	10 GB	20 GB	5 GB

Źródło: zestawienie na podstawie materiałów dostawców.

Jeśli chodzi o wielkość przestrzeni na dane, przodującym rozwiązaniem jest więc Mega, oferujące 20 GB bezpłatnego miejsca. Drugi pod tym względem jest Dysk Google, a trzeci – Box.

Tabela 2. Zestawienie planów płatnych, wielkości przestrzeni na dane w chmurze wraz z ich cenami oraz średnią ceną za 1 TB*

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Przestrzeń na dane w planach płatnych	30 GB 1 użytkownik 27 zł/miesięcznie 2 TB 1 użytkownik 54 zł/miesięcznie 5 TB 1 użytkownik 54 zł/miesięcznie	1 TB 1 użytkownik od 21 do 52 zł/miesięcznie (cena uzależniona od pakietu z dodatkowymi aplikacjami)	3 TB 1 użytkownik 75 zł/miesięcznie 5 TB min. 3 użytkowników 54 zł/miesięcznie bez limitu min. 3 użytkowników 81 zł/miesięcznie	50 GB 1 użytkownik 4,50 zł/miesięcznie 200 GB 1 użytkownik 13,50 zł/miesięcznie 2 TB 1 użytkownik 45 zł/miesięcznie	100 GB 1 użytkownik 54 zł/miesięcznie 100GB min. 3 użytkowników 27 zł/miesięcznie bez limitu min. 3 użytkowników od 81 zł/miesięcznie	Minimalny pakiet dla firm 3 TB 3 użytkowników 68 zł/miesięcznie	2 TB 1 użytkownik 36 zł/miesięcznie 6 TB 1 użytkownik 90 zł/miesięcznie
Średni koszt 1 TB na dane w chmurze	27 zł	21 zł	25 zł	22,50 zł	25 zł	22,60 zł	18 zł

* Warunki oferty i ceny z dnia 28.05.2023 r.
Źródło: zestawienie na podstawie materiałów dostawców.

Najtańszym pod względem średniej ceny za 1 TB danych jest Sync – z najbardziej ubogimi parametrami, jeśli chodzi dane przechowywane w chmurze (tabela 2). Najdroższym rozwiązaniem w tym zestawieniu jest Dysk Google, w którym oprócz miejsca na dane dostajemy pokaźną dawkę aplikacji do wykorzystania, takich jak np. Dokumenty, Arkusze czy Prezentacje. Podobnie wyposażony pakiet Microsoft 365 Business Basic otrzymamy już za 25,20 zł[25].

Tabela 3. Historia przechowywanych plików w chmurze, kompatybilność z systemami operacyjnymi

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Historia plików*	30 dni	30 dni	180 dni	–	–	od 30 do 365 dni	od 180 do 365 dni
Aplikacje na komputer stacjonarny	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS	Windows MacOS
Aplikacje na urządzenia mobilne wraz z ocenami Google Play	Android (4,2)	Android (4,7)	Android (4,3)	Android (3,8)	Android (4,5)	Android (4,4)	Android (3,8)

* Czas na przywrócenie usuniętych plików lub cofnięcie wprowadzonych zmian.
Źródło: zestawienie na podstawie materiałów dostawców.

Wszystkie przedstawione w tabeli 3 rozwiązania mogą być stosowane z systemem operacyjnym Windows i MacOS w przypadku komputerów stacjonarnych oraz Android na urządzeniach mobilnych.

W tabeli 4 przedstawiono porównanie usług pod względem szyfrowania danych, zgodności z RODO i korzystania z weryfikacji dwuetapowej.

Tabela 4. Parametry szyfrowania, zgodność usługi z wymogami RODO oraz dostępność weryfikacji dwuetapowej

Badany parametr	Dysk Google	Microsoft OneDrive	Dropbox	Apple iCloud	Box	Mega	Sync
Szyfrowanie	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Zgodny z RODO	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Weryfikacja dwuetapowa	Tak	Tak	Tak	Tak	Tak	Tak	Tak

Źródło: zestawienie na podstawie materiałów dostawców.

Opis badania

Badanie zostało przeprowadzone między wrześniem 2022 a kwietniem 2023 r. w Krakowie, w małej firmie zatrudniającej siedem osób. Do badania wykorzystano siedem

[25] Ceny z dnia 28.05.2023 r.

komputerów stacjonarnych, w tym trzy z zainstalowanym systemem operacyjnym Windows 10 oraz cztery z Windows 11. Każdy z komputerów miał zainstalowany pakiet biurowy Microsoft Office 2021, program antywirusowy ESET oraz przeglądarki Microsoft Edge, Google Chrome, Mozilla Firefox i aplikację dedykowaną do danego dysku chmurowego. W badaniu wykorzystane zostały również telefony pracowników z systemem Android, na których zainstalowane zostały aplikacje poszczególnych producentów. Do siedziby firmy doprowadzony jest światłowód i wykupiony pakiet internetowy pozwalający na osiągnięcie 2 Gb/s przy pobieraniu i 1 Gb/s przy wysyłaniu. Urządzania sieciowe są dostosowane do wyższych prędkości, niż wskazały testy szybkości łącza, a okablowanie wewnątrz firmy jest przynajmniej kategorii 6. Testy prędkości były wykonywane jednocześnie na wszystkich komputerach w firmie. Dane przetwarzane przez pracowników mieszczą się w przedziałach od 200 do 700 MB. Część danych wykorzystywanych w badaniu była współdzielona przez użytkowników. Każdy z pracowników miał założone indywidualne konto w każdej usłudze, wykorzystano pakiety bezpłatne. Badanie prowadzono na każdym oprogramowaniu, które zostało ujęte w opisie, przez około 30 dni (20 dni roboczych).

W wywiadach przeprowadzonych z użytkownikami po badaniu ustalono, że praca przebiegała płynnie, nie było problemów z synchronizacją danych. Współdzielone dane pojawiały się folderach na wszystkich komputerach i telefonach bez zauważalnych opóźnień. Aplikacje do synchronizacji danych pracowały w tle, nie powodowały opóźnienia w zapisie ani spowolnienia pracy komputerów.

Po zakończonym badaniu właściciel firmy zdecydował się na zastosowanie na stałe chmury Mega. Głównym argumentem, dla którego został wybrany ten konkretny pakiet, było to, że ma on zastosowane klucze szyfrujące i dane na serwerach są zaszyfrowane. Jest to informacja zdecydowanie premiująca to rozwiązanie w stosunku do pozostałych. Wszystkie dane w Mega są szyfrowane kluczami generowanymi na podstawie hasła użytkownika. To jest główny klucz szyfrowania. To, co sprawia, że jest to tak bezpieczne, to fakt, że nikt oprócz samego użytkownika nie ma dostępu do hasła. Mega nie posiada klucza deszyfrującego, a dane na ich serwerach przechowywane są w postaci zaszyfrowanej. Posiadacz klucza deszyfrującego, czyli użytkownik, decyduje, kto i jak może uzyskać dostęp do danych. W Mega przywrócenie dostępu do własnego konta jest to możliwe jedynie za pomocą klucza odzyskiwania. Klucz odzyskiwania chroni również konto przed cyberatakami. Takie bezkompromisowe podejście do bezpieczeństwa oznacza, że Mega nie wysyła linków do resetowania haseł. To niestety oznacza problem, gdy użytkownik zapomni hasło. Jedynym sposobem na odzyskanie dostępu do konta w Mega jest posiadanie klucza odzyskiwania. Należy więc pamiętać o tym, aby klucz odzyskiwania był przechowywany w bezpiecznym miejscu. Dodatkowym bardzo dobrym rozwiązaniem jest udostępnianie linków – domyślnie klucz deszyfrujący jest wysyłany razem z nimi, ale można zwiększyć bezpieczeństwo i wybrać eksport i wysyłanie

klucza deszyfrującego oddzielnie. Użytkownik, który otrzyma łącze, musi wprowadzić klucz, zanim będzie mógł je otworzyć. Rozwiązanie to dobrze się sprawdza przy udostępnianiu zasobów z danymi osobowymi. Mega wspiera również dwuskładnikowe uwierzytelnianie (2FA). Jest to dodatkowa warstwa ochrony konta. Po włączeniu 2FA, za każdym razem, gdy użytkownik loguje się lub dokonuje zmian na swoim koncie, musi wprowadzić 6-cyfrowy kod z aplikacji uwierzytelniającej.

Podsumowanie

Przedstawione zostały aktualne zagadnienia związane z problemami zarządzania bezpieczeństwem – w tym bezpośrednio cyberbezpieczeństwem. Jest to niezwykle istotne z uwagi na rozwój cyfryzacji w każdej dziedzinie życia, także – a może szczególnie – w procesach biznesowych. Obecnie trudno sobie wyobrazić jakąkolwiek organizację, która nie przetwarza danych w sposób cyfrowy. W niektórych przypadkach inny sposób byłby nawet niemożliwy z uwagi na ilość tych danych lub sposób prowadzenia działalności. Zapewnienie bezpieczeństwa danych i informacji staje się ważnym elementem strategii zarządzania bezpieczeństwem w organizacjach. Obowiązujące przepisy prawa regulują obowiązki podmiotów związane z bezpieczeństwem przetwarzanych danych. W obliczu coraz szerszych możliwości naruszenia bezpieczeństwa danych – ze względu na szybki rozwój technologiczny nieprzewidzianych wcześniej – przepisy te są aktualizowane i zaostrzane.

Ważnym zagadnieniem jest bezpieczeństwo rozwiązań chmurowych, które są coraz częściej wybierane jako alternatywa dla przechowywania danych na serwerach firmowych. Wybór konkretnego rozwiązania nie jest łatwy: oprócz ceny, wielkości miejsca na przechowywanie danych czy wygody podczas użytkowania, szczególną uwagę należy zwrócić na zapewnienie bezpieczeństwa. Odpowiedzialność za zapewnienie bezpieczeństwa serwera leży na dostawcy rozwiązania chmurowego. Natomiast odpowiedzialność za bezpieczne przetwarzanie danych tam zawartych spoczywa już na firmie, która z takiego rozwiązania korzysta. Dlatego warto z rozwagą wybierać rozwiązanie chmurowe, przy zapewnieniu odpowiednich mechanizmów zarządzania bezpieczeństwem w organizacji.

Bibliografia

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

The CFO Programme. 2023 Central Europe CFO Survey, Deloitte, https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/cfo/CE_CFO_2023_Report.pdf [dostęp 12.05.2023].

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2 (2), s. 7–23.

Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Wydawnictwo Adam Marszałek, Toruń 1999.

Huczek M., *Problematyka zarządzania bezpieczeństwem w organizacjach samorządu terytorialnego i szkołach wyższych*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie" 2010, nr 2, s. 96–102.

Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, red. M. Kwieciński, Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM, Kraków 2010, s. 23–38.

Kibil M., Piecuch I., *Cyberbezpieczeństwo a praca zdalna*, „Monitor Prawniczy" 2020, nr 20, dodatek: *Prawo nowych technologii – dane osobowe i prywatność, cyberbezpieczeństwo, handel elektroniczny, innowacje, internet i media, prawo IT*, red. X. Konarski, https://iuscase.pl/cyberbezpieczenstwo-a-praca-zdalna [dostęp 12.05.2023].

Korzeniowska H., *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, European Association for Security, Kraków 2004.

Kwieciński M., *Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki*, „Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie" 2016, nr 70, s. 149–170.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Mąkosa G., *Zarządzanie bezpieczeństwem krajowych systemów teleinformatycznych*, „Studia Bezpieczeństwa Narodowego" 2020, R.10, nr 17, s. 129–146, https://doi.org/10.37055/SBN/144283.

Sawicka A.E., *Cyberbezpieczeństwo jako współczesne wyzwanie w zarządzaniu małym i średnim przedsiębiorstwem*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie" 2022, nr 47, s. 43–59, https://znz.pcz.pl/fcp/uGBUKOQtTKlQhbx08SlkTUQJEUWRuHQwFDBoIVURNWHlBG1gnBVcoFW8SBDRKTxMWRxcBFyUJT1hLd1kIU0FYMA/_users/code_BEFIYKhdNJlY7HgMxDRFLAVVDMzgvF0MSBQ/znz/zeszyty/47/47_4.pdf [dostęp: 18.05.2023].

Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.

Šmid W., *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu Kraków 2000.

Wojciechowska K., *Cyberbezpieczeństwo – definicja*, ISPortal, 3.01.2023, https://isportal.pl/cyberbezpieczenstwo-definicja [dostęp 12.05.2023].

Akty prawne

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, tekst jedn. Dz.U. z 2017 r., poz. 2247.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE L 119 z 4 maja 2016 r. ze zm.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19 lipca 2016 r.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2018 r., poz. 1560 ze zm.

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. z 2019 r., poz. 730.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.Urz. UE L 333 z 27 grudnia 2022 r.

Bezpieczeństwo danych w małej firmie – wybór rozwiązań chmurowych
Streszczenie

W związku z rozwojem cyfryzacji praktycznie w każdej dziedzinie życia, cyfryzacji podlegają również procesy biznesowe. Konieczność ochrony danych, dodatkowo w zgodzie z obowiązującymi przepisami, nastręcza wielu problemów. Szczególnym przypadkiem jest kwestia cyberbezpieczeństwa w aspekcie rozwiązań chmurowych. W opracowaniu przedstawione zostały zagadnienia dotyczące bezpieczeństwa informacji, cyberbezpieczeństwa, zarządzania bezpieczeństwem, wdrażania RODO, a także wyboru rozwiązania chmurowego na przykładzie małej firmy.

Słowa kluczowe: bezpieczeństwo informacji, cyberbezpieczeństwo, zarządzanie bezpieczeństwem, RODO, rozwiązania chmurowe

Data security in a small company: choosing cloud solutions
Abstract

With the development of digitalisation in virtually every area of life, business processes are also being digitised. The need to protect data, additionally in accordance with applicable regulations, poses many problems. A special case is the issue of cyber security in terms of cloud solutions. This paper presents issues relating to information security, cyber security, security management, implementation of GDPR and the choice of a cloud solution based on the example of a small company.

Key words: information security, cyber security, security management, GDPR, cloud solutions

Varia

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-009
Data wpłynięcia: 3.04.2023
Data akceptacji: 25.09.2023

Tomasz Banasik

dr, Politechnika Świętokrzyska, Stowarzyszenie Aktywności Zawodowej „PASSA" w Kielcach
https://orcid.org/0000-0002-5646-829X

Katarzyna Banasik

mgr, Stowarzyszenie Aktywności Zawodowej „PASSA" w Kielcach

Działalność organizacji pozarządowych na rzecz poprawy obronności państwa. Studium przypadku

Wprowadzenie

Agresja Rosji na Ukrainę w lutym 2022 r. potwierdziła roszczeniową politykę Kremla, który dąży do odbudowy swoich wpływów w państwach Europy Środkowo-Wschodniej. Rok po rozpoczęciu działań wojennych nie ulega wątpliwości, że wojna będzie trwać – obliczona na wyczerpanie zasobów ludzkich, gospodarczych i finansowych przeciwnika. Jej skutki będzie odczuwać cały świat, w tym Polska.

Konflikt zbrojny za wschodnią granicą implikował szereg inicjatyw polskiego rządu w zakresie zwiększenia działań na rzecz obronności kraju. 23 kwietnia 2022 r. weszła w życie ustawa o obronie Ojczyzny, która kodyfikuje znajdujące się dotychczas w różnych ustawach przepisy prawa wojskowego. Ustawa zwiększyła nakłady państwa na obronność, wprowadziła modernizację techniczną wojska, nowy podział służby wojskowej i reformę administracji wojskowej[1]. Niezwłocznie po wybuchu wojny w Ukrainie Minister Edukacji i Nauki zapowiedział zmiany w podstawie programowej

[1] Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. z 2022 r., poz. 2305 z późn. zm.

przedmiotu „edukacja dla bezpieczeństwa" w zakresie proobronnym[2]. Zmiany weszły w życie z dniem 1 września 2022 r. i rozszerzyły podstawę programową przedmiotu o kwestie związane m.in. z obronnością państwa, nabyciem umiejętności strzeleckich oraz przygotowaniem uczniów do radzenia sobie z zagrożeniami wywołanymi działaniami wojennymi[3]. Ministerstwo Obrony Narodowej (MON) zainicjowało realizację projektu „Trenuj z wojskiem", który zakłada organizację jednodniowych szkoleń obronnych dla cywilów w całej Polsce[4]. Z kolei z inicjatywy Ministerstwa Sportu i Turystyki uruchomiono rządowy program upowszechniania strzelectwa, mający także na celu naukę podstawowych umiejętności obronnych[5]. Zmienił się również sposób postrzegania bezpieczeństwa, działań zbrojnych i współczesnych zagrożeń przez polskie społeczeństwo. Wojna w Ukrainie uzmysłowiła Polakom, jak ważna i nieoceniona jest umiejętność posługiwania się bronią palną, walki wręcz czy odpowiednia taktyka działania na wypadek działań zbrojnych.

Celem artykułu jest zaprezentowanie instytucji pozarządowej jako podmiotu skutecznie wspierającego organy rządowe i samorządowe w działalności na rzecz poprawy obronności państwa. W części teoretycznej zastosowano metodę analizy literatury przedmiotu oraz przywołano akty prawne związane z aktywnością trzeciego sektora w zakresie obronności państwa. W części praktycznej wykorzystano metodę studium przypadku. Na przykładzie Stowarzyszenia Aktywności Zawodowej „PASSA" w Kielcach przedstawiono – w trzech aspektach – realizację projektu „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych". Należy podkreślić, że w aktualnej literaturze przedmiotu trudno znaleźć opracowania nawiązujące do realizacji przez organizacje pozarządowe projektów na rzecz poprawy obronności państwa w kontekście zbrojnej agresji Rosji na Ukrainę. Zdaniem Autorów niniejszy artykuł uzupełnia lukę w tym zakresie.

---

[2] Przedmiot „edukacja dla bezpieczeństwa" jest obowiązkowo realizowany w klasie VIII szkoły podstawowej oraz w klasie I szkół ponadpodstawowych (liceum ogólnokształcącego, technikum i branżowej szkoły I stopnia) w wymiarze 1 godziny tygodniowo.

[3] Rozporządzenie Ministra Edukacji i Nauki z dnia 1 sierpnia 2022 r. zmieniające rozporządzenie w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, Dz.U. z 2022 r., poz. 1705 z późn. zm.; Rozporządzenie Ministra Edukacji i Nauki z dnia 1 sierpnia 2022 r. zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz.U. z 2022 r., poz. 1717 z późn. zm.

[4] *„Trenuj z wojskiem" – szkolenia wojskowe dla każdego*, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/trenuj-z-wojskiem-szkolenia-wojskowe-dla-kazdego [dostęp: 26.02.2023].

[5] *Wystartował Program Upowszechniania Strzelectwa dla grupy wiekowej 18–26 lat*, 6.09.2022, https://www.gov.pl/web/sport/wystartowal-program-upowszechniania-strzelectwa-dla-grupy-wiekowej-18-26-lat [dostęp: 25.02.2023].

Istota działalności organizacji pozarządowych w Polsce

W państwach o ustroju demokratycznym organizacje pozarządowe[6], obok organizacji rządowych i samorządowych, stanowią istotny element systemu bezpieczeństwa państwa. Na wstępie należy podkreślić, że nie ma jednego aktu prawnego, który regulowałaby całość zagadnień związanych z funkcjonowaniem organizacji pozarządowych. Biorąc pod uwagę kwestie założycielskie oraz definicje pojęć, organizacje pozarządowe działają w oparciu o Ustawę z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach[7], a także Ustawę z dnia 6 kwietnia 1984 r. o fundacjach[8]. Zarówno stowarzyszenia, jak i fundacje podlegają Ustawie z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie. Wprowadzono w niej m.in. pojęcie pożytku publicznego oraz definicje: wolontariatu i organizacji pozarządowej. Zgodnie z tą ustawą organizacje pozarządowe to „niebędące jednostkami sektora finansów publicznych w rozumieniu ustawy o finansach publicznych i niedziałające w celu osiągnięcia zysku osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej, którym odrębna ustawa przyznaje zdolność prawną, w tym fundacje i stowarzyszenia”[9].

Istota trzeciego sektora polega na tym, że stanowi on specyficzną zbiorowość odrębną od sektora państwowego i komercyjnego. O ile działanie struktur państwa opiera się na zasadzie administracyjnej hierarchii i możliwości zastosowania przymusu, a działanie podmiotów gospodarczych i ich personelu nakierowane jest na maksymalizację zysku, o tyle działanie trzeciego sektora odwołuje się do dobrowolnego zaangażowania ludzi opartego na wspólnych wartościach. Organizacje pozarządowe wypełniają przestrzeń między jednostką a społeczeństwem, obywatelem a państwem. Działają zatem nie tylko na rzecz spójności społecznej, ale także przyczyniają się do rozwoju kompetencji obywatelskich i społecznych, sprawiając, że społeczeństwo jest bardziej świadome i rozwinięte[10]. Można stąd wysnuć wniosek, że nadrzędnym celem działalności trzeciego sektora jest szeroko pojmowane dobro społeczne. Realizując ten cel, organizacje non-profit pełnią kilka istotnych funkcji w życiu społeczno-gospodarczym:

- pomocową (związaną z działalnością charytatywną i ideą samopomocy),

---

[6] W opracowaniach z dziedziny ekonomii i mediach bardzo często używa się zamiennie terminów: „organizacje non-profit”, „trzeci sektor” i „organizacje społeczne”. W przypadku tego ostatniego stosowanie go jako synonimu „organizacji pozarządowej” bywa czasami kwestionowane.

[7] Ustawa z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach, Dz.U. z 1989 r., nr 20, poz. 104 z późn. zm.

[8] Ustawa z dnia 6 kwietnia 1984 r. o fundacjach, Dz.U. z 1984 r., nr 21, poz. 97 z późn. zm.

[9] Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie, Dz.U. z 2003 r., nr 96, poz. 873 z późn. zm., art. 3.

[10] B. Žuromskaitė, M. Zakrzewska, *Charakterystyka i dynamika trzeciego sektora na Litwie i w Polsce*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania Uniwersytetu Szczecińskiego” 2015, nr 40, t. 1, s. 302, https://doi.org/10.18276/sip.2015.40/1-23.

- opiekuńczo-wychowawczą (obejmującą działania na rzecz pobudzania postaw prospołecznych, aktywizacji społecznej w najbliższym otoczeniu, niesienia pomocy ludziom chorym i niepełnosprawnym),
- afiliacyjną (polegającą na integrowaniu ze sobą przedstawicieli konkretnych grup poprzez tworzenie np. stowarzyszeń kombatantów czy organizacji kobiecych),
- ekspresyjną (umożliwiającą realizację potrzeb wyższego rzędu związanych z uznaniem w oczach innych i samorealizacją)[11].

Organizacje pozarządowe są samorządne i niezależne. Zasady ich działalności (w tym tworzenie struktur organizacyjnych) określają wewnętrzne mechanizmy samoregulacji[12]. Niezależność – zarówno od źródeł finansowania, jak i politycznych ośrodków władzy – jest podstawowym wyzwaniem dla tych organizacji.

Ustawa o działalności pożytku publicznego i wolontariacie identyfikuje sferę zadań publicznych, w których przewidziana jest aktywność organizacji pozarządowych. Są to m.in. zadania z zakresu:

- ochrony i promocji zdrowia,
- działalności na rzecz osób niepełnosprawnych,
- działalności wspomagającej rozwój gospodarczy,
- porządku i bezpieczeństwa publicznego,
- obronności państwa i działalności Sił Zbrojnych Rzeczypospolitej Polskiej,
- pomocy ofiarom katastrof, klęsk żywiołowych, konfliktów zbrojnych i wojen w kraju i za granicą[13].

Z punktu widzenia rozważań podjętych w niniejszym artykule najistotniejsze są zadania prowadzone w obszarze obronności państwa i działalności Sił Zbrojnych RP. Analiza doświadczeń polskich i zagranicznych wskazuje, iż organizacje pozarządowe mają możliwość współdziałania z siłami zbrojnymi na wielu płaszczyznach. Działania te mogą wspierać wojsko bezpośrednio (dotyczyć realizacji konkretnych zadań na rzecz sił zbrojnych lub wspólnie z nimi) albo pośrednio, np. poprzez tworzenie społecznej akceptacji dla wojska, oddziaływanie na społeczeństwo oraz jego stosunek do spraw obronnych.

---

[11] K. Zioło, *Funkcjonowanie organizacji pozarządowych a motywacje ich uczestników*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie" 2016, nr 4, s. 223–224, http://dx.doi.org/10.5604/18998658.1232698.

[12] Każda organizacja pozarządowa przy tworzeniu struktur organizacyjnych powinna co najmniej rozróżnić w swoim statucie funkcje zarządzające od nadzorczych. W zależności od potrzeb, organ nadzorczy powinien pełnić funkcje programowe i kontrolne. Od członków kolegialnego organu nadzorczego wymaga się bezstronności, rzetelności i zaangażowania w działalność organizacji. *Karta zasad działania organizacji pozarządowych*, https://wartowiedziec.pl/serwis-glowny/aktualnosci/18042-karta-zasad-dziaania-organizacji-pozarzdowych [dostęp: 15.09.2023].

[13] Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie, art. 4.

Zaangażowanie organizacji pozarządowych w działania na rzecz obronności państwa

Współcześnie wypracowana definicja obronności państwa informuje, iż „jest to jedna z podstawowych dziedzin państwa, ukierunkowana na przeciwdziałanie wszelkiego rodzaju zagrożeniom polityczno-militarnym". W praktyce oznacza możliwość odparcia agresji oraz przygotowania państwa do działalności obronnej[14].

Potencjał organizacji pozarządowych w realizacji zadań na rzecz bezpieczeństwa i obronności spowodował, że zostały one uwzględnione w dokumencie *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 2020 roku. Przyjęte w strategii założenia stanowią, że budowa systemu obrony powszechnej, „który będzie stanowił kompleksową odporność państwa na zagrożenia niemilitarne i militarne"[15], powinna w pełni wykorzystywać potencjał instytucji państwowych i samorządowych, podmiotów systemu edukacji i szkolnictwa wyższego, społeczności lokalnych, podmiotów gospodarczych, organizacji pozarządowych oraz obywateli. Strategia zakłada również zaangażowanie organizacji pozarządowych w budowanie wiedzy na temat bezpieczeństwa narodowego, w powiązaniu z promowaniem postaw patriotycznych, powinności obywatelskich oraz zachowań prospołecznych[16].

Z kolei Rozporządzenie Rady Ministrów z dnia 24 lutego 2004 r. w sprawie utworzenia okręgów wojskowych oraz określenia ich siedzib i terytorialnego zasięgu działania umożliwia dowódcom okręgów wojskowych podejmowanie wspólnych zadań z organizacjami pozarządowymi w zakresie obronności państwa. W świetle zapisów Rozporządzenia organizacje pozarządowe mogą delegować swoich przedstawicieli do udziału we wspólnych zamierzeniach szkoleniowych, jak również partycypować w projektach upowszechniających problematykę patriotyczno-obronną i popularyzowaniu spraw obronności i wojska[17].

Minister Obrony Narodowej 7 grudnia 2020 r. wydał decyzję w sprawie wprowadzenia zasad współpracy resortu obrony narodowej z organizacjami pozarządowymi i innymi partnerami społecznymi. Decyzja wprowadza m.in. możliwość zawarcia partnerskiej umowy proobronnej pomiędzy MON a organizacją pozarządową, prowadzącą działalność proobronną i współpracującą z resortem. Umowa partnerska ma zawierać zobowiązania resortu w zakresie podnoszenia kwalifikacji

---

[14] *Słownik terminów z zakresu bezpieczeństwa*, red. J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, Wydawnictwo Adam Marszałek, Toruń 2020, s. 137.

[15] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, 12.05.2020, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/8808,Strategia-Bezpieczenstwa-Narodowego-Rzeczypospolitej-Polskiej.html, s. 15 [dostęp: 21.02.2023].

[16] *Ibidem*.

[17] Rozporządzenie Rady Ministrów z dnia 24 lutego 2004 r. w sprawie utworzenia okręgów wojskowych oraz określenia ich siedzib i terytorialnego zasięgu działania, Dz.U. z 2004 r., nr 40, poz. 355.

członków organizacji oraz zobowiązania organizacji do angażowania się w przedsięwzięcia resortu związane z upowszechnianiem umiejętności ważnych dla bezpieczeństwa państwa[18].

W tym miejscu można postawić pytanie o skalę zaangażowania trzeciego sektora w obszarze obronności państwa. Należy podkreślić, że dokładna liczba polskich organizacji pozarządowych działających w Polsce w tym obszarze jest trudna do oszacowania. Z raportu opublikowanego przez Główny Urząd Statystyczny (GUS) wynika, że na koniec 2020 r. na terenie Polski aktywnie działało 95,2 tys. rejestrowych organizacji non-profit[19]. W strukturze badanych organizacji, według głównej dziedziny działalności statutowej, obronność państwa nie została uwzględniona. Nieco światła na omawianą kwestię rzucają ustalenia Najwyższej Izby Kontroli (NIK), poczynione w trakcie oceny współpracy MON z organizacjami proobronnymi. Wynika z nich, że w latach 2014–2017 r. o dotację z MON wystąpiło około 1000 fundacji i stowarzyszeń, z czego otrzymało ją 180[20]. Z kolei Autorzy niniejszej publikacji dokonali przeglądu otwartych konkursów ofert ogłaszanych przez Ministra Obrony Narodowej na realizację zadań publicznych w formie wsparcia w zakresie „Obronność państwa i działalność Sił Zbrojnych Rzeczypospolitej Polskiej". Z uzyskanych informacji wynika, że w latach 2019–2022 dofinansowanie na realizację zadań otrzymało 170 organizacji pozarządowych z terenu całej Polski[21]. Niestety nie udało się oszacować, ile organizacji pozarządowych zgłosiło chęć wzięcia udziału we wspomnianych konkursach.

W bogatej literaturze przedmiotu na temat aktywności trzeciego sektora w Polsce niewiele opracowań dotyczy działalności organizacji pozarządowych na rzecz obronności państwa. Podkreśla się pozytywne znaczenie działań edukacyjnych i szkoleniowych trzeciego sektora we wspomnianym obszarze.

Grzegorz Wierzbicki argumentuje, że podmioty państwowe nie są w stanie skutecznie działać na rzecz bezpieczeństwa obywateli bez ich partycypacji. Autor, dokonując analizy obszarów i możliwości działań trzeciego sektora w zakresie przygotowania obronnego społeczeństwa, dochodzi do wniosku, że idea organizacji

---

[18] Decyzja Nr 168/MON Ministra Obrony Narodowej z dnia 7 grudnia 2020 r. w sprawie wprowadzenia zasad współpracy resortu obrony narodowej z organizacjami pozarządowymi i innymi partnerami społecznymi, Dz.Urz. MON z 2020 r., poz. 194.

[19] *Działalność stowarzyszeń i podobnych organizacji społecznych, fundacji, społecznych podmiotów wyznaniowych, kół gospodyń wiejskich oraz samorządu gospodarczego i zawodowego w 2020 r. – wyniki wstępne*, https://stat.gov.pl/obszary-tematyczne/gospodarka-spoleczna-wolontariat/gospodarka-spoleczna-trzeci-sektor/dzialalnosc-stowarzyszen-i-podobnych-organizacji-spolecznych-fundacji-spolecznych-podmiotow-wyznaniowych-oraz-samorzadu-gospodarczego-i-zawodowego-w-2020-r-wyniki-wstepne,3,9.html, s. 2 [dostęp: 7.03.2023].

[20] *Współpraca Ministerstwa Obrony Narodowej z organizacjami proobronnymi. Informacja o wynikach kontroli*, NIK, Warszawa 2018, s. 52.

[21] MON, Otwarte konkursy ofert – Szkolenia – Zakończone postępowania, https://www.gov.pl/web/obrona-narodowa/zakonczone-postepowania [dostęp: 6.03.2023].

pozarządowych opierająca się na zaangażowaniu społeczeństwa jest istotnym ogniwem w procesie przygotowania obronnego. Zdaniem Autora, potencjał dydaktyczno-wychowawczy organizacji pozarządowych koresponduje z całościowym podejściem do problematyki bezpieczeństwa i obronności. Największą rolę w propagowaniu problematyki obronności powinny odegrać stowarzyszenia o charakterze militarnym i sportowym, a także skupiające byłych żołnierzy zawodowych oraz kombatanckie[22].

Tomasz Kośmider i Krzysztof Gąsiorek, dostrzegając duże zróżnicowanie trzeciego sektora pod względem aktywności, zasięgu terytorialnego, liczebności i struktur organizacyjnych, postulują ich federalizację branżową. Zdaniem Autorów powinno to ułatwić współpracę z organami administracji publicznej i włączenie organizacji pozarządowych w system bezpieczeństwa narodowego[23]. Autorzy akcentują rolę organizacji proobronnych w tworzeniu społecznej bazy bezpieczeństwa narodowego. Doświadczenia z funkcjonowania organizacji proobronnych (np. Strzelec, Legia Akademicka) oraz tzw. klas mundurowych w szkołach ponadgimnazjalnych stanowią dobrą podstawę do wypracowania koncepcji ochotniczej służby wojskowej na potrzeby Narodowych Sił Rezerwowych oraz stworzenia, obok armii zawodowej, obywatelskiej formy systemu wojskowego na wzór państw skandynawskich, w których Gwardie Narodowe działają jako stowarzyszenia[24].

W podobnym tonie wypowiadają się w swojej publikacji Andrzej Soboń i Marta Adamczewska. Autorzy na konkretnych przykładach dowodzą, że organizacje proobronne w Polsce w ramach swojej działalności statutowej udanie realizują wiele szkoleń oraz programów mających na celu zwiększanie wiedzy, jak również rozwój postaw patriotycznych i proobronnych nie tylko swoich członków, ale i całego społeczeństwa[25]. Następnie Autorzy, dokonując przeglądu aktów prawnych obowiązujących w Polsce, Czechach, Słowacji, Węgrzech i Litwie, próbowali ustalić, jak wspomniane państwa wykorzystują organizacje pozarządowe w obszarze podnoszenia zdolności obronnych. W oparciu o przeprowadzoną analizę Soboń i Adamczewska konkludują, że obowiązujący w Polsce system prawny nie stawia przed organizacjami społecznymi jasnych zadań w ramach systemu bezpieczeństwa państwa. W opinii Autorów, aby zmienić istniejący stan rzeczy, warto posłużyć się rozwiązaniami przyjętymi

---

22 G. Wierzbicki, *Potencjał organizacji pozarządowych w zakresie przygotowanie obronnego społeczeństwa*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2020, t. 6, nr 2, s. 205–215, https://doi.org/10.34739/dsd.2020.02.14.

23 T. Kośmider, K. Gąsiorek, *Organizacje proobronne w tworzeniu społecznej bazy bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Zarys problemu*, [w:] *Kultura bezpieczeństwa. Potrzeby i uwarunkowania*, t. 1, red. S. Jaczyński, J. Kunikowski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016, s. 509.

24 *Ibidem*, s. 510.

25 A. Soboń, M. Adamczewska, *Organizacje społeczne w realizacji zadań proobronnych*, „Civitas et Lex" 2023, t. 37, nr 1, s. 31, https://doi.org/10.31648/cetl.8101.

na Litwie, gdzie Litewski Związek Strzelecki włączony jest do systemu obronnego państwa i wspiera organy państwowe w realizacji związanych z nim zadań[26].

Realizacja projektu na rzecz obronności państwa przez organizację pozarządową na przykładzie Stowarzyszenia Aktywności Zawodowej „PASSA" w Kielcach

Stowarzyszenie Aktywności Zawodowej „PASSA" w Kielcach powstało w 2012 r. Jego założycielem i Prezesem Zarządu jest mgr Katarzyna Banasik. Misją organizacji jest propagowanie bezpieczeństwa publicznego i osobistego oraz aktywizacja zawodowa. Stowarzyszenie realizuje cele statutowe, którymi są przede wszystkim:

- kształcenie ustawiczne,
- edukacja dla bezpieczeństwa,
- działania na rzecz obronności państwa.

Stowarzyszenie prowadzi kursy i szkolenia aktywizacji zawodowej osób dorosłych w ramach Niepublicznej Placówki Kształcenia Ustawicznego „PASSA", która posiada wpis do ewidencji szkół i placówek niepublicznych i jest objęta systemem oświaty w rozumieniu przepisów o systemie oświaty. Placówka jest wpisana do rejestru instytucji szkoleniowych Wojewódzkiego Urzędu Pracy w Kielcach. Posiada akredytację Świętokrzyskiego Kuratora Oświaty. Stowarzyszenie realizuje ponadto szereg projektów z zakresu bezpieczeństwa publicznego i proobronności, dofinansowanych ze źródeł publicznych, m.in. przez Ministerstwo Spraw Wewnętrznych i Administracji oraz Ministerstwo Obrony Narodowej. Współpracuje z Europejskim Centrum Bezpieczeństwa, w którym zrzeszone jest grono międzynarodowych ekspertów ds. bezpieczeństwa, m.in. z Francji, Włoch, Hiszpanii, Wielkiej Brytanii, Irlandii i Ukrainy. Współpraca polega na wymianie doświadczeń w zakresie usług szkoleniowych oraz wdrażaniu międzynarodowych standardów w obszarze procedur działania w sytuacji zagrożenia.

Aspekty prawne realizowanego projektu

Stowarzyszenie Aktywności Zawodowej „PASSA" w Kielcach opracowało autorski projekt „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych". Projekt otrzymał dofinansowanie w ramach otwartego konkursu ofert na realizację zadań publicznych w formie wsparcia w zakresie: Obronność państwa i działalność Sił Zbrojnych RP pn. „I Ty możesz służyć Ojczyźnie", ogłoszonego przez Ministra Obrony Narodowej[27]. Przedsięwzięcie

[26] *Ibidem*, s. 36.

[27] MON, Otwarty konkurs ofert nr ew. 03/2022/WD/DEKiD, https://www.gov.pl/web/obrona-narodowa/otwarty-konkurs-ofert-nr-ew-032022wddekid [dostęp: 6.03.2023].

realizowane było w oparciu o umowę o realizację zadania publicznego zawartą pomiędzy Ministrem Obrony Narodowej a Stowarzyszeniem „PASSA". Umowa nakładała na Stowarzyszenie szereg obowiązków dotyczących m.in. promocji zadania publicznego, ochrony danych osobowych przetwarzanych w trakcie realizacji zadania, zapewnienia dostępności osobom ze szczególnymi potrzebami czy prowadzenia wyodrębnionej dokumentacji finansowo-księgowej i ewidencji księgowej zadania publicznego. W związku z tym, iż projekt zakładał realizację szkoleń strzeleckich z wykorzystaniem broni i amunicji, Stowarzyszenie „PASSA" było zobligowane przestrzegać także przepisów prawa określonych w ustawie z dnia 21 maja 1999 r. o broni i amunicji[28], ustawie z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym[29] oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 15 marca 2000 r. w sprawie wzorcowego regulaminu strzelnic[30]. Ponadto Stowarzyszenie zobowiązane było zapewnić kadrę instruktorską posiadającą stosowne uprawnienia do prowadzenia szkoleń o charakterze strzeleckim. Trzeba nadmienić, iż projekt był odpowiedzią na ogłoszoną niezwłocznie po wybuchu wojny w Ukrainie zapowiedź zmian w programie nauczania przedmiotu „edukacja dla bezpieczeństwa" w zakresie proobronnym. Treści merytoryczne realizowane w ramach projektu szkoleń odpowiadały dokonanym przez Ministra Edukacji i Nauki zmianom w podstawie programowej przedmiotu dla klas ósmych szkół podstawowych i pierwszych szkół ponadpodstawowych[31]. Umowa o dofinansowanie zadania publicznego regulowała także zasady jej rozliczenia i rozwiązania. Strony dopuściły rozwiązanie umowy za porozumieniem stron, odstąpienie od umowy przez zleceniobiorcę i rozwiązanie umowy przez zleceniodawcę. Rozliczenie umowy nastąpiło poprzez zatwierdzenie przez Ministerstwo Obrony Narodowej pisemnego sprawozdania z wykonania zadania publicznego złożonego przez Stowarzyszenie[32].

Aspekty organizacyjne i finansowe

Inicjatorem projektu było Stowarzyszenie „PASSA". Do współorganizacji zaproszono Centrum Przygotowań do Misji Zagranicznych w Kielcach, Komendę Wojewódzką

---

28 Ustawa z dnia 21 maja 1999 r. o broni i amunicji, Dz.U. z 2020 r., poz. 955 z późn. zm.

29 Ustawa z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym, Dz.U. z 2022 r., poz. 268 z późn. zm.

30 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 marca 2000 r. w sprawie wzorcowego regulaminu strzelnic, Dz.U. z 2000 r., nr 18, poz. 234 z późn. zm.

31 Zob. przypis 3.

32 Sprawozdanie z wykonania zadania publicznego „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych", Stowarzyszenie Aktywności Zawodowej „PASSA", Kielce 2022.

Policji w Kielcach, Komendę Wojewódzką Państwowej Straży Pożarnej w Kielcach oraz Kuratorium Oświaty w Kielcach. Każdy ze współorganizatorów miał określone zadania do realizacji. Koordynatorem projektu została Prezes Stowarzyszenia „PASSA", posiadająca wieloletnie doświadczenie w realizacji projektów współfinansowanych ze środków publicznych. Patronat honorowy nad przedsięwzięciem objął Minister Edukacji i Nauki oraz Wojewoda Świętokrzyski. Głównymi celami projektu były: przygotowanie społeczeństwa do prawidłowego działania w sytuacji konfliktu zbrojnego na terenie Rzeczypospolitej Polskiej, nabycie przez społeczeństwo umiejętności przydatnych w służbie wojskowej oraz ukształtowanie społecznej świadomości o prawach i obowiązkach obywateli wobec ojczyzny. Zadanie publiczne realizowane było od czerwca do listopada 2022 r.

Projekt został podzielony na trzy etapy: przygotowanie, merytoryczną realizację działań oraz ich podsumowanie. W ramach zadania publicznego przeprowadzono szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych, podczas których omawiane były m.in.: zasady przygotowania bezpiecznego schronu i plecaka przetrwania, sygnały alarmowania o zagrożeniu z powietrza, procedury działania w przypadku znalezienia granatu i materiałów wybuchowych, zasady działania na polu walki. Szkolenie strzeleckie zorganizowano na strzelnicy, z użyciem broni palnej oraz laserowych symulatorów strzelań. Ponadto dla kadry zarządzającej i dydaktycznej zorganizowano konferencję edukacyjną poświęconą zmianom w podstawie programowej przedmiotu „edukacja dla bezpieczeństwa" w kontekście proobronnym, opracowano pakiety edukacyjne dla uczniów i nakręcono dwa proobronne filmy instruktażowe. Za pośrednictwem Kuratorium Oświaty w Kielcach wytworzone w ramach projektu narzędzia dydaktyczne przekazano wszystkim placówkom oświatowym z województwa świętokrzyskiego.

Efektem realizowanego projektu był wzrost poziomu wiedzy i nabycie przez uczniów świętokrzyskich szkół nowych umiejętności z zakresu bezpieczeństwa oraz znajomości procedur reagowania w przypadku konfliktu zbrojnego na terenie Polski[33]. Kadra zarządzająca i dydaktyczna poszerzyła swoją wiedzę na temat problematyki przysposobienia obronnego (sposobów i metod realizacji zajęć, zakresu programowego oraz instytucji działających we wspomnianym obszarze)[34].

Zakres zrealizowanych w ramach projektu działań ilustrują następujące dane liczbowe:

- w projekcie wzięło udział 14 placówek oświatowych,
- szkolenia zostały zrealizowane dla 2577 uczniów (łącznie 364 godzin zajęć),
- 140 uczniów wzięło udział w zajęciach praktycznych na strzelnicy, podczas

[33] Do oceny efektów projektu posłużył kwestionariusz wywiadu. Uczestniczyło w nim 2577 uczniów szkół biorących udział w projekcie. Uczniowie wypełniali kwestionariusz przed rozpoczęciem zajęć oraz po ich zakończeniu. Wzrost poziomu wiedzy i umiejętności przydatnych w służbie wojskowej potwierdzono u 100% uczniów.

[34] Sprawozdanie z wykonania zadania publicznego..., *op. cit.*, s. 1–12.

których wykorzystano 3780 sztuk amunicji,
- placówkom oświatowym przekazano 840 pakietów edukacyjnych i 840 pakietów promujących zadanie publiczne,
- w konferencji edukacyjnej dla kadry zarządzającej i dydaktycznej wzięło udział 220 osób,
- wydrukowano 7000 broszur informacyjno-edukacyjnych[35].

Aspekty finansowe projektu – źródła finansowania oraz koszty realizacji poszczególnych działań – prezentuje tabela 1.

Tabela 1. Źródła finansowania oraz koszty realizacji działań projektu „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych"

Źródła finansowania projektu		
Całkowity koszt realizacji projektu		82 520 zł
1.	Kwota dotacji	66 000 zł
2.	Wkład własny finansowy	8260 zł
3.	Wkład własny niefinansowy	8260 zł
Koszty realizacji działań		
1.	Działania informacyjno-promocyjne	8877 zł
2.	Narzędzia dydaktyczne	14 028 zł
3.	Wynagrodzenia za realizację szkoleń dla uczniów	36 400 zł
4.	Koszty związane z realizacją szkoleń dla uczniów	20 015 zł
5.	Badanie ankietowe	3200 zł

Źródło: Sprawozdanie z wykonania zadania publicznego „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych", Stowarzyszenie Aktywności Zawodowej „PASSA", Kielce 2022.

Z danych przedstawionych w tabeli 1 wynika, że pozycją, która generowała największe koszty w ramach realizowanego projektu, były szkolenia proobronne dla uczniów (68% kosztów całkowitych). Należy dodać, iż szkolenia były najważniejszym działaniem realizowanym w ramach zadania publicznego (364 godziny), wymagały od prowadzących uprawnień instruktorskich i dysponowania specjalistycznym sprzętem (broń palna, atrapy broni, symulatory strzelań, granaty szkoleniowe itp.). Na koszt organizacji szkoleń składały się również wysokie ceny amunicji i wynajmu strzelnicy. Najniższe koszty w ramach projektu poniesiono w związku z przeprowadzeniem badania ankietowego oceniającego postawę młodzieży wobec służby ojczyźnie (3,8%).

Na koniec warto dodać, że Stowarzyszenie „PASSA" było zobligowane do prowadzenia wyodrębnionej dokumentacji finansowo-księgowej i ewidencji księgowej zadania publicznego. Zasady rozliczenia dotacji regulowała umowa i regulamin

[35] *Ibidem*.

otwartego konkursu ofert. Zatwierdzenie sprawozdania nastąpiło po weryfikacji przez zleceniodawcę założonych w ofercie rezultatów, działań oraz prawidłowości poniesionych kosztów.

Podsumowanie

Całkowita ocena zaangażowania organizacji pozarządowych na rzecz obronności państwa nie jest możliwa, ponieważ trudno ustalić liczbę organizacji działających w Polsce w tym obszarze. Wydaje się, że postulat wysunięty w literaturze przedmiotu o konieczności wprowadzenia rozwiązań prawnych włączających instytucje trzeciego sektora do systemu bezpieczeństwa państwa jest uzasadniony. Takie rozwiązanie przyczyniłoby się do podwyższenia możliwości obronnych państwa i wzmocnienia poczucia bezpieczeństwa w polskim społeczeństwie.

Zaprezentowane studium przypadku udowadnia, że w zakresie edukacji dla bezpieczeństwa instytucje trzeciego sektora potrafią szybko reagować, dostosowywać ofertę szkoleń i podejmować działania w sytuacjach nadzwyczajnych zagrożeń. Realizacja projektu „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych" uwidoczniła przewagę edukacji prowadzonej przez organizacje pozarządowe nad zajęciami prowadzonymi w szkołach w ramach przedmiotu „edukacja dla bezpieczeństwa". Placówki oświatowe nie są przygotowane do realizacji podstawy programowej, tzn. nie mają funduszy, kadry instruktorskiej ani zaplecza (strzelnice, strzelnice wirtualne, atrapy broni). Działania podjęte przez Stowarzyszenie Aktywności Zawodowej „PASSA" w ramach projektu pozwoliły 14 uczestniczącym w nim szkołom na zrealizowanie wymaganych treści dydaktycznych. Warty podkreślenia jest fakt, że wiedza teoretyczna z zakresu obsługi broni, zasad celnego strzelania czy taktyki działania na polu walki, zdobyta przez uczniów w trakcie trwania projektu, była natychmiast sprawdzana w praktyce. W efekcie prowadziło to wzrostu zainteresowania udziałem w tego typu projektach w przyszłości.

Warto przywołać wyniki badania ankietowego przeprowadzonego na próbie 270 uczniów szkół zakwalifikowanych do projektu. Podstawowym celem ankiety była ocena postaw młodzieży z terenu województwa świętokrzyskiego wobec służby ojczyźnie. Z badania wynika, że respondenci w większości rozumieją, czym jest patriotyzm, popierają rozwój obrony terytorialnej w Polsce, gotowi są w razie zagrożenia bronić ojczyzny nawet z narażeniem życia. Zdaniem ankietowanych udział w szkoleniach proobronnych w celu doskonalenia umiejętności na wypadek konfliktu zbrojnego na terenie Rzeczypospolitej Polskiej jest koniecznością.

Bibliografia

Działalność stowarzyszeń i podobnych organizacji społecznych, fundacji, społecznych podmiotów wyznaniowych, kół gospodyń wiejskich oraz samorządu gospodarczego i zawodowego w 2020 r. – wyniki wstępne, https://stat.gov.pl/obszary-tematyczne/gospodarka-spoleczna-wolontariat/gospodarka-spoleczna-trzeci-sektor/dzialalnosc-stowarzyszen-i-podobnych-organizacji-spolecznych-fundacji-spolecznych-podmiotow-wyznaniowych-oraz-samorzadu-gospodarczego-i-zawodowego-w-2020-r-wyniki-wstepne,3,9.html [dostęp: 7.03.2023].

Karta zasad działania organizacji pozarządowych, https://wartowiedziec.pl/serwis-glowny/aktualnosci/18042-karta-zasad-dziaania-organizacji-pozarzdowych [dostęp: 15.09.2023].

Kośmider T., Gąsiorek K., *Organizacje proobronne w tworzeniu społecznej bazy bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Zarys problemu*, [w:] *Kultura bezpieczeństwa. Potrzeby i uwarunkowania*, t 1, red. S. Jaczyński, J. Kunikowski, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016, s. 509–522.

MON, Otwarte konkursy ofert – Szkolenia – Zakończone postępowania, https://www.gov.pl/web/obrona-narodowa/zakonczone-postepowania [dostęp: 6.03.2023].

Słownik terminów z zakresu bezpieczeństwa, red. J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, Wydawnictwo Adam Marszałek, Toruń 2020.

Soboń A., Adamczewska M., *Organizacje społeczne w realizacji zadań proobronnych*, „Civitas et Lex" 2023, t. 37, nr 1, s. 27–37, https://doi.org/10.31648/cetl.8101.

Sprawozdanie z wykonania zadania publicznego „My Młode Pokolenie – Tobie Ojczyzno. Szkolenia proobronne dla uczniów świętokrzyskich placówek oświatowych", Stowarzyszenie Aktywności Zawodowej „PASSA", Kielce 2022.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 12.05.2020, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/8808,Strategia-Bezpieczenstwa-Narodowego-Rzeczypospolitej-Polskiej.html [dostęp: 21.02.2023].

„Trenuj z wojskiem" – szkolenia wojskowe dla każdego, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/trenuj-z-wojskiem-szkolenia-wojskowe-dla-kazdego/ [dostęp: 26.02.2023].

Wierzbicki G., *Potencjał organizacji pozarządowych w zakresie przygotowanie obronnego społeczeństwa*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2020, t. 6, nr 2, s. 205–215, https://doi.org/10.34739/dsd.2020.02.14.

Współpraca Ministerstwa Obrony Narodowej z organizacjami proobronnymi. Informacja o wynikach kontroli, NIK, Warszawa 2018.

Wystartował Program Upowszechniania Strzelectwa dla grupy wiekowej 18–26 lat, 6.09.2022, https://www.gov.pl/web/sport/wystartowal-program-upowszechniania-strzelectwa-dla-grupy-wiekowej-18-26-lat [dostęp: 25.02.2023].

Zioło K., *Funkcjonowanie organizacji pozarządowych a motywacje ich uczestników*, „Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie" 2016, nr 4, s. 217–232, http://dx.doi.org/10.5604/18998658.1232698.

Žuromskaitė B., Zakrzewska M., *Charakterystyka i dynamika trzeciego sektora na Litwie i w Polsce*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania Uniwersytetu Szczecińskiego" 2015, nr 40, t. 1, s. 301–314, https://doi.org/10.18276/sip.2015.40/1-23.

Akty prawne

Ustawa z dnia 6 kwietnia 1984 r. o fundacjach, Dz.U. z 1984 r., nr 21, poz. 97 z późn. zm.

Ustawa z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach, Dz.U. z 1989 r., nr 20, poz. 104 z późn. zm.

Ustawa z dnia 21 maja 1999 r. o broni i amunicji, Dz.U. z 2020 r., poz. 955 z późn. zm.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 marca 2000 r. w sprawie wzorcowego regulaminu strzelnic, Dz.U. z 2000 r., nr 18, poz. 234 z późn. zm.
Ustawa z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie, Dz.U. z 2003 r., nr 96, poz. 873 z późn. zm.
Rozporządzenie Rady Ministrów z dnia 24 lutego 2004 r. w sprawie utworzenia okręgów wojskowych oraz określenia ich siedzib i terytorialnego zasięgu działania, Dz.U. z 2004 r., nr 40, poz. 355.
Ustawa z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym, Dz.U. z 2022 r., poz. 268 z późn. zm.
Decyzja Nr 168/MON Ministra Obrony Narodowej z dnia 7 grudnia 2020 r. w sprawie wprowadzenia zasad współpracy resortu obrony narodowej z organizacjami pozarządowymi i innymi partnerami społecznymi, Dz.Urz. MON z 2020 r., poz. 194.
Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz. U. z 2022 r., poz. 2305 z późn. zm.
Rozporządzenie Ministra Edukacji i Nauki z dnia 1 sierpnia 2022 r. zmieniające rozporządzenie w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, Dz.U. z 2022 r., poz. 1705 z późn. zm.
Rozporządzenie Ministra Edukacji i Nauki z dnia 1 sierpnia 2022 r. zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz.U. z 2022 r., poz. 1717 z późn. zm.

Działalność organizacji pozarządowych na rzecz poprawy obronności państwa. Studium przypadku

Streszczenie

Inwazja Rosji na Ukrainę utwierdziła polski rząd w przekonaniu, że konieczna jest nieustanna aktywizacja społeczeństwa w dziedzinie obronności państwa. Nieocenioną rolę w tym zakresie odgrywają organizacje pozarządowe, które stały się istotnym partnerem sił zbrojnych w realizowaniu edukacji proobronnej i podnoszeniu zdolności obronnych Polski. W artykule przedstawiono akty prawne umożliwiające działalność organizacji pozarządowych w obszarze obronności Polski, dokonano krótkiego przeglądu literatury przedmiotu oraz zaprezentowano efekty realizowanego przez Stowarzyszenie Aktywności Zawodowej „PASSA" w Kielcach projektu w ramach ogłoszonego przez Ministra Obrony Narodowej konkursu: „Obronność państwa i działalność Sił Zbrojnych RP pn. I Ty możesz służyć Ojczyźnie". Analiza literatury przedmiotu oraz przedstawione studium przypadku uprawniają do stwierdzenia, że instytucje trzeciego sektora potrafią skutecznie wspierać organy rządowe w działalności na rzecz poprawy obronności państwa.

Słowa kluczowe: obronność państwa, organizacja pozarządowa, edukacja dla bezpieczeństwa, Stowarzyszenie Aktywności Zawodowej „PASSA" w Kielcach

Activities of non-governmental organizations to improve state defence: A case study
Abstract

The Russian invasion of Ukraine convinced the Polish government that permanent mobilization of Polish people in the state defence is an absolute necessity. The third sector organizations play an invaluable role in this respect, and they have become an essential partner of the country's defence system as far as their effort to organize suitable educational courses and improvement in upgrading pro-defensive abilities of Polish people are concerned. The article presents legal acts enabling the third sector to act effectively in the field of the state defence, a short overview of the articles concerning the subject as well as the results of the project conducted by the „PASSA" Association of Professional Activity in Kielce. The project was carried out within the competition announced by the Polish Ministry of Defence: „A State Defence and Activity of the Armed Forces of the Republic of Poland: You too can serve your homeland". The analysis of the subject literature as well as the presented case study justify the conclusion that the third sector organizations can effectively support the government in its effort to improve the state defence system.

Key words: state defence, non-governmental organization, education for safety, „PASSA" Association of Professional Activity in Kielce

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)

DOI: 10.48269/2451-0718-btip-2023-4-010
Data wpłynięcia: 17.04.2023
Data akceptacji: 19.09.2023

Bartosz Włodarczyk

mgr, Ministerstwo Klimatu i Środowiska, Departament Spraw Obronnych, Zarządzania Kryzysowego i Bezpieczeństwa, Wydział Zarządzania Kryzysowego
https://orcid.org/0000-0002-5556-0481

Wojska Obrony Terytorialnej jako element rekonstrukcji polskiej obrony cywilnej

Wprowadzenie

Zapewnianie powszechnego bezpieczeństwa jest jedną z najważniejszych funkcji każdego państwa. To właśnie instytucje państwowe mogą stanowić najdoskonalszą formę zabezpieczenia potrzeb człowieka (jednostki) i grup społecznych[1]. Bezpieczeństwo należy tu rozumieć jako jedną z podstawowych dziedzin funkcjonowania państwa, mającą na celu zapewnianie nie tylko przetrwania, ale przede wszystkim umożliwiającą rozwój i swobodę realizacji interesów politycznych w konkretnym środowisku bezpieczeństwa. W tym zakresie należy wyróżnić podejmowanie wyzwań, wykorzystywanie szans, redukowanie wielowymiarowego ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla interesów przyjętego ośrodka decyzyjnego.

W rozważaniach na temat istoty bezpieczeństwa zwraca się uwagę, że dla państwa, jako podmiotu stosunków międzynarodowych, istotnymi zagrożeniami stają się czynniki wewnętrzne i zewnętrzne. Ten podział jest najbardziej rudymentarny, lecz zarazem dyskusyjny ze względu na intensyfikację powiązań i relacji w systemie internacjonalnym, co należy utożsamiać z progresywnym zjawiskiem globalizacji.

[1] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Wydawnictwo AON, Warszawa 2011, s. 25.

Oprócz poziomu i charakteru niebezpieczeństw należy uwzględnić także jeszcze niezdefiniowane grupy zagrożeń, mogących mieć negatywny wpływ na poziom bezpieczeństwa państwa. Łączy się to między innymi z utrzymaniem ciągłej potrzeby analizowania nowych wymiarów bezpieczeństwa. Postępujące przeobrażenia w definiowaniu kluczowych terminów sprawiły, że akcenty zostały przesunięte z zagadnień militarnych na inne płaszczyzny pojęciowe – gospodarkę, środowisko naturalne, kulturę oraz społeczeństwo. Ewolucja skali zagrożeń pozamilitarnych jest rezultatem złożonych przemian oraz wynika z gwałtownej ingerencji człowieka w sferę środowiska naturalnego, która przyczynia się do eskalacji rozległych zakłóceń klimatycznych, degradacji ekosystemu, a także wzrostu częstotliwości pojawiania się nieprzewidywalnych anomalii pogodowych.

Bezpieczeństwo podmiotu społecznego jest zależne od czynników militarnych i warunków współczesnych przeobrażeń. Dalsze zagrożenia, identyfikowane wraz z procesami społecznymi lub kulturowymi, są przykładem równie silnego oddziaływania na jednostkę, która jest najsłabszym elementem struktury państwa. Współczesna klasyfikacja zagrożeń jest zbiorem stale otwartym, poszerzanym i modyfikowanym przez liczne ośrodki akademickie. W związku z powyższym środowiska utożsamiane z naukami społecznymi dostrzegają żywotną potrzebę nieprzerwanego prowadzenia badań oraz redefiniowania pojęć z obszaru bezpieczeństwa militarnego i pozamilitarnego.

Realizacja ustalonych kryteriów odbywa się przy udziale licznych instytucji, służb oraz formacji. Jedną z nich jest obrona cywilna (OC), która odpowiada za wypełnianie zadań humanitarnych odnoszących się między innymi do zapewniania ochrony ludności cywilnej przed różnorodnymi zagrożeniami.

Niniejszy artykuł przedstawia syntetyczne obserwacje dotyczące przebiegu epidemii COVID-19. Dodatkowo charakterystyka rozszerzonej współpracy licznych podmiotów z zakresu bezpieczeństwa staje się przyczynkiem do rozważań na temat stanu systemu ochrony ludności cywilnej w Polsce. W dalszej części Autor postanawia skupić się na znaczeniu oraz potencjalnej roli Wojsk Obrony Terytorialnej (WOT) w ramach formułowanej konieczności dostosowania omawianego systemu do postępujących przeobrażeń, a także oczekiwań społecznych. Zgodnie z przyjętą hipotezą badawczą, potencjał WOT umożliwia im większą partycypację w systemie ochrony ludności. Próba sprawdzenia zdolności oraz zdefiniowania wyzwań w obszarze rekonstrukcji polskiej obrony cywilnej może nakreślić perspektywę długo oczekiwanej nowej roli przytaczanych podmiotów w całościowym budowaniu powszechnego bezpieczeństwa Polski.

Intensyfikacja działań przeciwkryzysowych na przykładzie epidemii COVID-19

Pierwszy przypadek zachorowania na COVID-19 w Polsce został odnotowany 4 marca 2020 r. Zakażenie zdiagnozowano u mężczyzny z województwa lubuskiego, który kilka dni wcześniej wrócił z Niemiec. Ta informacja spowodowała, iż niemal od razu władze różnych szczebli oraz instytucji zaczęły implementować wielorakie środki ostrożności oraz działania zapobiegawcze – na przykład przekazywanie zaleceń Głównego Inspektora Sanitarnego dla uczelni wyższych w związku z potencjalnym ryzykiem rozprzestrzenienia się wirusa[2]. Fundamentalne decyzje legislacyjne na szczeblu centralnym przyjęto 2 marca 2020 r. w postaci ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[3]. Akt prawny, określany mianem specustawy, zmienił kształt kilkunastu innych ustaw. Prezes Rady Ministrów, starając się nie dopuścić do eskalacji zagrożenia, w dniu 11 marca 2020 r. zapowiedział ustanowienie, w ramach wymaganej profilaktyki, licznych ograniczeń w funkcjonowaniu życia społecznego i gospodarczego.

Zagrożenia związane z rozprzestrzenianiem się wirusa SARS-CoV-2, powodującego chorobę COVID-19, stosunkowo szybko stały się czynnikiem bezpośrednio wpływającym na bezpieczeństwo wewnętrzne Polski. Choć jest to stwierdzenie stosunkowo trywialne, to jednak może posłużyć jako wstęp do podjęcia próby zrozumienia działań odpowiednich struktur instytucjonalnych, które zostały wyznaczone do realizowania zadań związanych z minimalizowaniem negatywnych konsekwencji dla wspomnianego bezpieczeństwa. Warto zaznaczyć, iż stan epidemii, którym został objęty teren całego państwa, nie jest zjawiskiem częstym. Potencjał występujących zdarzeń nie wydawał się wysoko oceniany przez ośrodki decyzyjne przed rokiem 2020. Dodatkowo skala oraz nieprzewidywalność rozszerzającego się zagrożenia zaczęły implikować szereg wyzwań dla całego aparatu państwowego. Należy zatem przyjąć założenie, iż w tej niecodziennej rzeczywistości istotną zręcznością instytucji administracji publicznej powinno być takie zarządzanie dostępnymi siłami i środkami, aby w sposób najbardziej efektywny reagować na pojawiające się

---

[2] *Informacja Głównego Inspektora Sanitarnego dla uczelni w związku z potencjalnym ryzykiem zakażenia koronawirusem*, Ministerstwo Edukacji i Nauki, https://www.gov.pl/web/edukacja-i-nauka/informacja-glownego-inspektora-sanitarnego-dla-uczelni-w-zwiazku-z-potencjalnym-ryzykiem-zakazenia-koronawirusem [dostęp: 2.12.2022].

[3] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020 r., poz. 374. Ustawa weszła w życie 8 marca 2020 r.

niebezpieczeństwo, zachowując przy tym sprawność nieustannego i niezagrożonego funkcjonowania państwa[4].

Wojska Obrony Terytorialnej zostały utworzone 1 stycznia 2017 r. i są piątym rodzajem Sił Zbrojnych Rzeczypospolitej Polskiej[5]. Od momentu włączenia formacji w struktury wojskowe, WOT są na etapie intensywnego rozwoju – zarówno organizacyjnego, jak i szkoleniowego. Zgodnie z obowiązującym ustawodawstwem, WOT posiadają rozszerzający się potencjał dla prowadzenia działań z zakresu ochrony ludności cywilnej. W perspektywie eskalacji ewentualnych zagrożeń należy wyróżnić zwalczanie klęsk żywiołowych oraz likwidację ich skutków, ochronę mienia, a także uczestnictwo w akcjach poszukiwawczo-ratowniczych.

Charakterystyka WOT sprawiła, że żołnierze zostali skierowani w trybie pilnym do działań mających na celu ograniczenie rozprzestrzeniania się wirusa SARS-CoV-2. W dniu 13 marca 2020 r. Dowódca Wojsk Obrony Terytorialnej wprowadził istotną zmianę w modelu funkcjonowania WOT. Całość formacji przeszła w stan dwunastogodzinnej gotowości do działania, natomiast wybrane grupy żołnierzy o określonej specjalizacji weszły w tryb sześciogodzinnej gotowości[6]. Zwiększenie dyspozycyjności było pierwszą z serii decyzji, które następnie nakreśliły główne obszary przedsięwzięć w ramach operacji pod kryptonimem „Odporna Wiosna"[7].

Pierwsza zdefiniowana płaszczyzna działań obejmowała wspieranie służb, wojewodów, i władz samorządowych w zakresie zapobiegania rozprzestrzenianiu się koronawirusa oraz zapewniania opieki nad osobami starszymi, zakażonymi i przebywającymi na kwarantannie[8]. Decyzje administracji centralnej w ramach stanu zagrożenia epidemicznego oraz stanu epidemii sprawiły, iż w początkowym etapie rozwijającego się niebezpieczeństwa minister obrony narodowej postanowił włączyć Wojska Obrony Terytorialnej do służby lotniskowej. Zakres wykonywanych czynności skupiał się na przeprowadzaniu pomiarów temperatury oraz gromadzeniu i zarządzaniu kartami lokalizacyjnymi wszystkich osób przylatujących do Polski[9]. W miarę upływu czasu zaangażowane zasoby Wojska Polskiego współdziałały z jednostkami Straży Granicznej oraz brały udział w działaniach Policji, które polegały na kontrolowaniu

---

4 B. Włodarczyk, *Instytucje państwa polskiego wobec zagrożeń wywołanych przez epidemię COVID-19*, „Studia Polityczne" 2021, t. 49, nr 4, s. 69.

5 Obok Wojsk Obrony Terytorialnej w skład Sił Zbrojnych RP wchodzą: Wojska Lądowe, Siły Powietrzne, Marynarka Wojenna oraz Wojska Specjalne. Każdy z tych rodzajów wojsk dysponuje osobnym składem osobowym, uzbrojeniem, a także zakresem wykonywanych zadań.

6 *Odpowiedź WOT na COVID-19*, Wojsko Polskie, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2020-03-27j-odpowiedz-wot-na-covid-19 [dostęp: 2.12.2022].

7 A. Kukuła, *Działania Wojsk Obrony Terytorialnej w obliczu zagrożenia, jakim jest SARS-CoV-2*, „Zeszyty Naukowe PWSZ im. Witelona w Legnicy" 2020, nr 36, s. 27.

8 *Ibidem.*

9 *MON i wojsko zaangażowane w działania związane z zagrożeniem koronawirusem*, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/mon-i-wojsko-zaangazowane-w-dzialania-zwiazane-z-zagrozeniem-koronawirusem [dostęp: 2.12.2022].

tudzież wspieraniu osób objętych kwarantanną w miejscach izolacji. Żołnierze uczestniczyli również w procesach logistycznych, skupiających się na zapewnianiu placówkom służby zdrowia odpowiedniej ilości środków ochrony osobistej. Na terenie całego kraju zorganizowano wojskowe zgrupowania zadaniowe, które w ramach wymaganego wsparcia były w stanie rozdysponować specjalistyczny sprzęt medyczny. Utworzona struktura umożliwiła między innymi powstanie kontenerowego szpitala polowego we Wrocławiu. Prowadzone w trybie alarmowym czynności polegały także na natychmiastowej ewakuacji narażonych na zakażenie podopiecznych z Domów Pomocy Społecznej do zapasowych miejsc tymczasowego pobytu. W tym celu, na podstawie decyzji przedstawicieli resortu, w każdej brygadzie Obrony Terytorialnej (OT) zorganizowano zespoły interwencji kryzysowej, których głównym zadaniem było podjęcie natychmiastowych działań w razie potrzeb wynikających z ograniczeń ośrodków władz cywilnych. Następną płaszczyzną omawianych przedsięwzięć było egzekwowanie ograniczeń oraz restrykcji epidemicznych. Znacząca część policjantów została skierowana do czynności patrolowych mających zapewniać przestrzeganie obowiązującego ustawodawstwa. Dla odpowiedniej efektywności, działania patrolowo-interwencyjne zostały wzbogacone o żołnierzy WOT oraz Żandarmerii Wojskowej[10]. Ostatni obszary działań obejmował ograniczenie ryzyka transmisji koronawirusa w środowisku żołnierzy WOT i ich rodzin, a także prowadzenie edukacji personelu i otoczenia w zakresie profilaktyki i zapobiegania zakażeniom.

Przedstawiane zadania WOT wynikały w głównej mierze z bezprecedensowego zapotrzebowania oraz braku odpowiedniej skuteczności działań poszczególnych samorządów, służb państwowych oraz innych organizacji. Pierwotne lapidarne założenia zwracają uwagę na udzielanie niezbędnego wsparcia w realizacji ówczesnych potrzeb związanych z eskalacją zagrożenia epidemicznego. Z biegiem czasu zakres zadań wykonywanych przez ten komponent Sił Zbrojnych RP został rozbudowany do szerokiego spektrum czynności. Dodatkowo, w związku z koniecznością utrzymania efektywnego reagowania na powstałe zagrożenia, przedstawiciele brygad OT brali czynny udział w działaniach realizowanych przez podmioty odpowiedzialne za zarządzanie kryzysowe na szczeblu krajowym, wojewódzkim oraz powiatowym[11].

Wydarzenia związane z intensyfikacją zagrożenia epidemicznego pozwalają na przedstawienie cennych wartości operatywnego współdziałania w obszarze zapewniania bezpieczeństwa wewnętrznego Polski. Wymienione przykłady współpracy WOT z licznymi podmiotami państwowymi, których podstawowym celem było utrzymanie sprawnego zarządzania bezpieczeństwem, zwracają uwagę na

---

[10] *Policja egzekwuje przestrzeganie zasad w związku z epidemią koronawirusa*, Policja, https://www.policja.pl/pol/aktualnosci/186907,Policja-egzekwuje-przestrzeganie-zasad-wzwiazku-z-epidemia-koronawirusa.html?search=31896 [dostęp: 2.12.2022].

[11] K. Gąsiorek, A. Marek, *Działania Wojsk Obrony Terytorialnej podczas pandemii COVID-19 jako przykład wojskowego wsparcia władz cywilnych i społeczeństwa*, „Wiedza Obronna" 2020, nr 3, s. 70.

wzmocnienie efektywności oraz wzajemne uzupełnianie się w realizacji nałożonych obowiązków. Analizując czynności podjęte w ramach przeciwdziałania rozwojowi epidemii COVID-19 w Polsce, należy stwierdzić, iż w momencie pojawienia się sytuacji nadzwyczajnych Wojska Obrony Terytorialnej okazały się istotnym wsparciem na płaszczyźnie zagadnień pozamilitarnych. Obserwacje wskazują także, że w celu skutecznego reagowania na sytuacje kryzysowe instytucje państwowe potrzebują formacji zdolnych do elastycznego realizowania nałożonych zadań. W tym przypadku niezwykle istotnym czynnikiem potęgującym skuteczność omawianego podmiotu był fakt, że formacje WOT są budowane przy wykorzystaniu zasobów osobowych reprezentujących lokalne wspólnoty. Dlatego tak ważne jest pielęgnowanie wartości społeczeństwa obywatelskiego, bazującego na silnym przywiązaniu ochotników do miejsc pochodzenia, zgodnie z przyjętą maksymą WOT: „Zawsze gotowi, zawsze blisko".

Pomimo że Wojska Obrony Terytorialnej nadal są na etapie intensywnego tworzenia własnych struktur, zdecydowano o pilnym zaangażowaniu około 50% stanu osobowego w zmagania z epidemią COVID-19 na jej początkowym etapie. Uczestnictwo żołnierzy w akcji o kryptonimie „Odporna Wiosna" pozwoliło na sprawdzenie przyjętego kierunku rozwoju. Co więcej, WOT nawiązały relewantną współpracę z innymi formacjami służb mundurowych podległych ministrowi właściwemu do spraw wewnętrznych i administracji. W kontekście podjętej tematyki badawczej, WOT przyczyniły się do urzeczywistnienia praktycznego wymiaru ochronnego, polegającego na wspieraniu lokalnych społeczności. Tym samym stanowiły uzupełnienie w systemie ochrony ludności – niezbędne ze względu na długoletni brak sprawnie działającej obrony cywilnej oraz nieadekwatność sił i środków dostępnych cywilnym władzom centralnym i lokalnym.

Czy Wojska Obrony Terytorialnej mogą stać się nową formą obrony cywilnej?

Kontekst pojawienia się epidemii COVID-19 w Polsce mógł przyczynić się do interesujących obserwacji na temat kształtującej się roli Wojsk Obrony Terytorialnej. W opinii Autora brak należytego funkcjonowania obrony cywilnej skłonił decydentów do podjęcia działań doraźnych, skupiających się na właściwym reagowaniu na zaistniałe zagrożenie. Przywołana ekstraordynaryjna aktywność WOT stała się przyczynkiem do pytania badawczego stanowiącego tytuł niniejszej części artykułu. Aby uzyskać na nie odpowiedź, należy w szerszym zakresie przeanalizować genezę, a także cele związane z utworzeniem nowego rodzaju Sił Zbrojnych RP.

W Polskiej Rzeczypospolitej Ludowej system Obrony Terytorialnej miał wyrażać narodową siłę, niezależną od ośrodków decyzyjnych Układu Warszawskiego. Wojska Obrony Terytorialnej Kraju (OTK) zaczęto tworzyć dopiero na początku

lat 60. XX w. w celu poszerzenia zdolności oraz potencjału sił układu wewnętrznego państwa, funkcjonującego obok wojsk operacyjnych[12].

Jednostki OTK były przewidziane do realizacji różnorodnych zadań taktycznych w swoich rejonach odpowiedzialności. Systematycznie kształtujące się cele obejmowały działania w czasie pokoju i wojny. Omawiane formacje uczestniczyły w przygotowaniach do wykonywania bezpośrednich działań bojowych prowadzonych wspólnie z wojskami operacyjnymi, działań w strefie tyłowej oraz działań nieregularnych na terytorium opanowanym przez przeciwnika. Ponadto przewidywano istotną potrzebę doskonalenia procesów związanych z ochroną obiektów szczególnego znaczenia dla bezpieczeństwa, udzielaniem pomocy w likwidowaniu skutków uderzeń lotniczych i broni masowego rażenia oraz ze zwalczaniem skutków klęsk żywiołowych.

Niemniej jednak można było dostrzec procesy zmierzające do deprecjacji formacji OTK. Upowszechnił się pogląd o wojsku „drugiej kategorii", nadającym się wyłącznie do nieistotnych zadań. W związku z postępującymi przeobrażeniami struktur bezpieczeństwa oraz rozpoczętą redukcją Sił Zbrojnych po 1989 r. wojska lądowe OTK zostały rozformowane[13].

Następnie Polska długo należała do grupy nielicznych państw, które nie posiadały wojsk o opisywanej charakterystyce. Warto zaznaczyć, że niewielka, zaledwie pięciomilionowa Finlandia posiada ponad 200 000 ochotników Obrony Terytorialnej. Ochotnicza organizacja obronna jest także podstawą systemu bezpieczeństwa Szwecji. W związku z redukcją armii regularnej, dużą część zadań przejęła tam Gwardia Krajowa (*Hemvärnet*), licząca około 50 000 członków i podzielona zgodnie ze strukturą organizacyjną szwedzkiej administracji publicznej. Podobne rozwiązania funkcjonują także w innych państwach, takich jak Norwegia, Szwajcaria, Niemcy czy Izrael. Największą na świecie armię ochotniczą mają Stany Zjednoczone Ameryki. Jest ona znana jako Gwardia Narodowa i w czasie pokoju liczy prawie 360 000 żołnierzy (około 8% całości wojsk lądowych). W kontekście przyjętej tematyki należy wskazać na istotne zaangażowanie jej żołnierzy w przeciwdziałaniu i usuwaniu skutków huraganu Katrina w 2005 r.[14].

Długoletnie prace resortowe doprowadziły do stopniowego odbudowania Wojsk Obrony Terytorialnej. Aktualnie dowództwu WOT podlega 15 brygad OT, dwa centra szkoleniowe i batalion dowodzenia. Po pięciu latach od powołania WOT, potrzebę obrony i wspierania lokalnych społeczności realizuje ponad 32 000

---

[12] Z. Polcikiewicz, *Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski*, „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2016, nr 7, s. 405.

[13] *Ibidem.*

[14] Zob. K. Derlatka, *Rola amerykańskiej Gwardii Narodowej, wojska oraz sił NATO przed, w trakcie i po ustąpieniu huraganu Katrina*, [w:] *Oblicza wojny*, t. 2: *Armia kontra natura*, red. T. Grabarczyk, M. Pogońska-Pol, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2020, s. 359–377.

żołnierzy[15]. Według przyjętej koncepcji, WOT stanowią odpowiedź na pogarszającą się sytuację w środowisku bezpieczeństwa Polski. Celem strategicznym WOT jest „powszechne wojskowe przygotowanie i wykorzystanie zasobów ludzkich, materiałowych i przestrzeni lądowej do prowadzenia ochrony i obrony miejscowej na całym terytorium Polski dla zapewnienia skutecznego odstraszania, ochrony i obrony przed agresją i atakami grup terrorystycznych, a także niezwłocznego i skutecznego wsparcia władz i społeczeństwa w ratowaniu i zabezpieczeniu ludzi, mienia i środowiska w sytuacjach klęsk żywiołowych, katastrof technicznych i innych nieszczęść i potrzeb"[16].

Zgodnie z założeniami sformułowanymi przez ustawodawcę, Wojska Obrony Terytorialnej powinny być gotowe do realizacji zadań z zakresu zarządzania kryzysowego. W czasie pokoju zaangażowane formacje mają przeciwdziałać klęskom żywiołowym i likwidować ich skutki, prowadzić akcje ratownicze i poszukiwawcze, chronić zdrowie i życie ludzkie oraz mienie. Poza tym prowadzone rozbudowane szkolenia przygotowują żołnierzy OT do wykonywania ewentualnych działań antyterrorystycznych, w tym polegających na ochronie społeczności lokalnych przed skutkami ataków w cyberprzestrzeni. Inna aktywność WOT skupia się na utrzymywaniu powszechnej gotowości do obrony oraz kształtowaniu współpracy z elementami systemu bezpieczeństwa państwa, w tym szczególnie z wojewodami i organami samorządów terytorialnych. Dodatkowo należy wyróżnić przedsięwzięcia zmierzające do propagowania w społeczeństwie postaw patriotycznych i obronnych[17]. Natomiast w momencie eskalacji ewentualnego konfliktu zbrojnego WOT powinny gwarantować wsparcie dla regularnych pododdziałów, oddziałów i związków taktycznych Sił Zbrojnych RP w strefie bezpośrednich działań bojowych, głównie na płaszczyźnie obronnej. Ponadto zakłada się uzyskanie zdolności do skutecznego prowadzenia szerokich akcji nieregularnych, przeciwdywersyjnych i przeciwdesantowych[18].

Warto zaznaczyć, że wymienione przedsięwzięcia nie wyczerpują pełnej puli zadań możliwych do realizacji przez WOT – ten nowy rodzaj Sił Zbrojnych RP jest wciąż na początkowym etapie budowania i realizuje założenia szkoleniowe. Należy dostrzec ewentualną korzyść z kształtowania się nowych koncepcji wykorzystania szczególnego potencjału Wojsk Obrony Terytorialnej.

---

[15] *Wojska Obrony Terytorialnej*, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-terytorialnej- [dostęp: 2.12.2022].

[16] J. Marczak, R. Jakubczak, *Raport strategiczny: Siły Zbrojne RP w drugiej dekadzie XXI wieku. Koncepcja strategiczna Obrony Terytorialnej RP*, Akademia Obrony Narodowej, Warszawa 2014, s. 74.

[17] *Zadania WOT*, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/zadania-wot [dostęp: 2.12.2022].

[18] J. Tomaszewski, *Formowanie Wojsk Obrony Terytorialnej*, „Wrocławskie Studia Politologiczne", 2019, t. 26, s. 72.

Porównanie WOT i obrony cywilnej pokazuje wyraźne podobieństwa na płaszczyźnie niektórych aktywności, skoncentrowanych wokół ochrony ludności i mienia przed skutkami klęsk żywiołowych, kształtowania w społeczeństwie właściwych postaw obywatelskich i utrzymywania wartościowej współpracy w ramach struktur bezpieczeństwa wewnętrznego Polski. W związku z powyższym można przyjąć założenie, że w pewnym zakresie Wojska Obrony Terytorialnej sukcesywnie stają się podmiotem realizującym zadania, które leżą w kompetencjach obrony cywilnej. Dodatkowo potwierdzają to przywołane wydarzenia związane z eskalacją zagrożenia epidemicznego.

Dla pełnowartościowej analizy sytuacji należy odnieść się też do warunków wojennych. W tym kontekście prezentowane podobieństwa tracą swoją moc, przede wszystkim ze względu na wyraźnie odmienne uwarunkowania potencjalnych przedsięwzięć, które są definiowane na wypadek wybuchu konfliktu zbrojnego, i całkowicie militarny charakter formacji WOT. Zgodnie z założeniami prawa międzynarodowego, odnoszącego się do utrzymania rozdzielenia struktur OC od ośrodków wojskowych, jednostki OT nie mogą pełnić funkcji pełnowartościowej obrony cywilnej. Potwierdzeniem powyższych obserwacji jest wypowiedź Grzegorza Matyasika, byłego zastępcy dyrektora Rządowego Centrum Bezpieczeństwa, który wskazał, że: „[...] przejęcie zadań obrony cywilnej przez WOT to nie jest dobre rozwiązanie, bo jest obarczone wieloma ryzykami. Obronę cywilną chronią przepisy prawa międzynarodowego i trudno sobie wyobrazić, by w trakcie wojny zadania te wykonywali żołnierze w mundurach z przewieszonymi przez plecy karabinkami. Na myśli mam nie przejęcie tych zadań przez WOT, a ewentualne wsparcie, jakiego ta formacja może – w sytuacji kryzysowej – udzielić. Oczywiście, wyjściem idealnym byłoby, gdybyśmy mieli formacje ochrony ludności, które w trakcie konfliktu zmieniają się w formacje obrony cywilnej kraju, a zbyt duże zaangażowanie wojska jest w pewnym sensie niepożądane, ale pod względem systemowym «spięcie» tych dwóch porządków – militarnego i pozamilitarnego – jest naprawdę konieczne. Te zadania obronne w części się pokrywają, więc nierozsądnym, chociażby biorąc pod uwagę koszty, byłoby ich dublowanie”[19].

Wielokrotne przywoływanie problematyki polskiej obrony cywilnej kieruje tym samym uwagę na pilną potrzebę określenia działań zmierzających do podwyższenia standardów w tym zakresie. Ze względu na coraz silniejsze poparcie polityczne oraz społeczne dla Wojsk Obrony Terytorialnej Autor dostrzega możliwość częstszego wykorzystywania formacji WOT w czasie pokoju w charakterze obrony cywilnej. Niemniej jednak urzeczywistnienie proponowanych praktyk musiałoby się wiązać z przyjęciem przez decydentów politycznych odpowiednich regulacji prawnych, które formułowałyby szerszy zakres kompetencji WOT, obejmujący też zobowiązania

[19] D. Mikołajczyk, *Wicedyrektor RCB: potrzebny system, w którym każdy obywatel wie, co w razie kryzysu, wojny ma robić, jakie ma zadania*, InfoSecurity24, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/wicedyrektor-rcb-potrzebny-system-w-ktorym-kazdy-obywatel-wie-co-w-razie-kryzysu-wojny-ma-robic-jakie-ma-zadania [dostęp: 2.12.2022].

odnoszące się na przykład do zabudowań ochronnych. Rosnący potencjał Wojsk Obrony Terytorialnej sprawia, że możliwy staje się scenariusz zakładający rzeczywiste zwiększenie operatywności systemu ochrony ludności.

Podsumowanie

Wydarzenia związane z wystąpieniem zagrożeń epidemicznych pozwalają na przedstawienie analizy intensywnego współdziałania wielu podmiotów w obszarze utrzymywania bezpieczeństwa wewnętrznego Polski. Wojska Obrony Terytorialnej zapewniły w tym czasie istotne uzupełnienie konstrukcji bezpieczeństwa. W ramach akcji „Odporna Wiosna" brygady OT aktywnie uczestniczyły w przedsięwzięciach ochronnych. Dzięki efektywnemu realizowaniu postawionych zadań, WOT potwierdziły zdolność do elastycznego dostosowywania się do ekstraordynaryjnych warunków. Zwraca uwagę wzmocnienie efektywności dzięki współpracy różnych formacji w trakcie realizacji obowiązków w celu utrzymania *utilitas publica*.

Przytaczane przedsięwzięcia, choć bez wątpienia są źródłem cennego doświadczenia, mają jednak również inny, mniej pozytywny kontekst. Niebezpieczeństwa wynikające z rozprzestrzeniania się wirusa SARS-CoV-2 w pewnym zakresie nadwyrężyły struktury państwa polskiego. Częste angażowanie różnych formacji w ramach szerokiej współpracy potwierdza powszechną wiedzę na temat niewystarczających zasobów sił i środków, które dotyczą między innymi struktur OC, Policji oraz Straży Granicznej. Wydarzenia związane z epidemią COVID-19 winny stać się początkiem poważnej debaty na temat poprawy sytuacji (przede wszystkim kadrowej) wielu podmiotów dbających o powszechne bezpieczeństwo. W innym wypadku zdarzenia o podobnej lub poważniejszej skali mogą stanowić wyzwanie, które jeszcze bardziej nadwyręży system bezpieczeństwa wewnętrznego.

Przedstawiona tematyka nie uzyskała silnej obecności w dotychczasowej literaturze przedmiotu. Może to wynikać ze znaczącej abstrakcyjności wybrzmiewających założeń. Tym niemniej zagrożenia związane z epidemią COVID-19 uintensywniają potrzebę poszukiwania nowych rozwiązań w kwestii zapewniania ochrony ludności cywilnej. Warto ponownie zaznaczyć, że pojawienie się epidemii poddało poważnej próbie znaczną część instytucji publicznych ze względu na nieadekwatność posiadanych przez nie sił i środków. Potwierdziły się także wielokrotnie formułowane zastrzeżenia co do braku właściwej konstrukcji obrony cywilnej, która mogłaby przyczynić się do zminimalizowania negatywnych skutków zagrożeń epidemicznych lub związanych z klęskami żywiołowymi. Na podstawie nakreślonych obserwacji Autor dostrzega silny potencjał przeprowadzenia częściowej rekonstrukcji polskiej obrony cywilnej poprzez odpowiednie przeformatowanie zadań Wojsk Obrony Terytorialnej w czasie pokoju.

Bibliografia

Derlatka K., Rola *amerykańskiej Gwardii Narodowej, wojska oraz sił NATO przed, w trakcie i po ustąpieniu huraganu Katrina*, [w:] *Oblicza wojny*, t. 2: *Armia kontra natura*, red. T. Grabarczyk, M. Pogońska-Pol, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2020, s. 359–377.

Gąsiorek K., Marek A., *Działania Wojsk Obrony Terytorialnej podczas pandemii COVID-19 jako przykład wojskowego wsparcia władz cywilnych i społeczeństwa*, „Wiedza Obronna" 2020, nr 3, s. 61–75.

Informacja Głównego Inspektora Sanitarnego dla uczelni w związku z potencjalnym ryzykiem zakażenia koronawirusem, Ministerstwo Edukacji i Nauki, https://www.gov.pl/web/edukacja-i-nauka/informacja-glownego-inspektora-sanitarnego-dla-uczelni-w-zwiazku-z-potencjalnym-ryzykiem-zakazenia-koronawirusem [dostęp: 2.12.2022].

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Wydawnictwo AON, Warszawa 2011.

Kukuła A., *Działania Wojsk Obrony Terytorialnej w obliczu zagrożenia jakim jest SARS-CoV-2*, „Zeszyty Naukowe PWSZ im. Witelona w Legnicy" 2020, nr 36, s. 17–31.

Marczak J., Jakubczak R., *Raport strategiczny: Siły Zbrojne RP w drugiej dekadzie XXI wieku. Koncepcja strategiczna Obrony Terytorialnej RP*, Akademia Obrony Narodowej, Warszawa 2014.

Mikołajczyk D., *Wicedyrektor RCB: potrzebny system, w którym każdy obywatel wie, co w razie kryzysu, wojny ma robić, jakie ma zadania*, InfoSecurity24, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/wicedyrektor-rcb-potrzebny-system-w-ktorym-kazdy-obywatel-wie-co-w-razie-kryzysu-wojny-ma-robic-jakie-ma-zadania [dostęp: 2.12.2022].

MON i wojsko zaangażowane w działania związane z zagrożeniem koronawirusem, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/mon-i-wojsko-zaangazowane-w-dzialania-zwiazane-z-zagrozeniem-koronawirusem [dostęp: 2.12.2022].

Odpowiedź WOT na COVID-19, Wojsko Polskie, https://www.wojsko-polskie.pl/articles/tym-zyjemy-v/2020-03-27j-odpowiedz-wot-na-covid-19 [dostęp: 2.12.2022].

Polcikiewicz Z., *Wojska Obrony Terytorialnej w systemie bezpieczeństwa narodowego Polski*, „Acta Scientifica Academiae Ostroviensis. Sectio A, Nauki Humanistyczne, Społeczne i Techniczne" 2016, nr 7, s. 399–413.

Policja egzekwuje przestrzeganie zasad w związku z epidemią koronawirusa, Policja, https://www.policja.pl/pol/aktualnosci/186907,Policja-egzekwuje-przestrzeganie-zasad-wzwiazku-z-epidemia-koronawirusa.html?search=31896 [dostęp: 2.12.2022].

Tomaszewski J., *Formowanie Wojsk Obrony Terytorialnej*, „Wrocławskie Studia Politologiczne" 2019, t. 26, s. 70–87.

Włodarczyk B., *Instytucje państwa polskiego wobec zagrożeń wywołanych przez epidemię COVID-19*, „Studia Polityczne" 2021, t. 49, nr 4, s. 63–86.

Wojska Obrony Terytorialnej, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/wojska-obrony-terytorialnej- [dostęp: 2.12.2022].

Zadania WOT, Ministerstwo Obrony Narodowej, https://www.gov.pl/web/obrona-narodowa/zadania-wot [dostęp: 2.12.2022].

Akty prawne

Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020 r., poz. 374.

Wojska Obrony Terytorialnej jako element rekonstrukcji polskiej obrony cywilnej
Streszczenie

Wydarzenia ostatnich kilku lat sprawiają, iż kontekst ochrony ludności cywilnej w Polsce niezaprzeczalnie zyskuje na znaczeniu. Świadczy o tym również fakt zintensyfikowania prac legislacyjnych zmierzających do ustanowienia nowego prawa w obszarze obrony cywilnej, zarządzania kryzysowego oraz stanu klęski żywiołowej. W związku z powyższym Autor niniejszego artykułu postanowił przedstawić aktywność Wojsk Obrony Terytorialnej, a także najważniejsze założenia w tym obszarze tematycznym, który wymaga rzeczywistych i pilnych przeobrażeń. Jednym z podejmowanych przykładów jest czas epidemii COVID-19, który zmusił decydentów licznych instytucji państwowych do zastosowania ekstraordynaryjnych rozwiązań. Artykuł stanowi szczegółową analizę roli Wojsk Obrony Terytorialnej w ramach szerszej struktury ochrony ludności, a także warunków związanych z wprowadzeniem stanu epidemii. Syntetyczne wnioski z przeprowadzonego badania wskazują na wyraźny potencjał WOT w ramach oczekiwanej rekonstrukcji polskiej obrony cywilnej.

Słowa kluczowe: bezpieczeństwo państwa, obrona cywilna, Wojska Obrony Terytorialnej, WOT, COVID-19

Territorial Defence Forces as part of the reconstruction of Polish civil defence
Abstract

The events of the past few years make the context of civil protection in Poland undeniably gaining importance. This is also evidenced by the fact that legislative work has intensified, aimed at establishing a new law in the area of civil defence, crisis management and state of natural disaster. In view of the above, the author of this article decided to present the activity of the Territorial Defence Forces (Polish: Wojska Obrony Terytorialnej), and also to apply the most important assumptions to the subject area in need of real and urgent transformation. One of the examples taken is the time of the COVID-19 epidemic, which obliged decision-makers of numerous state institutions to apply extraordinarily coordinated solutions. The article is a detailed analysis of the role of the Territorial Defence Forces within the broader population protection structure, as well as the conditions resulting from the introduced epidemic state. Synthetic conclusions resulting from the study indicate the clear potential of the TDF as part of the expected reconstruction of Polish civil defence.

Keywords: state security, civil defence, Polish Territorial Defence Forces, TDF, WOT, COVID-19

Sprawozdania

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-011

Anna Bałamut
dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0001-7300-7367

Krzysztof Waśniewski
dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-0076-4804

Krynica Forum 13–15 września 2023 r. w Krynicy-Zdroju. Aspekty bezpieczeństwa

Krynica Forum to spotkania nie tylko ludzi biznesu, ale też polityki i świata akademickiego. Hasłem konferencji w 2023 r. było: *Empowering the Region*. Stwierdzenie to odnosi się do obszaru geograficznego zarówno Europy Środkowo-Wschodniej, jak i Małopolski. Obrady miały miejsce w dniach 13–15 września 2023 r. i zostały podzielone na 7 ścieżek programowych na 8 scenach (około 100 paneli). Tematyka dotyczyła m.in. takich zagadnień jak: Bezpieczeństwo strategiczne; Bezpieczeństwo energetyczne; Bezpieczeństwo klimatyczne; Ukraina – wsparcie, współpraca, odbudowa; Forum Koreańsko-Polskie; Biznes i gospodarka; Patrząc w przyszłość.

Wydarzenie zostało wsparte przez prelegentów z takich uczelni jak: Uniwersytet Ekonomiczny w Krakowie, Akademia Górniczo-Hutnicza, Uniwersytet Rolniczy w Krakowie, Politechnika Krakowska i Politechnika Rzeszowska, Wyższa Szkoła Biznesu – National Louis University w Nowym Sączu, Uniwersytet Jagielloński, Szkoła Główna Handlowa, Polska Akademia Nauk, Akademia Sztuki Wojennej, Uniwersytet Łódzki czy Krakowska Akademia im. Andrzeja Frycza Modrzewskiego. Dodatkowo zorganizowano debaty przy współudziale Narodowej Rady Rozwoju przy Prezydencie RP, Biura Bezpieczeństwa Narodowego oraz Klubu Jagiellońskiego, a w ramach tzw. Forum Koreańsko-Polskiego nastąpiło spotkanie Prezydenta RP Andrzeja Dudy i premiera Republiki Korei Han Duck-soo.

W ramach trzydniowej konferencji na szczególną uwagę zasłużyły panele z dwóch ścieżek programowych: „Bezpieczeństwo energetyczne" i „Bezpieczeństwo klimatyczne". W pierwszym dniu konferencji, tj. 13 września w ramach ścieżki „Bezpieczeństwo klimatyczne" miał miejsce panel: „Nauka i edukacja w służbie transformacji energetycznej. Jak kształcić kadry zielonej transformacji?" z udziałem takich gości jak: Jan Tabor (zastępca dyrektora generalnego Lasów Państwowych ds. Gospodarki Leśnej), Arkadiusz Sekściński (prezes Zarządu, PGE Baltica Sp. z o.o.), Jakub Bator (wiceprezydent Confederation of European Waste-to-Energy Plants – CEWEP), dr hab. Katarzyna Jasikowska, prof. UJ (koordynatorka Rady Klimatycznej Uniwersytetu Jagiellońskiego), Marta Malec-Lech (członek Zarządu Województwa Małopolskiego) oraz Jacek Bańka (moderator, kierownik redakcji publicystyki Radia Kraków).

W drugim panelu „Na straży środowiska. Jakie są najpoważniejsze wyzwania dla samorządów, jeśli chodzi o ochronę zasobów środowiska naturalnego?" wzięli udział: Damian Sieber (dyrektor Regionalnej Dyrekcji Lasów Państwowych w Katowicach), Piotr Ziętara (prezes Zarządu Wodociągów Miasta Krakowa S.A.), Kazimierz Koprowski (prezes Zarządu Wojewódzkiego Funduszu Ochrony Środowiska i Gospodarki Wodnej w Krakowie) oraz Marcin Koczyba (moderator, Radio Kraków).

Trzeci panel stanowił panel patronacki Lasów Państwowych: „Nasz Zielony Ład. Polski model gospodarki leśnej". W dyskusji wzięli udział: Józef Kubica (dyrektor generalny Lasów Państwowych), prof. Jarosław Socha (kierownik Katedry Zarządzania Zasobami Leśnymi, Uniwersytet Rolniczy w Krakowie), dr Luiza Tymińska-Czabańska (adiunktka w Katedrze Zarządzania Zasobami Leśnymi na Wydziale Leśnym Uniwersytetu Rolniczego im. H. Kołłątaja w Krakowie) oraz Maksymilian Wysocki (moderator, Fratria).

W ramach ścieżki „Bezpieczeństwo energetyczne" pierwszy panel nosił tytuł: „Derusyfikacja europejskiej energetyki – realny cel czy utopia?". Wzięli w nim udział: Agnieszka Kaźmierczak (dyrektor generalny Agencji Dostaw Euratomu – Europejskiej Wspólnoty Energii Atomowej), Paweł Strączyński (wiceprezes Zarządu Banku Pekao S.A., nadzoruje Pion Finansowy), dr hab. Tomasz Młynarski, prof. UJ (ekspert w zakresie współpracy energetycznej w Unii Europejskiej), Magdalena Maj (kierownik zespołu Klimatu i Energii w Polskim Instytucie Ekonomicznym) oraz Michał Niewiadomski (moderator, założyciel Klubu Energetycznego, publicysta energetyczno-klimatyczny).

Drugie spotkanie to panel patronacki PGE Polska Grupa Energetyczna S.A.: „Stabilna energia, niskie rachunki – czy to możliwe?". Wzięli w nim udział: Arkadiusz Wronka (dyrektor wykonawczy ds. obrotu w Tauron Polska Energia S.A.), Andrzej Bondyra (wiceprezes Zarządu Agencji Rynku Energii S.A.) oraz Agnieszka Łakoma (moderator, Fratria).

W pierwszym dniu konferencji miał także miejsce panel pt. „Dobry klimat dla innowacji – jak go budować?" z udziałem: dra inż. Jarosława Bułki (pełnomocnik

Prezydenta Miasta Krakowa ds. transformacji cyfrowej), Kazimierza Murzyna (prezes Fundacji Klaster LifeScience Kraków i dyrektor zarządzający inicjatywy Klaster LifeScience Kraków, członek grupy strategicznej SCANBALT), Macieja Mroza (wiceprezes Zarządu ds. Operatora TAURON Dystrybucja), prof. Jana Tadeusza Dudy (przewodniczący Sejmiku Województwa Małopolskiego), dra Krzysztofa Waśniewskiego (doktor nauk ekonomicznych, wykładowca w Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego) oraz Doroty Rojek-Koryzny (moderator, Radio Kraków). Podczas panelu omawiano tworzenie przyjaznego środowiska dla innowacyjnych przedsiębiorstw, w tym rolę rządu oraz samorządów lokalnych. Dyskusji poddano również systemowe wsparcie dla polskich firm prowadzących badania i rozwijających innowacyjne technologie. Poddano analizie programy edukacyjne i szkoleniowe samorządów dla kształcenia kadr innowacyjnej gospodarki, jak również polityki publiczne dla wsparcia badań naukowych i współpracy uczelni z przemysłem. Uczestnicy debatowali też nad tworzeniem partnerstw między sektorem publicznym, prywatnym i akademickim w celu promowania innowacyjności, w tym nad tworzeniem inkubatorów przedsiębiorczości i parków technologicznych na poziomie lokalnym i regionalnym.

W drugim dniu konferencji w ramach ścieżki „Bezpieczeństwo klimatyczne" miały miejsce dwa panele pod patronatem Jastrzębskiej Spółki Węglowej. Pierwszy nosił tytuł: „Polskie drogi do neutralności klimatycznej. Cele, kierunki i inspirujące przykłady". Wzięli w nim udział: Marek Wesoły (sekretarz stanu w Ministerstwie Aktywów Państwowych, pełnomocnik rządu do spraw transformacji spółek energetycznych i górnictwa węglowego), Artur Badylak (dyrektor Biura Odmetanowania i Gospodarki Metanem w Jastrzębskiej Spółce Węglowej), prof. Stanisław Prusek (dyrektor Głównego Instytutu Górnictwa – Państwowego Instytutu Badawczego), prof. Marek Borowski (Akademia Górniczo-Hutnicza w Krakowie, Wydział Inżynierii Lądowej i Gospodarki Zasobami, Katedra Inżynierii Środowiska) oraz Tomasz Cudny (moderator, prezes Zarządu Jastrzębskiej Spółki Węglowej S.A.).

Drugi panel nosił nazwę „Własne surowce – kapitał na trudne czasy?". Wzięli w nim udział: Paweł Sałek (doradca Prezydenta RP), Piotr Chęciński (dyrektor ds. komunikacji korporacyjnej KGHM Polska Miedź S.A.), Krzysztof Janusz Kozik (polski polityk, samorządowiec, górnik i związkowiec, poseł na Sejm VIII i IX kadencji), Robert Ostrowski (zastępca prezesa Zarządu ds. Ekonomicznych, JSW S.A.), Wojciech Łabus (partner associate, KPMG w Polsce) oraz Agnieszka Łakoma (moderator, Fratria).

Trzeci panel odbył się pod patronatem Narodowej Rady Rozwoju przy Prezydencie Rzeczypospolitej Polskiej. Miał on tytuł: „Globalne ocieplenie – jak podejście do zmian klimatu wpłynie na przewagi konkurencyjne UE i państw członkowskich". Głos zabrali: Paweł Sałek (doradca Prezydenta RP), Jan Tabor (zastępca dyrektora generalnego Lasów Państwowych ds. Gospodarki Leśnej) oraz Paweł Mzyk (zastępca

dyrektora ds. zarządzania emisjami w Instytucie Ochrony Środowiska; Rada ds. Środowiska, Energii i Zasobów Naturalnych przy Prezydencie RP).

W ramach ścieżki „Bezpieczeństwo energetyczne" miał miejsce panel patronacki KGHM Polska Miedź S.A.: „Polski atom. Co oznacza dla nas zwrot ku energetyce jądrowej?". W spotkaniu wzięli udział: Jacek Sasin (Minister Aktywów Państwowych), Piotr Podgórski (dyrektor naczelny ds. transformacji w KGHM Polska Miedź S.A), Dawid Jackiewicz (wiceprezes Zarządu Orlen Synthos Green Energy), Jakub Rybicki (prezes PGE PAK Energia Jądrowa S.A.) oraz Agnieszka Łakoma (moderator, Fratria).

Drugi panel nosił tytuł „Bezpieczeństwo energetyczne Polski. Debata z udziałem przedstawicieli klubów parlamentarnych", tj. Rafała Komarewicza (Polska 2050, przewodniczący Rady Miasta Krakowa), Filipa Kaczyńskiego (poseł na Sejm RP) oraz Jacka Bańki (moderator, kierownik redakcji publicystyki Radia Kraków).

W trzecim dniu konferencji w ramach ścieżki „Bezpieczeństwo klimatyczne" miała miejsce debata Narodowej Rady Rozwoju przy Prezydencie Rzeczypospolitej Polskiej pod patronatem Lasów Państwowych: „Między suwerennością a centralizacją. Czy Polska może kształtować własną politykę w sektorze środowiska (klimat, przyroda, lasy, sprawiedliwa transformacja)?". Swoją obecnością zaszczyciły panel następujące osoby: Edward Siarka (sekretarz stanu w Ministerstwie Klimatu i Środowiska, pełnomocnik rządu ds. leśnictwa i łowiectw), Marek Marecki (dyrektor Regionalnej Dyrekcji Lasów Państwowych w Krośnie) oraz prof. Krystian Szczepański (dyrektor Instytutu Ochrony Środowiska – Państwowego Instytutu Badawczego).

W ramach ścieżki „Bezpieczeństwo energetyczne" odbyła się dyskusja na temat: „Czy dekarbonizacja polskiej energetyki jest możliwa bez atomu?". W spotkaniu głos zabrali: Tadeusz Widuch (dyrektor projektu, TAURON Nowe Technologie), dr inż. Paweł Gajda (ekspert w zakresie energetyki jądrowej), Zuzanna Nowak (dyrektor ds. analiz w The Opportunity Institute for Foreign Affairs), dr Anna Bałamut (adiunktka Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego) oraz Michał Niewiadomski (moderator, założyciel Klubu Energetycznego, publicysta energetyczno-klimatyczny).

Dyskusja w ramach ścieżek programowych „Bezpieczeństwo energetyczne" i „Bezpieczeństwo klimatyczne" toczyła się wokół problemu budowy w Polsce elektrowni atomowej oraz SMR-ów (*Small Modular Reactors*), czyli małych modułowych reaktorów jądrowych. Dyskutowano, które rozwiązanie jest właściwe i dlaczego. Mówiono o problemie dezinformacji oraz o roli edukacji w kształtowaniu odpowiednich postaw społecznych. Podkreślano, że problem bezpieczeństwa energetyczno-ekologicznego powinien być celem ponadpartyjnym. Mówiono o przechowywaniu energii w wodorze i konwertowaniu jej do amoniaku, jako formie łatwiejszej do przechowywania i transportu. Dyskutowano nad pojęciami „surowce strategiczne" i „surowce krytyczne", podkreślając, że nie są to pojęcia tożsame. Dodatkowo pojawienie się na

takiej liście nie daje pewnego źródła finansowania ze środków unijnych. Bezpieczeństwo energetyczne w swej definicji zakłada bowiem stabilne dostawy po akceptowalnych cenach. Podkreślano, że transformacja energetyczna zaczyna się kilometr pod ziemią, dlatego też trzeba zwrócić uwagę na potencjał takich surowców jak np. węgiel koksowy. Zaznaczano, że zmiany dotyczące niskoemisyjności UE to zmiany kluczowe dla bezpieczeństwa energetyczno-ekologicznego, jednakże dzieją się one zbyt szybko z uwagi na różnorodność miksów energetycznych krajów członkowskich, w tym Polski. Niskoemisyjność niesie za sobą wyrzeczenia oraz wysokie koszty dla gospodarki – takie informacje pojawiają się już nawet w prasie niemieckiej, gdzie mówi się, że transformacja energetyczna będzie kosztować nie tylko rządy państw, ale także przedsiębiorców i społeczeństwo. Z tą myślą trzeba się oswoić. Przykładem może być chociażby kwestia ETS-ów jako element zachwiania się konkurencyjności w przestrzeni UE i krajów członkowskich. Dlaczego? Ponieważ w konsekwencji rozwiązanie to wymusza kształt miksu energetycznego, a przecież państwa członkowskie UE mają utożsamiać się z polityką i strategią Unii, ale w ich gestii pozostaje prawo decydowania o sposobie i źródłach pozyskania energii.

BEZPIECZEŃSTWO TEORIA I PRAKTYKA SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-012

Anna Bałamut

dr, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0001-7300-7367

Izabela Kapera

dr hab., prof. KAAFM, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
https://orcid.org/0000-0003-1691-5275

Ogólnopolska konferencja naukowa „Zarządzanie w układzie przedsiębiorstwo – miasto – region w zmiennym otoczeniu. Wpływ współczesnych zagrożeń", Kraków, 19–20 czerwca 2023 r.

Ogólnopolska konferencja naukowa pt. „Zarządzanie w układzie przedsiębiorstwo – miasto – region w zmiennym otoczeniu. Wpływ współczesnych zagrożeń" odbyła się w formie zdalnej w dniach 19–20 czerwca 2023 r. Jej organizatorami byli: Wydział Zarządzania i Komunikacji Społecznej Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego oraz Towarzystwo Naukowe Organizacji i Kierownictwa – Oddział w Kielcach przy udziale partnera: Wydziału Zarządzania i Modelowania Komputerowego Politechniki Świętokrzyskiej. Patronat honorowy nad konferencją objął Rektor Krakowskiej Akademii prof. KAAFM dr Klemens Budzowski.

Pierwszego dnia konferencja miała charakter teoretyczny, natomiast drugiego celem było omówienie zagadnień od strony praktycznej. W sesji pierwszej „Zarządzanie" moderatorem był prof. dr hab. Andrzej Chodyński reprezentujący Krakowską Akademię im. Andrzeja Frycza Modrzewskiego (KAAFM), a udział wzięli zarówno przedstawiciele nauki, jak i instytucji samorządowych oraz przedsiębiorstw.

Instytucje i przedsiębiorstwa były reprezentowane przez dra hab. inż. Adama Jabłońskiego, prof. UWSB MERITO, i dra hab. inż. Marka Jabłońskiego, prof. UWSB MERITO (przedstawicieli Uniwersytetu WSB MERITO) oraz Sławomira Kamińskiego (prezes Zarządu, dyrektor Spółki Przedsiębiorstwo Energetyki Cieplnej Sp. z o.o.). Przedstawili oni zagadnienia teoretyczne dotyczące *Strategii bezpieczeństwa elektroenergetycznego regionu z udziałem klastra innowacji energetycznych na przykładzie miasta Bytom*. Podkreślili przy tym, że nowy wymiar prowadzenia biznesu w okresie kryzysów społecznych, gospodarczych, politycznych, klimatycznych, zdrowotnych, imigracyjnych czy militarnych generuje nowe potrzeby i nowe rozwiązania, które powinny implementować organizacje oraz gminy chcące nie tylko przetrwać, ale przede wszystkim zapewniać swój rozwój, będąc także odpornymi na wymienione kryzysy. Specyficzna sprężystość podmiotów powinna być osadzona we właściwie przyjętej i dobrze rozumianej perspektywie strategicznej. W wystąpieniu dotyczącym *Społecznych i ekologicznych aspektów audytów – od ECSR do ESG* prof. Andrzej Chodyński i mgr Wojciech Huszlak (KAAFM) skupili się na możliwości wykorzystania audytu w realizacji koncepcji ECSR (*Environmental Corporate Social Responsibility*) w ramach doskonalenia organizacji, uwzględniając działania na rzecz doskonałości procesowej. Temat *Zarządzania łańcuchem dostaw w sektorze energetycznym w Polsce* przedstawiła dr Anna Bałamut (KAAFM); referat miał na celu wskazanie, czym jest odpowiedzialne zarządzanie łańcuchem dostaw. Polega ono na integracji kluczowych procesów biznesowych od początkowych dostawców do końcowych użytkowników, którzy dostarczają produkty, usługi i informacje oraz dodają wartości dla klientów i innych interesariuszy łańcucha dostaw. Dr Michał Leśniewski (KAAFM) przedstawił z kolei zagadnienie dotyczące *Myślenia elastycznego menedżerów w procesie podejmowania decyzji – spojrzenie teoretyczno-koncepcyjne*. Podkreślił w nim, że menedżer jako osoba odpowiedzialna za proces zarządzania musi kierować się w swoich decyzjach myśleniem, które ma ukierunkować organizację na tory rozwoju, postępu. Kolejne wystąpienie dotyczyło *Zagrożeń w otoczeniu biznesowym – kapitał intelektualny – audit. Perspektywa praktyków* – dr Wioletta Zając i dr Agnieszka Giszterowicz (przedstawicielki KAAFM) określiły identyfikację zagrożeń otoczenia biznesowego oraz wskazały rolę, jaką kapitał intelektualny może pełnić w przeciwdziałaniu tym zagrożeniom. Zagadnienie *Funkcji i roli controllingu w zwinnej firmie produkcyjnej* przestawili dr hab. Janusz Nesterak, prof. UEK (Uniwersytet Ekonomiczny w Krakowie), dr Angelika Wodecka-Hyjek (Uniwersytet Ekonomiczny w Krakowie) oraz mgr Ewa Bąchor (KAAFM). Kolejne wystąpienie miało na celu przybliżenie działania *Systemów informatycznych wspomagających zarządzanie szkołą: dziennik elektroniczny na przykładzie oprogramowania Librus SYNERGIA* – jego autorami byli dr Dominik Borowski i dr inż. Renata Uryga (przedstawiciele KAAFM). Ostatnie wystąpienie dotyczyło *Systemów monitorowania realizacji celów SDG's w Polsce – stan obecny i wyzwania* – dr hab. Agnieszka Piotrowska-Piątek, prof. PŚk (Politechnika

Świętokrzyska) podjęła problematykę monitorowania realizacji celów zrównoważonego rozwoju (SDG) w Polsce. Zaprezentowała stan obecny oraz kierunki rozwoju systemu monitorowania SDG, proces tworzenia Krajowej Platformy Raportującej SDG, a także wyzwania związane z pomiarem zrównoważonego rozwoju.

W ramach dyskusji potwierdzono kontynuację i potrzebę współpracy pomiędzy pracownikami KAAFM reprezentującymi dyscyplinę nauk o zarządzaniu i jakości z jednostkami administracji publicznej, przedsiębiorstwami i organizacjami non profit.

Moderatorem sekcji drugiej – „Zarządzanie Marketingiem" – był dziekan Wydziału Zarządzania i Komunikacji Społecznej KAAFM dr hab. Dariusz Fatuła, prof. KAAFM. Uczestnikami panelu byli przedstawiciele różnych ośrodków akademickich oraz eksperci-praktycy. W referacie *Konwergencja w zarządzaniu procesami w skali makro* dr Katarzyna Kucab-Bąk (KAAFM) dokonała oceny procesów konwergencyjnych z uwzględnieniem problemów realizacji założonych celów różnych instytucji wobec skutków pandemii COVID-19 oraz ogólnoświatowych reperkusji gospodarczych wojny Rosji z Ukrainą. Celem wystąpienia dr Katarzyny Czajkowskiej (KAAFM) była analiza *Wpływu nowych technologii w marketingu na funkcjonowanie przedsiębiorstw w warunkach niepewności* jako przyczynek do dyskusji, jak rozwiązania marketingowe, opierające się na nowych technologiach, mogą wpływać na zmniejszenie ryzyka prowadzenia działalności gospodarczej i zwiększenie przewidywalności otoczenia biznesowego. Następne wystąpienie dotyczyło *Odbioru treści biznesowych przedstawionych w formie infografik przygotowanych w systemie SAP Analitycs Cloud* i zostało wygłoszone przez dra Mariana Krupę (Małopolska Uczelnia Państwowa im. rtm. W. Pileckiego w Oświęcimiu) oraz dra Macieja Pękalę (KAAFM). Zagadnienie *Współczesne radio internetowe i jego patroni. Działanie organizacji medialnej w warunkach niepewnego finansowania* rozpatrywano pod kątem zależności rozgłośni nadających w Internecie od finansujących ich działalność „patronów", a referat został wygłoszony przez dra Dariusza Barana (KAAFM).

W ramach sekcji trzeciej „Zarządzanie w turystyce", prowadzonej przez dr hab. Izabelę Kaperę, prof. KAAFM, miało miejsce pięć wystąpień. Pierwsze dotyczyło zagadnień związanych z *Zarządzaniem systemem ochrony zdrowia w Polsce. Aspekty interdyscyplinarne*, ze szczególnym uwzględnieniem związków z turystyką/obsługą ruchu turystycznego – zaprezentowała je Izabela Kapera. Drugi referat pt. *Wybrane instytucje kultury w obliczu współczesnych zagrożeń* wygłosił dr Marcin Cziomer (KAAFM). Prelegent zwrócił uwagę zarówno na kwestie odnoszące się do pandemii COVID-19 i jej wpływu na instytucje kultury, jak i na inne zagrożenia mogące oddziaływać na walory kulturowe mające istotne znaczenie w turystyce. *Zarządzanie turystyką w Polsce z perspektywy przedsiębiorcy turystyki przyjazdowej* przedstawiła prezes Symposium Cracoviense, mgr Anna Jędrocha. Wystąpienie, zwierające spostrzeżenia ekspertki reprezentującej sektor turystyczny, było jednym z kilku w ramach

wydarzenia, które pozwoliło na integrację środowisk naukowców i praktyków. W ten cel konferencji wpisały się także dwie następne prelekcje. Pierwszą, dotyczącą *Determinantów funkcjonowania systemu zarządzania kryzysowego w branży hotelarskiej*, przygotowała mgr inż. Barbara Podwysocka (Wojskowa Akademia Techniczna, dyrektor Pionu Jakości i Bezpieczeństwa w Polskim Holdingu Hotelowym Sp. z o.o.). Z kolei o cyberbezpieczeństwie i jego roli w turystyce (*Cybersecurity in travel based on the opinions of university students engaging in tourism*) mówił Artur Kapera (Security Engineer, z firmy Apius Technologies S.A.).

Dzień drugi konferencji składał się z trzech sesji praktycznych, które stanowiły kontynuacje zagadnień poruszanych w panelach teoretycznych. Pierwszy panel nosił tytuł „Problemy zarządzania wobec współczesnych zagrożeń, zarządzanie bezpieczeństwem energetyczno-ekologicznym", a prowadzącym był prof. Andrzej Chodyński. Pierwsze wystąpienie Wojciecha Huszlaka miało na celu wskazanie *Praktycznych aspektów audytów społeczno-ekologicznych*, przedstawienie obszaru tematycznego oraz stanu prowadzonych badań. W wystąpieniu Anny Bałamut wskazano ważność klastrów energetyczno-ekologicznych dla zapewnienia bezpieczeństwa energetycznego Polski, obecny stan badań i perspektywę kolejnych. Wystąpienie dra hab. inż. Adama Jabłońskiego, dra hab. inż. Marka Jabłońskiego oraz Sławomira Kamińskiego dotyczyło *Doświadczeń miasta Bytom związanych z budową samowystarczalności energetycznej z wykorzystaniem Klastra Innowacji Energetycznych*. Autorzy wskazywali na konieczność transformacji obecnych modeli w kierunku odporności na zmiany klimatu. Następnie mgr Andrzej Kasiński (Polski Instytut Kontroli Wewnętrznej) mówił o *CMMI 2.0 jako nowym spojrzeniu na dojrzałość organizacji*, a mgr Paweł Cybulski (Polski Instytut Kontroli Wewnętrznej) o *Gospodarce dla dobra wspólnego – próbie rozwiązań globalnych problemów współczesnego świata*. Ważnymi stwierdzeniami, które padły podczas wystąpienia były: „nie żyjemy ponad stan, ale poza możliwościami innych" oraz „więcej dobrobytu społecznego zamiast większego produktu krajowego brutto". Skłaniają one do refleksji nad wyborami które podejmowane są przez państwa, przedsiębiorstwa i społeczeństwo. Rozwiązaniem może być zatem model ekonomiczny dobra wspólnego ECG.

Panel ukazał ścisły związek pomiędzy obszarami tematycznymi badań pracowników Wydziału Zarządzania i Komunikacji Społecznej KAAFM i problemami poruszanymi przez zaproszonych gości. Dodatkowo podkreślił znaczenie badań i analiz naukowych w rozwiązaniach, które stosowane są na rynku, np. Klaster – Miasto Bytom. Kooperacja na linii przedsiębiorstwo–uczelnie jest zatem kluczowym elementem do wypracowania właściwych rozwiązań, które sprawdzą się w warunkach rynkowych.

W ramach panelu drugiego wystąpiło czterech prelegentów. Ich prezentacje zapowiedziała dr hab. Izabela Kapera, odnosząc się jednocześnie do roli jednostek samorządu terytorialnego w rozwoju turystyki. Prowadząca przedstawiła wyniki wcześniej realizowanych badań, omówionych w książce *Rola samorządu terytorialnego*

w gospodarowaniu i zarządzaniu przestrzenią turystyczną wydanej przez Oficynę Wydawniczą AFM w Krakowie. Przywołana tematyka nawiązywała bezpośrednio do wystąpienia wójta gminy Tymbark dra Pawła Ptaszka, który omówił zagadnienie *Strategia rozwoju gminy a budowa marki miejsca*. Kontynuacją tematu jednostek samorządu terytorialnego był też referat dra Pawła Dziekańskiego i dra hab. Grzegorza Drozdowskiego, prof. UJK (przedstawicieli Uniwersytetu Jana Kochanowskiego w Kielcach): *Jakie przestrzenne zróżnicowanie zrównoważonej turystyki w warunkach przemian zielonej infrastruktury? Case study powiatów w Polsce w latach 2010–2020.* Kolejny poruszany wątek dotyczył *Partycypacji w kulturze w obliczu współczesnych wyzwań i zagrożeń*. *Perspektywa twórcy i odbiorcy* i został zaprezentowany przez Marcina Cziomera. Ostatnia w ramach tej części prelekcja, którą zaproponowała Barbara Podwysocka, dotyczyła zagadnienia *Wielowymiarowości systemu bezpieczeństwa w hotelarstwie.*

Obecność na spotkaniu przedstawicieli różnych podmiotów związanych z sektorem turystycznym pozwoliła w ramach dyskusji wieńczącej panel na przedstawienie wybranych problemów towarzyszących zarządzaniu turystyką. Przykładem tego rodzaju sytuacji mogą być odmienne stanowiska pomiędzy gminami a położonymi na ich terenie obszarami chronionymi. Zwracał na to uwagę Paweł Ptaszek w odniesieniu do obszarów Natura 2000. Stanowisko z perspektywy ochrony przyrody prezentowała Monika Olszewska (Gorczański Park Narodowy).

Trzeci i ostatni panel drugiego dnia konferencji nosił tytuł „Wpływ nowych trendów w marketingu na rzecz *sustainability* i zwiększenia/budowania sprężystości (*resilience*) firm w obliczu kryzysów ekonomicznych i pozaekonomicznych, rola nowych technologii", a prowadzącymi byli: dziekan Wydziału Zarządzania i Komunikacji Społecznej KAAFM, dr hab. Dariusz Fatuła, dr Krzysztof Waśniewski (KAAFM) oraz mgr Bartolomeo Rafael Bialas (KAAFM, specjalista kreowania i zarządzania marką w USA). Wygłoszono następujące referaty: *Las Vegas Brand Strategy Consultancy – Impact of new trends in marketing for sustainability and increasing/building resilience of companies in the face of economic and non-economic crises, role of new technologies* (Bartolomeo Rafael Bialas), *Impact of new trends in marketing for sustainability and increasing/building resilience of companies in the face of economic and non-economic crises, role of new technologies* (Hania Krück, Innova IP – A.D. Sosa & Soto), *Customer Experience in multichannel marketing* (dr Marcin Szplit, Uniwersytet Jana Kochanowskiego w Kielcach) oraz *Korzyści i wyzwania związane z digitalizacją przedsiębiorstw* (dr Katarzyna Czajkowska). Panel zakończył się dyskusją, w której wzięli udział praktycy ze Stanów Zjednoczonych Ameryki Północnej oraz Gwatemali.

Ważnymi zagadnieniami w dyskusji były współczesne problemy marketingu wobec nowych technologii, zagrożenia dla funkcjonowania różnego typu organizacji i rosnąca rola zarządzania bezpieczeństwem dla zapobiegania tym zagrożeniom. Zwrócono uwagę na takie aspekty jak e-commerce, inteligentne miasta, *data leaks*,

robotyzacja pracy. Ciekawym wątkiem w dyskusji był temat sztucznej inteligencji, który wkracza w wiele obszarów zarządzania, w tym w optymalizację procesów produkcyjnych. Ma również zdolność do przetwarzania i analizy dużych ilości danych, przez co jest w stanie identyfikować niewydajne obszary i sugerować właściwe usprawnienia. Zagadnienie to zainicjowało pytanie, czy sztuczna inteligencja jest szansą, czy zagrożeniem dla przedsiębiorców, pracowników i klientów, wskazując tym samym na nowe obszary badawcze w zakresie nauk o zarządzaniu i jakości.

Zasygnalizowane w wystąpieniach zagadnienia, niezwykle ciekawe, ważne i aktualne, zostaną rozwinięte w planowanej publikacji pokonferencyjnej.

BEZPIECZEŃSTWO TEORIA I PRAKTYKA
SECURITY THEORY AND PRACTICE
e-ISSN 2451-0718
ISSN 1899-6264
2023
Nr 4 (LIII)
DOI: 10.48269/2451-0718-btip-2023-4-013

Mirosław Kwieciński

dr hab., prof. PANS, Państwowa Akademia Nauk Stosowanych w Krośnie
https://orcid.org/0000-0001-6719-5501

VI Multidyscyplinarne Autorskie Seminarium Naukowe *Modus Securitas* „Determinanty skuteczności zarządzania bezpieczeństwem państwa i biznesu – koncepcje, modele, podejścia, praktyka, wizje, wyniki badań", Dwór Rychwałd w Rychwałdzie, 17–19 września 2023 r.

Litera ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. z 2022 r., poz. 655) nakłada na wszystkie organy władzy i administracji rządowej oraz na inne organy i instytucje państwowe, organy samorządu terytorialnego, przedsiębiorców, organizacje pozarządowe i inne podmioty, a także na każdego obywatela realizację wielu nowych zadań z zakresu obronności państwa. Liczne nowe obowiązki spoczywające na wyżej wymienionych podmiotach wynikają z niezwykle aktualnej potrzeby zapewnienia odpowiedniego poziomu obronności państwa. Realizacja procesów przygotowań obronnych w aktualnej sytuacji międzynarodowej powinna być również, jak wydaje się, przedmiotem pilnej uwagi i dociekań przedstawicieli środowiska nauki i praktyki z obszaru nauk o bezpieczeństwie oraz nauk o zarządzaniu i jakości. Niniejsze sprawozdanie stanowi opis jednej z inicjatyw o charakterze naukowym, polegającej na podjęciu dyskusji wokół aktualnego stanu wiedzy i rozwijania potrzeby przygotowań obronnych Polski.

W dniach 17–19 września 2023 r. w Dworze Rychwałd w Rychwałdzie w Beskidzie Żywieckim odbyło się VI Multidyscyplinarne Autorskie Seminarium Naukowe *Modus Securitas* pt. „Determinanty skuteczności zarządzania bezpieczeństwem państwa i biznesu – koncepcje, modele, podejścia, praktyka, wizje, wyniki badań". Pomysłodawcą oraz organizatorem obrad był, podobnie jak w poprzednich latach, dr hab. Mirosław Kwieciński, prof. Państwowej Akademii Nauk Stosowanych w Krośnie, kierownik Zakładu Bezpieczeństwa Wewnętrznego, profesor w Zakładzie Zarządzania. Seminarium zostało zorganizowane przy współudziale Fundacji Instytut Wywiadu Gospodarczego w Krakowie.

Obrady uczestników VI edycji skupione były wokół problematyki zarządzania procesami przygotowań obronnych w państwie i biznesie, głównie wokół następujących wiodących zagadnień:

1. Problemy przygotowań obronnych w obszarze zarządzania kryzysowego w samorządzie terytorialnym – prawidłowości i zasady oparte na wartościach.
2. Skokowy postęp w zastosowaniach sztucznej inteligencji oraz technologii kosmicznej jako współczesna i przyszłościowa podwalina bezpieczeństwa.
3. Determinanty i koncepcje aktywności przedsiębiorców w planowaniu obronnym jako podstawa poszukiwań źródeł skuteczności poczynań.
4. Pilna potrzeba narzędziowego wsparcia rozwijania koncepcji kultury obronności dla zachowania narodowego bytu Polaków jako dewiza i przekonanie.

Szeroko nakreślona problematyka seminarium, budząca wielkie zainteresowanie, przyciągnęła uwagę 25 uczestników. Środowisko akademickie reprezentowali przedstawiciele ośrodków z Warszawy, Łodzi, Krakowa, Wrocławia, Górnego Śląska, Częstochowy, Bielska-Białej, Wałbrzycha, Nowego Sącza i Krosna. Głównym celem obrad, podobnie jak podczas wcześniejszych edycji, było przedyskutowanie wybranych niezwykle aktualnych problemów odnoszących się do determinant skutecznego zarządzania bezpieczeństwem państwa oraz biznesu.

Uwaga uczestników wykładu inauguracyjnego skupiła się na istotnym problemie teorii i praktyki zarządzania bezpieczeństwem w świetle aktualnej sytuacji geopolitycznej Polski. VI edycję seminarium otworzył prof. dr hab. Stanisław Sagan, który przedstawił wykład pt. *Zagrożenia dla Polski w doktrynie Aleksandra Dugina*. Stanowił on niezwykle interesujący przekaz aktualnej wiedzy dotyczącej perspektyw rosyjskiej agresji w świetle koncepcji jednego z wiodących kremlowskich strategów. Wystąpienie inauguracyjne wywołało duże poruszenie i zainteresowanie omawianymi zagadnieniami.

Kolejną część seminarium stanowiła dyskusja w ramach I sesji pod hasłem: „Aktualne wyzwania dla procesów zarządzania przygotowaniami obronnymi w państwie i biznesie". Obradom przewodniczyli prof. dr hab. Andrzej Chodyński z Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego oraz dr inż. Iwona Gawron z Akademii Nauk Stosowanych w Nowym Sączu.

W panelu wygłoszono następujące referaty:

- *Ontologia niebezpieczeństwa jako paradygmat projektowania strategii bezpieczeństwa* – prof. dr hab. Kazimierz Perechuda, dr Krzysztof Hauke (Uniwersytet Ekonomiczny we Wrocławiu);
- *Zarządzanie cyberbezpieczeństwem infrastruktury krytycznej dla bezpieczeństwa Państwa na przykładzie rozwiązań sektora transportu kolejowego* – dr hab. inż. Adam Jabłoński, prof. Uniwersytetu WSB MERITO (Uniwersytet WSB MERITO w Poznaniu, Wydział Zamiejscowy w Chorzowie);
- *Zastosowanie AI w wykrywaniu przestępczości oraz sytuacji kryzysowych* – dr hab. Iwona Chomiak-Orsa, prof. UEW, mgr Kamil Hudaszek (Uniwersytet Ekonomiczny we Wrocławiu);
- *Zarządzanie przygotowaniami obronnymi w obszarze wybranych obiektów infrastruktury krytycznej (na przykładzie Miasta Stołecznego Warszawy)* – podinsp. mgr Zdzisław Mazurski (Fundacja Instytut Wywiadu Gospodarczego w Krakowie).

Zagadnienie różnorodności problematyki przygotowań obronnych dla procesów bezpieczeństwa, zasadniczo dotyczących państwa i ludności, kontynuowane było podczas II sesji pt. „Próba społecznej oraz systemowej diagnozy znaczenia kultury obronności oraz polityki obronnej na tle wyzwań wzmacniania odporności państwa" pod przewodnictwem prof. dra hab. Kazimierza Perechudy oraz dr Dominiki Karwoth-Zielińskiej (Uniwersytet Ekonomiczny W Krakowie). Uwagę uczestników przyciągnęły referaty:

- *Aspekt edukacji w kulturze obronności narodowej* – dr Nina Orzech (Akademia Wojsk Lądowych imienia generała Tadeusza Kościuszki we Wrocławiu);
- *Koszty przygotowań obronnych przedsiębiorcy – nowa okazja do optymalizacji podatkowej?* – dr Waldemar Szewc (A.F.O. Kancelaria Doradztwa Podatkowego we Wrocławiu);
- *Znaczenie gospodarki narodowej w polityce obronnej państwa* – dr Tomasz Orzech (Akademia Nauk Stosowanych Angelusa Silesiusa w Wałbrzychu).

Wystąpienia zakończyła ożywiona dyskusja na temat różnorodnych aspektów realizacji koncepcji zarządzania przygotowaniami obronnymi we współczesnych organizacjach.

Kolejną III sesję obrad pt. „Kondycja etyczno-warsztatowa służb i struktur odpowiedzialnych za umacnianie odporności i obronności w państwie i biznesie", przeprowadzono pod przewodnictwem dr hab. Zofii Wilk-Woś, prof. Uniwersytetu WSB MERITO (Uniwersytet WSB MERITO w Toruniu, Wydział Zamiejscowy w Łodzi) oraz dra Waldemara Szewca. Wygłoszono następujące referaty:

- *Spór o granice skuteczności realizacji zadań obronnych w ogniwach Krajowego Systemu Ratowniczo-Gaśniczego – priorytety czy wszystkoistość* – dr Andrzej Marjański (Uniwersytet WSB MERITO w Toruniu, Wydział Zamiejscowy w Łodzi);

– *Własne problemy etyczno-zawodowe Policji w służbie prawa i bezpieczeństwa obywateli* – dr Ryszard Bełdzikowski (Wyższa Szkoła Administracji w Bielsku-Białej);
– *Konflikt interesów jako stymulator przełomu w negocjacjach nad kontraktami obejmującymi przedsięwzięcia w ramach realizacji zadań obronnych spółek Skarbu Państwa* – mgr Krzysztof Grząba (Uniwersytet Ekonomiczny w Krakowie, doktorant);
– *Zarządzanie projektami wzmacniania zdolności zachowania bezpieczeństwa informacyjnego organizacji* – dr hab. inż. Paweł Kobis (Politechnika Częstochowska).

Podobnie jak w poprzednich sesjach referaty wywołały ożywioną dyskusję, wzbogacając w ten sposób dorobek obrad seminarium.

Wieńczącym obrady był panel dyskusyjny pt. „Aplikacyjność realizacji koncepcji zarządzania przygotowaniami obronnymi w sektorze publicznym i biznesie – możliwości i zagrożenia", którego obradom przewodniczyli: dr hab. Mirosław Kwieciński oraz dr Katarzyna Łyp-Wrońska (Akademia Górniczo-Hutnicza w Krakowie).

Burzliwa i merytoryczna dyskusja w gronie przedstawicieli środowiska naukowego i biznesu wokół określenia pryncypiów realizacji koncepcji zarządzania przygotowaniami obronnymi w państwie i biznesie przyniosła następujące wnioski:
– potrzeba badań i ocen możliwości obronnych Polski, także na tle zauważalnych słabości w gospodarce,
– niedocenianie potencjału tkwiącego w sektorze MSP, który jednak będzie wymagać dodatkowych inwestycji w zakresie wzmacniania militarnych zdolności obronnych w postaci technologii, maszyn, ludzi-specjalistów,
– zauważalna niekonsekwencja w realizacji polskich kontaktów politycznych z krajami Europy Zachodniej,
– upadek poziomu moralno-etycznego służb policji,
– niedocenianie kadry przedsiębiorstw sektora MSP,
– brak zaangażowania w wykorzystanie lokalnych sieci wytwórców jako znaczącego potencjału obronnego,
– brak zaangażowania w procesy wykorzystania obywateli Ukrainy dla wzmacniania polskiego potencjału obronnego.

Skomplikowana i obszerna problematyka obrad znalazła swoje różnorodne odzwierciedlenie w prezentowanych wystąpieniach. Wiele z założonych w programie seminarium zagadnień nie zostało jeszcze wystarczająco rozwiniętych w wystąpieniach uczestników obrad i w samej dyskusji, co stanowi potwierdzenie małej skali zaangażowania środowiska naukowego i praktyki wobec potrzeby zrozumienia aktualnego znaczenia procesów przygotowań obronnych Polski. Nadal brakuje odniesień do ogromnej roli zaangażowania przedsiębiorców, szczególnie w obszarze uporządkowania prawodawstwa w tym zakresie, realizacji obowiązujących standardów państw – uczestników paktu NATO odnośnie do przygotowań obronnych, szczególnie do wymogów zabezpieczenia bytu ludności na wypadek wydarzeń wojennych oraz pilnej

potrzeby zbudowania systemu obrony cywilnej. Powyższe rzuca także światło na poziom rozwoju kultury obronności jako systemu wzorców zachowań, preferencji, pryncypiów, wartości, uświadomienia potrzeb przygotowań obronnych.

VI edycja seminarium znalazła uznanie wśród uczestników i potwierdziła w pełni potrzebę organizacji kolejnych spotkań naukowych i szerokiej dyskusji. Zebrani podkreślali wysoki poziom zarówno naukowy, jak i ekspercki, a także konieczność kontynuacji obrad za rok w nieco przebudowanej formule obrad. W tym celu z grona uczestników powołano komitet organizacyjny kolejnego spotkania naukowego.

BEZPIECZEŃSTWO SECURITY
TEORIA I PRAKTYKA THEORY AND PRACTICE
e-ISSN 2451-0718 2023
ISSN 1899-6264 Nr 4 (LIII)

Lista recenzentów za rok 2023

W 2023 roku artykuły zgłoszone do „Bezpieczeństwa. Teorii i Praktyki" opiniowali pod kątem ich naukowej przydatności do rozpowszechniania:

dr hab. Grzegorz Bonusiak, prof. UR
dr hab. inż. Zbigniew Ciekanowski
prof. dr hab. Henryk Ćwięk
dr hab. Katarzyna Dośpiał-Borysiak
dr hab. Dariusz Fatuła, prof. KAAFM
dr hab. Małgorzata Kamola-Cieślik, prof. US
dr hab. Kazimierz Kraj, prof. AJP
prof. dr hab. Hubert Królikowski
dr hab. Aleksandra Kruk, prof. UZ
prof. dr hab. Krzysztof Kubiak
dr Piotr Kubiak
dr hab. Justyna Miecznikowska-Jerzak
dr hab. Agnieszka Piotrowska-Piątek, prof. PŚk
dr hab. Andrzej Szplit, prof. UJK
dr hab. Helena Wyligała, prof. Uniwersytetu Dolnośląskiego DSW
dr hab. Krzysztof Żarna, prof. UR