STAROPOLSKA AKADEMIA NAUK STOSOWANYCH W KIELCACH

STUDIA NAD BEZPIECZEŃSTWEM. SECURITY STUDIES

czasopismo naukowe
wydawane przez Instytut Nauk o Bezpieczeństwie
Staropolskiej Akademii Nauk Stosowanych w Kielcach

Czasopismo naukowe

Studia nad bezpieczeństwem.
Security Studies

wydawane przez Instytut Nauk o Bezpieczeństwie
Staropolskiej Akademii Nauk Stosowanych w Kielcach

Kielce 2023

ISSN 2956-7424

Oficyna Wydawnicza Staropolskiej Akademii Nauk Stosowanych w Kielcach
25-666 Kielce, ul. Ponurego Piwnika 49
www.stans.edu.pl

Skład i opracowanie graficzne
Krzysztof Kaputa

Druk i oprawa
Drukarnia Cyfrowa COMPUS,
Kielce, ul. Sandomierska 89

SPIS TREŚCI

AUTORZY ARTYKUŁÓW

Boyko Taras, Prof., *Lviv Polytechnic National University, Lviv, Ukraine.*

Czubocha Krzysztof, Dr, *adiunkt, Państwowa Wyższa Szkoła Techniczno-Ekonomiczna w Jarosławiu.*

Filip Zbigniew, Mgr, *wykładowca, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach; urzędnik Wydziału Zarządzenia Kryzysowego Urzędu Miasta Nowego Sącza.*

Harabin Radosław, Dr hab., *prof. ucz., Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach, ORCID ID: 0000-002-5180-5840.*

Konopka Tomasz, Dr, *dziekan, adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.*

Kuz Olha, Dr, *Lviv Polytechnic National University, Lviv, Ukraine.*

Paslavskyi Mykhailo, Dr, *Ukrainian National Forestry University, Lviv, Ukraine.*

Piotrowski Paweł, Mgr, *wykładowca, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.*

Ruda Mariia, Dr, *Lviv Polytechnic National University, Lviv, Ukraine.*

Służalska Beata, Dr, *adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.*

Służalski Jarosław, Dr, *adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.*

Stachowicz Mariusz, Mgr, *starszy sierżant, Komenda Powiatowa Policji w Wieliczce.*

Stasevych Serhiy, Assoc. Prof., *Lviv Polytechnic National University, Lviv, Ukraine.*

Węgliński Bogusław, Dr, *adiunkt, Dolnośląska Szkoła Wyższa we Wrocławiu, ORCID ID: 0000-0002-6587-8231.*

Wilk-Jakubowski Grzegorz, Dr hab., *prof. ucz., Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach, ORCID ID: 0000-0002-3906-4103*

Zając Grzegorz Krzysztof, Dr, *adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach, ORCID ID: 0000-0002-5504-5228*

WSTĘP

Zagadnienia bezpieczeństwa we współczesnym świecie stanowi częsty temat rozważań wielu naukowców, a także przedmiot analiz i dociekań badawczych prowadzonych przez naukowe instytucje. Dziedzina bezpieczeństwa jest fundamentem również w formułowaniu polityki wewnętrznej i zagranicznej państwa. Instytucje międzynarodowe podejmują kwestie regulacyjne i operacyjne w zapewnieniu odpowiedniego poziomu bezpieczeństwa gospodarczego, militarnego, politycznego, kulturalnego, zdrowotnego, informatycznego. Dzięki pojawiającym się nowym opracowaniom oraz upowszechnianiu różnych aspektów bezpieczeństwa wzrasta ogólna świadomość społeczeństwa w zakresie identyfikacji, reagowania, zapobiegania zagrożeniom. Bezpieczeństwo nie jest kategorią stałą, ani wąską, lecz stanowi pewien ciąg podejmowanych instrumentów i regulacji w odniesieniu do aktualnych wyzwań i uwarunkowań. Zmienność i dynamika stosunków międzynarodowych wymaga stałego koncentrowania uwagi na różnych obszarach życia narodów i państw pod kątem zapewnienia bezpieczeństwa.

W odpowiedzi na coraz to nowe rodzaje zagrożeń, w tym zagrożenia hybrydowe, konieczne jest podjęcie analizy wielopłaszczyznowej bezpieczeństwa. Niniejszy zbiór „Studia nad bezpieczeństwem. Security Studies" ma za zadanie spełniać tę rolę upowszechniając zagadnienia bezpieczeństwa szerokiemu gronu odbiorców. Pierwsze wydanie nowego czasopisma naukowego w Instytucie Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach wpisuje się w ramy krzewienia nauki w dziedzinie bezpieczeństwa wewnętrznego i międzynarodowego, jak również przyczynia się do podniesienia poziomu odpowiedzialności za podejmowane działania na wielu płaszczyznach bezpieczeństwa.

Celem publikacji jest zaangażowanie środowiska naukowego i pozanaukowego w rozwój badań nad bezpieczeństwem. Oddany do druku zbiór jest najlepszym przykładem synergii teoretycznych i praktycznych rozważań przez naukowców na co dzień podejmujących trud badawczo-rozwojowy oraz praktyków działających w rozmaitych instytucjach zajmujących się bezpieczeństwem w praktycznym wymiarze. W niniejszej publikacji poruszana będzie tematyka szeroko rozumianego bezpieczeństwa w różnych obszarach ważnych społecznie oraz dla państwa.

Artykuły zamieszczone w niniejszym zbiorze koncentrują się wokół następujących kategorii: bezpieczeństwa geopolitycznego, bezpieczeństwa zdrowotnego, bezpieczeństwa cybernetycznego, bezpieczeństwa lotniczego, a także bezpieczeństwa i porządku publicznego.

Poruszony zostaje aktualny problem agresji Federacji Rosyjskiej na Ukrainę. Dokonano analizy tego zjawiska pod kątem geopolitycznych uwarunkowań. Nie sposób nie odnieść do zjawiska zagrożenia zdrowotnego spowodowanego pandemią koronawirusa i rozprzestrzenianiem się choroby COVID-19. W związku z występowaniem od 2020 r. tej pandemii podjęto też analizę wpływu na ruch lotniczy, w szczególności na lotnisko we Wrocławiu. Ukazano też kwestie bezpieczeństwa lotniczego w szerokim aspekcie międzynarodowych regulacji prawnych. Innym zagadnieniem są również kwestie cyberbezpieczeństwa, które znalazły odzwierciedlenie w kilku artykułach. Omówiona została również problematyka zarządzania sprywatyzowaną częścią zadań dotyczących zapewnienia bezpieczeństwa i porządku publicznego.

W czasopiśmie prezentowane są aktualne zagadnienia bezpieczeństwa przez osoby z kraju jak i zagranicy. W bieżącym numerze znajdują się pozycje polskojęzyczne jak i angielskojęzyczne, dzięki czemu publikacja ta może być wykorzystana w wielu państwach świata. Od samego początku głównym zamierzeniem wydania tej publikacji był jej międzynarodowy charakter celem popularyzacji osiągnięć naukowych i praktycznych w obszarze bezpieczeństwa w Polsce i innych państwach.

Publikacja skierowana jest do wszystkich zainteresowanych problematyką bezpieczeństwa osób i instytucji, w szczególności polecana jest studentom kierunku bezpieczeństwo wewnętrzne, bezpieczeństwo narodowe, stosunki międzynarodowe. Publikacja ta z całą pewnością posłuży naukowcom i badaczom do pogłębiania swoich analiz w zakresie bezpieczeństwa. Niewątpliwie, również służbom państwowym, w szczególności policji, siłom zbrojnym, zbiór ten będzie pomagał w bieżącym działaniu i podejmowaniu właściwych decyzji. Zbiór ten jest poddany recenzji naukowej i zaprezentowane opracowania naukowe odzwierciedlają stanowiska ich autorów.

Serdeczne podziękowania kieruję na ręce Pana Profesora Dr hab. Antoniego Olaka, który poświęcił swój czas na recenzowanie artykułów zgłoszonych do naszego czasopisma. Dziękuję Panu Profesorowi za sumienną i wnikliwą ocenę merytoryczną, za życzliwość i bezinteresowną współpracę ze społecznością akademicką Staropolskiej Akademii Nauk Stosowanych w Kielcach. Dzięki profesjonalnemu [podejściu i zaangażowaniu Pana Profesora w wykonanie recenzji możliwe jest utrzymanie wysokiego poziomu czasopisma naukowego.

Gorąco zachęcam do współpracy z Naszą Redakcją i współtworzenia bezpiecznej przyszłości Polski oraz społeczeństwa. Zachęcam do współpracy zarówno badaczy krajowych jak i zagranicznych.

Krzysztof Czubocha[1]

Russian aggression of Ukraine and its conflict with the Westin the light of Russian geopolitical conceptions

Abstract

One of the meanings of geopolitics is 'mental maps' of national elites which guide their national foreign policy priorities. Russian elites always thought of Russia as one of the main poles of influence in the world predestined to shape the course of international events or create a new architecture of security. This way of conceptualizing international relations by the Russian elites involved such terms as empire, spheres of influence and dependent territories. Moreover, Russia has always resisted the unipolar world created after the fall of communism. Therefore, Russian elites decided that the time has come to topple American dominance and create a new architecture of international security based on a multipolar world. Ukraine was regarded as belonging to the Russian sphere of influence and therefore, any attempts at shedding the dependence on Russia were to be quashed. Ukraine was to be at best neutralized and east-bank Ukraine was regarded as Russian and even called 'little Russia' or new Russia. Western decision to admit Ukraine into NATO was interpreted by the Kremlin as an intrusion in the sphere of Russian dominance and as a result, it prompted the aggression which should be regarded more brodely as an attempt at changing world balance of power.

Keywords: Russia, geopolitics, international security, Ukraine war, multipolar world.

[1] Dr Krzysztof Czubocha, adiunkt, Państwowa Wyższa Szkoła Techniczno-Ekonomiczna w Jarosławiu.

Introduction

The Russian aggression of Ukraine of 2022 was to be expected for those who give importance to geopolitics. There are several perspectives concerning the origins of conflict between Russia and the West. The existing literature often seeks to apprortion blame. Those researchers who support liberalism believe that respect for international law and state sovereignty is essential to maintaining *democratic peace* and security in international relations. It is also the stance of the EU which maintains that lasting peace should be based on upholding the rules of international law[2]. Indeed, from the point of view of public international law Russia is the aggressor who broke basic norms governing the international community. On the other hand, realism and geopolitics give importance to power politics and the special role of great powers whose interests overrule the right of smaller states. This paper deals mostly with the geopolitical dimention of the conflict as it remains relatively under-researched and the author comes to a conclusion that the war should be interpreted as part of the Russian strategy to reshape the world balance of power by creating a multipolar world and a new security architecture. Geopolitics is closely connected to realism in that it is based rather on projecting power than on upholding the rules of international law. The aim of the paper is to recreate the Russian rationale behind the international policies Russia pursues. In particular, to explain reasons for the aggression against Ukraine in a broader geopolitical context. Geopolitics is here understood as ideological constructs, imageries and mental maps guiding the Russian elites and justifying Russia's political and military policies toward Ukraine, broader East-Central Europe, European Union and even the West. On the other hand, from practical point of view, these ideological constructs are put into practice by promoting discourses and pursuing relevant policies on international stage. The above mentioned aspects of geopolitics were chosen as they are characteristic of Russian geopolitical thought and Russian perception of themselves and the outside world. The Russian stance may be regarded as unfounded in the West but it is worth analyzing to understand what drives Russian elites and possibly predict their next moves.

New branches of geopolitical thought

Geopolitics can be understood as a method of academic analysis of correlations between space and international relations or geopolitical representations created by national elites. The classical geopolitical thinking dealt with the influence of geographic location, i.e. climate, topography, distance from the sea, on the history, strategies and foreign policy of states. Applied geopolitics in turn refers to strategy based on the definition of situation which is the result of state's elites geopolitical representations which are partially

[2] A. Moravcsik, *Taking Preferences Seriously: A Liberal Theory of International Politics*, "International Organization" 1997, 51(4), pp. 513-53

subjective and deeply entrenched in national history and culture. Geopolitical constructs can serve short-term political goals, e.g. justifying the unification of certain peoples on the basis of historical, genetic and cultural proximity (e.g. Pan-Slavism, Pan-Turkicism, Pan-Arabism). So geopolitics consists of both discourses and ideological constructs, as well as political practice or startegy. Geopolitics is closely related to the realistic paradigm in international relations allowing to predict trends in the world[3].

Geopolitical representations are closely related to constructivism in sociology and international relations. The object of scientific research in the field of geopolitics is therefore to find out what are the foundations of national elites' mindset, worldview or mental maps. Research questions from geopolitical point of view might be as follows: what motivates national elites, how national history shaped the mindset of elites, what are their representations of the world and themselves or what are their security concerns. Analysis from the point of view of the spatial angle which characterized early geopolitics are also relevant but they constitute only one of the angles of analysis. Purely material and realist analysis of international relations fail to explain international relations phenomena in their entirety. The international reality is socially constructed and therefore one should take into account such explanatory variables as images, ideas, perceptions or norms[4].

In accordance with constructivism images are more salient than ideology in contemporary international relations. The term image may refer to self-image or the labels attributed to a state by the outside world (ascription of identity). Reciprocal images and perceptions affect the actors of international relations. These constructs exist at the following three levels: national elites, whole nations, national system and international system. After the collapse of the Soviet Union Russia was labelled by the West as imperialistic, expansionist, revanchist, security threat and a destabilizing actor. The answer of Russia was to construct a new self-image as a civilisation in itself. The Russian civilisation was to be superior and forming the basis for a transcendent empire with a universal mission which implied that Russia can follow its own rules instead of accepting foreign civilisational designs. The West was increasingly seen as the „other" and Russian self-image was even constructed in opposition to the West[5].

Vladimir Kolosov dealt with the problem of Russian cultural and geographical codes and the related ways of perceiving the world. The ideas about the world are the result of hundreds of years of history of the nation and the state and at the same time they constitute an element of the ideology and national identity. Thanks to this innovative approach to geopolitics, Kolosov and his associates tried to show the historical and cultural

[3] M.T. Owens, *In Defense of Classical Geopolitics*, „Orbis" 2015, 59(4), pp. 463-478.

[4] A. Wendt, *Anarchy is what States Make of It: the Social Construction of Power Politics*, "International Organization" 1992, 46(2), pp. 391-425.

[5] R. Taras, *The power of images and the images of power: past and present identity in Russia's international relations,* In: R. Taras (ed.) *Russia's Identity in International Relations Images, Perceptions, Misperceptions*, Routledge, London - New York 2012, pp. 1-10.

foundations which shaped the Russian geopolitical horizon, and thus present the dynamics of the creation of the discourse around the Russian place in the world after the collapse of the USSR.

Dmitrij Zamiatin understood the term geopolitics as targeted and clearly structured images of space in terms of geography, containing the most expressive and preserved (recorded) symbols, signs, images and characteristic features in collective memory, specific territories, countries or regions, marking them as politically relevant. Geopolitical images, as a form of describing and organizing space by means of geopolitics, which are of key importance for a given society, are transferred onto the real political map of the world, becoming the basis for the emergence of specific geopolitical concepts. The description and characteristics of the Russian space are contained not only in works of a geographic nature, but above all in works of writers, poets, philosophers and historians. It was their works that had a decisive influence on the shaping of the geographic and geopolitical images of Russia[6].New branches of geopolitics involve critical geopolitics which holds that geopolitics should attach significance to discourses shaped by a certain balance of power or arising in response to political or social demands. Knowledge created in this way acquires the status of "scientific" in order to support certain interests or the balance of socio-political forces. Therefore, geopolitical knowledge is interpretative and constructed. The task of the scientist is to explain the theory of world politics in terms of the factors that led to the current state of international affairs and their consequences for the foreign policy of states. "The main task of critical geopolitics is to show the manipulative nature of spatial images and their demythologization"[7].

Understanding of state security in realistic, constructivist and critical theory

From the point of view of the realistic paradigm state security is defined primarily in terms of military force that provides protection against external aggression in the context of the threat of using force that needs to be controlled. Another definition indicates that in terms of security, it is about protecting the physical, political and cultural identity of a state against the threats on the part of other states. Traditionally, important changes in international relations were usually the result of the use of force[8]. Mearsheimer proposed the theory of offensive realism on the basis of realism. It assumes that states will always fight for hegemony in the world and that American domination will be threatened by China in the future[9].

[6] J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej, między nauką, ideologicznym dyskursem a praktyką*, Wyd Uniwersytetu Gdańskiego, Gdańsk 2010, pp. 299-303.

[7] *Ibidem*, p. 307.

[8] A.M. Slaughter, *International Relations. Principal Theories*. https://www.princeton.edu/~slaughtr/Articles/722_IntlRel-PrincipalTheories_Slaughter_20110509zG.pdf [accessed 25.10.2022].

[9] J. Mearsheimer, *The Tragedy of Great Power Politics.* W.W. Norton & Company, London-New York 2001, pp. 401-402.

Over time, it has been noticed that economic interests, deposits of natural resources, and environmental safety may also be threatened, and the threats may result from the activities of terrorist groups or organized crime smuggling drugs. Moreover, there has been a departure from the military security of the state understood autarkically in favor of analyzes of collective security also in the context of securing against mutual destruction as a result of nuclear war (scientific realism). The EU can be interpreted from a realistic point of view as an organization that ensures a balance of power in Europe and thus contributes to the maintenance of security and peace[10].

According to constructivists, the problem of security is associated with the subjective perception of this issue by security objects (e.g. the state) and with the discourses created by securitizing entities (e.g. politicians or scientists). If a given discourse is promoted by scientists as dominant, the problem is securitized, i.e. it is included in the state security policy[11]. Scientific production resulting from such endeavors influences the decisions of state representatives in various fields, e.g. in the sphere of economic or security policy, or may lead to a complete redefinition of state policy in some fields. It is not the facts themselves that matter, but their interpretation based on social interactions or historical events. The strategic security policy of the state is also the result of a subjective view of the international reality. To a large degree it is ideas that lead to the definition of foreign policy goals, not international reality. This means at least partially challenging the realism[12].

From critical pint of view security can be interpreted as a field of competition of many entities that use their resources in order to convince the entities responsible for security to take into account their own concept, i.e. to securitize certain areas of human activity. For this purpose, you use your capital, e.g. economic or scientific capital. This may consist in referring to scientific works or opinions of think tanks (symbolic strength), i.e. using the prestige of science as a carrier of objective truth. Knowledge production can be funded by security companies through foundations to win government contracts and earn money. As a result, new branches of human activity may be securitized. There is, therefore, a constant struggle in the field of security to force through his own concept and earn money or make a career on it[13]. This does not mean that the element of an objective view of security issues is not present in scientific production. However, scientists are subjected to various pressures in order not to undermine the current understanding of security and not to infringe certain interests[14]. The notion of state security is closely

[10] B. McSweeney, *Security, Identity and Interests: A Sociology of International Relations*, Cambridge Univesity Press, Cambridge 1999, pp. 32-39.
[11] B. Buzan, O. Wæver, J. de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder – London 1998, pp. 21-48.
[12] T.V. Berling, *The International Political Sociology of Security: Rethinking Theory and Practice*, Routledge, London – New York 2015, pp. 22-29.
[13] *Ibidem*, pp. 47-72.
[14] O. Waever, *Towards a Political Sociology of Security Studies*, "Security Dialogue" 2010, 41(6), pp. 649-658. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.870.4136&rep=rep1&type=pdf [accessed 25.10.2022].

connected with great powers fighting for power as they assume that the more powerful they become the more secure they are.

Russian elites assumed that the architecture of security in Europe was based on recognizing that former Soviet states belong to the Russian sphere of influence and therefore NATO and the EU were not entitled to take steps aiming at offering to Ukraine a membership in their respective structures. The same reasoning was applied to The Eastern Partnership offered by the EU to some post-Soviet states. It was allegedly part of the strategy to encircle Russia nad even create an arc of instability at Russian borders (e.g. Georgia and Chechen wars). In such situation, Russia felt that the security arrangements have been broken and it is entitled to carry out a counter-offensive in Ukraine.

It is debatable whether national foreign policy goals are the result of the will of the population or the priorities of national elites. In case of Russia one can assume that the elites' goals prevail and therefore Russian foreign policy priorities should be regarded as the goals of the Russian elite.

Russian geopolitical thought

Russian geopolitical thought is multi-threaded and it is influenced by the current state of international relations[15]. Russian geopoliticians created several images of Russia.

1. The Russia-island image – a specific image because it represents geopolitical isolationism and an orientation towards autarkic internal development. The image of Russia as a separate island began to play a special role during Putin's first term in office, and its importance resulted from his disillusionment with Atlanticism and EU-centered Eurasianism;
2. Russia-Eurasia – another of the key images of Russia rooted in social awareness, its dominance in the sphere of politics was particularly visible when Yevgeny Primakov became the minister of foreign affairs;
3. Russia and Europe, i.e. Russia as Europe – picture which was dominant and at the same time crucial for shaping Russian identity and politics in the first period of the political transformation at the turn of the 1980s and 1990s;
4. Russia as Byzantium – the image of Russia-Byzantium is built on the basis of Byzantine civilization and its key significance for the identity of Russians;
5. Russia as Eastern Europe - regardless of the fact that the concept of Eastern Europe is ambiguous, this image strongly influenced the perception of Russia as a country belonging to this part of the world and sharing a common history with it[16].

The most salient image of Russia presented by Russian geopoliticians include portraying Russia as a unique and great civilization and a pole of global power entitled to

[15] A. Nowak, *History and Geopolitics: A Contest for Eastern Europe*, PISM, Warszawa 2008, pp. 13-36.
[16] J. Potulski, *op. cit.,* pp. 304-305.

co-manage international affairs. Cymburski was with this respect of great importance. According to him Russia is an island, a separate civilization possessing its own border zones or limitroph which constitute a buffer that should be under Russia's control or at least neutralized as Russia has no natural borders[17]. Basically, this image of Russia influenced Russian concepts after 1991. Karl Haushoffer, was another very popular geopolitical thinker in Russia. He planned an alliance between Germany and Russia which would allow both states to gain hegemony in Eurasia. The partnership with Germany was built since the chancellorship of Gerhard Schröder[18].

The image of Russia as a separate civilization is of great importance and it relates to ideology and messinism. Russians perceive themselves as a unique civilization which possesses it own cultural values and therefore Russia does not have to follow the exmaple of the West. Under Vladimir Putin the Turanian origins of Russia was stressed. Russian civilization has its borders in the form of dependent teritories or spheres of influence. Alexander Dugin goes even further in his analysis claiming that Russia fights on behalf of all mankind against American expansionism, the heart of which are corporations seeking to establish the new world order as the anti-Christ order[19]. While fighting the liberal West, Russia must create a new ideology called the fourth way faithful to tradition and theology[20]. For example, in 1997 Aleksandr Dugin referred to Russia as a catechon, which was to be the Third Rome, Holy Russia and a "geopolitical ark"[21]. With this respect Dugin writes that:

In October 2022, Russia entered a new era – the era of ideas. Everything we guessed, imagined and hoped for has now been called by name. Russia is a civilization whose basic code is Tradition. There is another civilization against it, the code of which is antitradition, human dehumanization, lies, aggression, exploitation of countries and nations, neocolonialism, terror and evil. In addition, the collective West makes a claim to the universalism of its model, leaving no choice to others. Only one can be selected. […] Russia swears allegiance to traditional values, a person, his right to being, faith, a normal family, freedom and justice, and renounces individualism, posthumanism, cancellation culture, LGBT, feminism, legalization of perversions and direct satanism of the West [22].

Until the Enlightenment, in the cultural sense, Europe included Christian countries and thus also Central and Eastern Europe. During the Enlightenment, reason, technology and modernity were considered to be the constituent elements of Europe. Due to the division of Europe into the industrializing west and the agricultural East, the orientalization

[17] V.L. Cymburski, *Rossia – zemlya za velikim Limitrofom: civilizaciya i yeyo geopolitika*, Editorial URSS, Moskva 2000, passim.

[18] L. Sykulski, *Rosja-wyspa i Wielki Limitrof". Myśl geopolityczna Wadima Cymburskiego, In. Problemy współczesnej Europy – ujęcie interdyscyplinarne*, R. Fedan, B. Petrecka, S. Dyrda-Maciałek, (Eds.), Wydawnictwo Państwowej Wyższej Szkoły Techniczno-Ekonomicznej w Jarosławiu, Jarosław 2014, p. 356.

[19] P. Eberhardt, *Koncepcje geopolityczne Aleksandra Dugina*, „Przegląd Geograficzny" 2010, 82(2), pp. 221-240 s. 227.

[20] *Globalizm i liberalizm to cywilizacja Antychrysta*, wywiad z Aleksandrem Duginem, „DoRzeczy" 2017/1, https://dorzeczy.pl/kraj/18103/Globalizm-i-liberalizm-to-cywilizacja-Antychrysta.html [accessed, 26.10.2022].

[21] A. Dugin, *Что понимать под Православием? (часть 3), arcto.ru, 1999.* [accessed 01.07.2020]

[22] A. Dugin, *https://t.me/russica2/48678, https://t.me/russica2/48679, https://t.me/russica2/48680.* [accessed 28.10.2022].

of Central and Eastern Europe took place during this period. In Western Europe, the orient was associated with negative qualities. As a consequence, there was a division of Europe and the cultural construction of the "other". This state of affairs turned out to be permanent. When communism was overthrown, the West decided that post-communist states should undergo a process of socialization and the concept of the Western civilizational mission in post-communist states was created. The West was supposedly progressive and civilized and the East (Orient) backward and irrational. For the first time, the above issues were subject to a broader analysis by E.W. Said. The author states that the heritage of Orientalism remains alive in Western Europe to this day[23].

In such circumstances, the Eurocentric attitude of the West towards Russia can be interpreted as a clash of civilizations. Russia does not subscribe to Western interpretation of international reality which boils down to accepting that „the West knows best" and therefore it is entitled to impose its values on the „less civilized" rest of the world. Therefore, the goal of Russia is to protect itself against Western cultural currents[24].

After the fall of the Soviet Union Russia was faced with finding a new identity both internally and in international relations. Discursive battles ensured between pro-western and anti-Western elites. Ascending to presidency by Vladimir Putin meant the application of discursive constructions involving defining the russian nation in opposition to the West. „According to anti-Westernists the West strives to impose its system of values on Russia to weaken it. The West uses double standards to further its interests".[25] The turanian elements of Russian culture were invoked to prove that Russia is a civilization in itself and therefore it does not have to emulate the West. On the international stage Russia was defined as a great power entitled to shape the world order together with other powers. Russians were in the course of time persuaded by this discursive construction. As a result, pro-Western elites were put in a difficult situation and their influence petered out[26].

The above mentioned assumptions imply a certain worldview of Russian elites. J. Diec writes that: Valery Korovin perceives American foreign policy as a crusade against Russia – the continental power, which should be wary of the doctrines and pressures from the global monetary system, which fits the interest of the US only. The campaign against "the Rest", which has not been subordinated to the Atlantic world, embraces the actions against Russia, with the Ukrainian affairs being the most representative example. Korovin perceives the events of the Orange Revolution and the Euromaidan as elements of an anti-Russian campaign. According to his Eurasianist beliefs, there is no such thing as a separate

[23] M. Boatca, *Multiple Europes and the Politics of Difference Within*, „Worlds & Knowledge Otherwise", Spring 2013, https://globalstudies.trinity.duke.edu/wpcontent/themes/cgsh/materials/WKO/v3d3_Boatca2.pdf, [accessed: 15.12.2021].

[24] J. Diec, *Major trends in Russian Geopolitics after 1991*, „Politeja" 2019, 62(5), 150. pp. 141-160. https://doi.org/10.12-797/Politeja.16.2019.62.08. [accessed 22.10.2022].

[25] O. Malinova, *Russia and the West in the 2000'. Redefining Russian identity in official political discourse*. In R. Taras (Ed.), *Russia's identity in international relations: images, perceptions, misperceptions*, Routledge, London-New York 2013, p. 77.

[26] N. Trubetskoi, *On the Turanian Element in Russian Culture*, "Anthropology & Archeology of Eurasia" 1998, 37(1), pp. 8-29.

Ukrainian nation. Ukraine is a part of the Russian Orthodox civilization and even the Western Ukrainian (Galician) Greek-Catholic nationalism should be comprehended as a product of Western manipulation (in analogy to dividing the Serbian people)[27].

Russia has by some authors to build a new Eurasian empire that spatially and strategically overcome the previous version, which was the Soviet Union. New empire therefore must be Eurasian, and big-continental world perspective. According to Russian geopoliticians, the new Russian empire should include Central and Eastern Europe as the periphery of Russian civilization (part of great limitrof as seen by Cymburski) [28]. The West (the Atlanticists) created a sanitary cordon against Russia in this region. Therefore, the countries of the region must be destabilized and even broken up in order to undermine the plans of the West and finally regain control of the region.

Russian strategy or applied geopolitics

Russia is interpreted by Alexander Dugin as predestined to play a leading role in the world because of its location and the combination of Eastern and Western features. It is to create a great continental empire, which is associated with geographical determinism and Mackinder's views on the conflict between sea and land powers over world domination. To achieve Russia's goals, it is necessary to topple the Anglo-Saxon dominance and create a new world order based on multipolarity. Russian anti-Americanism is officially labeled as anti-hegemonism in the global perspective[29]. Russian elites think they are predestined to become one of the main players participating in reshaping world balance of power and creating a new architecture of security which would involve carving up new spheres of influence. Additionally, Russia should have a veto power with respect to local and global security issues. These goals were not necessarily openly pronounced by Russian politicians but the policies the Russian Federation has been pursuing corroborate the existence of such a plan not only in Russian academic doscourse.

The relations between the EU and Russia were always strained as the EU's policy towards its neighbours was tinted with Eurocentrism. The palpable traits of this attitude consisted in basing relations with the European Neighborhood Policy on European values which were to be adopted by EU's partners. Closer relations with the EU were conditional on the recognition of the leading role the organization which aimed at shaping the neighbouring contries in accordance with EU design. This value-based approach to international relations was not acceptable to Russia which preferred the concept of relations between equal partners based on interests. The Russian government sees

[27] J. Diec, op.cit., p. 147.

[28] R. Wiśniewski, Przemiany terytorialne państwa rosyjskiego – aspekt historyczno-polityczny, In. P. Eberhard (Ed.), *Studia nad geopolityką XX wieku.* „Prace Geograficzne" nr 242, Warszawa 2013, p. 383.

[29] L. Sykulski, *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, In. P. Eberhardt (Ed..), *Studia nad geopolityką XX wieku*, „Prace Geograficzne" nr 242, Warszawa 2013, pp. 349-364.

Russia as an Eurasian power pole in a multipolar world and has no intentions of treating EU values as a point of reference as it would amount to normative subordination to the EU and accepting a peripheral status. As a result, the EU's designs of greater Europe encompassing Russia has failed even though, originally Russia was interested in them. The Russian tactic was therefore to develop bilateral relations with Germany[30]. Additionally, the EU was increasingly perceived by Russia as part of the Anglo-Saxon world and not as an independent force. With this respect M. Galser, P.E Thomann write:

The EU also worked more and more in synergy with NATO. NATO enlargement preceded EU enlargement. It reinforced the Russian perception that the EU and NATO were working together to push the Euro-Atlantic space to the East at the detriment of Russian security and economic interest. Continuous enlargement of NATO, various regime changes in the former Soviet Union countries, withdrawal of the United States of *Anti-Ballistic Missile Treaty* (AMB treaty), and the continued installation of the American and NATO military infrastructure anti-missile system reinforced the perception of the encirclement of Russia[31].

In the course of time, Russian elites developed a new and more nuanced perception of the West as not a monolitic block. Instead, internal differencces within the cracked West were seen and Russia attempted to exploit them to weaken the West. First of all, the Franco-German alliance was seen as a potential ally against the US. Hence, attempts were made at forging a special relationship between these two countries. The same tactic was applied to the EU by not negotiating international agreements with the organization. Rather, Russia counted on agreeing with Germany first which would pave the way for accepting the terms by the whole organization due to German clout.

Germany is too strong to dominate it, so it must be won over by giving it the countries of Central Europe, mainly the Visegrad countries and the Baltic states[32]. The consent to German reunification was conceived by USSR strategists as part of building a common European home (Gorbachev's concept). The reunification of Germany was to be a pretext to involve Germany in cooperation with Russia[33]. A new continental block was to be built, i.e. the Paris-Berlin-Moscow axis which found some support in Western Europe. In this context, Henry de Grossouvre stated in his 2002 book that the US hegemony will last several years and then the Paris-Berlin-Moscow axis would be established[34].

Russian elites involved Russia in wars to counter the percieved American dominance or intrusions into Russian spheres of influence. Russia believes that the West will attack in

[30] M. Glaser, P.E Thomann, *The concept of "Greater Eurasia": The Russian "turn to the East" and its consequences for the European Union from the geopolitical angle of analysis*, „Journal of Eurasian Studies" 2022, 13(1), pp. 3-15.
[31] *Ibidem*, p. 5.
[32] A. Dugin, *Osnovy geopolitiki. Geopoliticheskoye budushcheye Rossii*, Arktogeja, Moskva 1977, passim.
[33] J.M. Dorsey, Towards a New World Order in Eurasia? The Role of Russia and China, https://www.rsis.edu.sg/wp-content/uploads/2016/12/CO16310.pdf. [accessed 20.10.2022].
[34] H. de Grossouvre, Paris-Berlin-Moscou: la voie de l'indépendance et de la paix, L'Age d'Homme, Lousanne 2002, passim.

several years due to the fact that Russia is the largest reservoir of raw materials in the world and their deposits are depleted worldwide. Therefore, Russia is intensively modernizing its army. Russia sees itself as a defensive power which only protects itself aganinst American dominance. The US have supposedly created an arc of instability at Russian borders to weaken Russia. It has been proven by wars in Chechenya and Georgia.

Ukraine is essential for the Eurasian balance of power as a region of strategic importance or a 'pivotal state' as stressed by Brzezinski[35]. Therefore, for Russia, the loss of Ukraine and Crimea would mean a complete defeat and even a loss of political independence. The initiative to admit Ukraine into NATO was perceived as a clear security threat for Russia as it would allow the NATO forces to be deployed very close the the Russian heartland[36]. Russians believe that the aim of the West is to limit Russia's importance by way of exporting Western democracy also through color revolutions. On the other hand, the West supposedly created a zone of instability at Russian borders to weaken Russia. The Georgian war was to be one expample of the tactic of the West. The Eastern partnership of the EU was treated as an encroachment on the Russian sphere of influence in Ukraine[37].

The Euromaidan and Yanukovych's ouster destroyed Russia's plans. In spite of two peace accords Minsk I and Minsk II fighting continued. It became evident that Ukraine will not belong to Russia's zone of priviledged interests. The response of Moscow was to dismember Ukraine. As a result, Russia's response to the Maidan revolution of 2014 and Ukraine moving westward was the annexation of Crimea and supporting separatists in Eastern Ukraine. The second aggression against Ukraine of 2022 was the consequence of the pledge to include Ukraine into Western political and military structures. Russia took advantage of the cultural and national divisions inside Ukraine claiming to protect Russian speaking populations against the Kyievan government[38].

Russia articulated that it treated the inclusion of Ukraine into Werstern structures as an existential threat. Putin's goal was to force Biden and Zelenskiy to change course and to end their efforts to integrate Ukraine with the West. In December the Russians demanded a guarantee that the integration of Ukraine with NATO should stop and no offensive weapons will be stationed near Russia's borders. Speaking at the Russian Ministry of Defense on December 21, 2021, he stated that what the West is doing in Ukraine is happening on Russian's doorstep. Russia has nowhere to go back and therefore should counter the security threats materializing in Ukraine[39]

---

[35] Z. Brzezinski The Grand Chessboard: American Primacy and Its Geostrategic Imperatives, Basic Books, New York 1997, p. 74.

[36] J. Mearsheimer, *Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin*, „Foreign Affairs" 2014, 93(5), pp. 77-84.

[37] A. Lukin, *What the Kremlin Is Thinking, Putin's Vision for Eurasia*, "Foreign Affairs" 2014, 93(4), pp. 85-93.

[38] T. Kuzio, P. D'Anieri, op. cit., p. 16. *In Moscow's eyes, Ukraine is central to rebuilding a sphere of influence within the former Soviet space and to re-establishing Russia as a great power*. *Ibidem*, p. vi.

[39] J. Mearsheimer – Lecture at Robert Schuman Centre for Advanced Studies, Florence, June 6, 2022. https://www.youtube-.com/watch?v=qciVozNtCDM. [accessed 18.10.2022].

The war of 2022 resulted in restructuring the Russian way of thinking about the new world order which was to be shaped after stripping the US of its global dominance. Initially Russian elites intended to cooperate with Germany and create the Paris-Berlin-Moscow Axis omitting China as a potential threat to Russia. After the orange revolution and and the war of 2022 which resulted in economic sanctions agains Russia, further cooperation with European powers seems unlikely. The Russian Federation started moving eastwards forging relations with the Asian powers in the framework of the Shanghai Organization of Cooperation. China is seen as an allay which would allow to create an alternative economic zone weaning Russia from its economic dependence on the West.

The Greater Eurasia partnership or community that Russia is looking for is a shared space for economic, logistic, and information cooperation, peace, and security from Shanghai to Lisbon and from New Delhi to Murmansk[40]. "Greater Eurasia" was then elaborated not as a copy of the EU-centric order but in an opposite way. There is a fundamental difference between the integration projects proposed by the EU which are EU-centered and Russian understanding of the concert of powers. The new "Greater Eurasia" will consist of equal partners and there will be no center of integration[41].

Conclusions

Self-identity influences the definition of national interests and foreign policies. To regain international status a high self-esteem is needed. Russian political and scientific elites constructed a subjective version of Russian security and its role in the world. It consists of Russia as a separate and supreme civilization with a mission to protect the world against the Anglo-Saxon economic and political dominance which spreads a corrupting culture. The most recent state of Russian self-image is based on the narrative according to which Russia plays the role of catechon. The Kremlin elite believes that the world we know is going away. Historical analysis shows breakdowns of the international political and economic order take place periodically at intervals of around 90 years. At the end of such periods, the global architecture of security and the balance of power is reformulated. Old powers often lose their importance and new ones emerge. Earlier periods of such transformations were associated with the Napoleonic wars and the two world wars. Currently, we are approaching the end of the current cycle.

The Russian Federation initially aimed at creating an architecture of security in Europe based on the relations of equal partners. This approach failed as the West accepted its own values as the basis for mutual relations. It would mean that Russia would have to abandon its policy of carving up spheres of influence and preventing independent states

[40] S. Karaganov, *From east to west or greater Eurasia*, Russia in Global Affairs 2016. https://eng.globalaffairs.ru-/pubcol/From-East-to-West-or-Greater-Eurasia-18440. [accessed 15.10.2022].
[41] M. Glaser, P.E Thomann, *op. cit*., p. 11.

from integrating with the West. When this approach failed, Russian elites gradually engaged in undermining US domination and building a polycentric world cooperating with the Asian powers. Russia's security goals involved as a result breaking up the Euro-Atlantic alliance and ousting the US from Europe. On the other hand, an alliance with Germany was to supplant the relations with the whole EU and former Soviet states were to be recognized as Russia's sphere of influence. At the same time Russia intended to create another 'concert of great powers' acting together to create a new security architecture and divide spheres of influence. According to Russian elites international security can be achieved only by applying the balance of power principle. Russia increasingly sees itself as an Asian empire and therefore, Russian foreign policy increasingly focuses on cooperation with the Asian powers. In a new multipolar world Russia would be recognized as one of the great powers entitled to co-create a new international order. In the framework of this decisive battle between sea (Anglo-Saxon) and land powers (Asian states) one should expect the eruption of other conflicts in the Middle-East and the Far-East.

Moscow interprets the war in Ukraine as part the proces of the creation of a new world order. The open conflict with the West brought about Moscow's counteroffensive portrayed as protecting Russia's security against Western encroachment into Russia's borderland (limitrophe). Moreover, the war of 2022 has led to the final reorientation of Russias' foreign policy goals. International contingencies bring about changes in the Russian perception of itself as a European and Slavic state or an Eurasian and even Pacific rim power. Russia abandoned the conception of Eurasian space based on the cooperation with European powers. It was replaced with the project of integration with the Asian powers which relegates Europe to the status of an Asian peninsula, i.e. a marginal area. This area is, however, of startegic importance for Russia and therefore, its Eastern part should be divided between Russia and Germany. Russian geopolitical conceptions usually relate to the current balance of power. Before 2022 Russia was prone to leave Poland within the German sphere of influence. Whether this view persists depends on the mutual relations between Germany and Russia. The cooperation between the two states has been broken off due to the economic sanctions imposed on Russia and therefore, the project of jointly controlling East-Central Europe is for now dead.

References:

Berling, T.W., The International Political Sociology of Security: Rethinking Theory and Practice, Routledge, London – New York 2015.

Boatca, M., Multiple Europes and the Politics of Difference Within, „Worlds & Knowledge Otherwise", Spring 2013, https://globalstudies.trinity.duke.edu/wpcontent/themes/cgsh/materials/WKO/v3d3_Boatca2.pdf, [accessed 15.12.2021].

Brzeziński, Z., The Grand Chessboard: American Primacy and Its Geostrategic Imperatives, Basic Books, New York 1997.

Buzan, B, Wæver, O, Wilde, de J., Security: A New Framework for Analysis, Lynne Rienner Publishers, Boulder – London 1998.

Cymburski, V.L., Rossia – zemlya za velikim Limitrofom: civilizaciya i yeyo geopolitika, Editorial URSS, Moskva 2000.

Diec, J., Major trends in Russian Geopolitics after 1991, „Politeja" 2019, 62(5), 150. pp. 141-160. https://doi.org/10.12797/Politeja.16.2019.62.08 [accessed 22.10.2022].
Dorsey, J.M., Towards a New World Order in Eurasia? The Role of Russia and China, https://www.rsis.edu.sg/wp-content/uploads/2016/12/CO16310.pdf [accessed 20.10.2022].
Dugin, A., https://t.me/russica2/48678, https://t.me/russica2/48679, https://t.me/russica2/48680. [accessed 28.10.2022].
Dugin, A., Osnovy geopolitiki. Geopoliticheskoye budushcheye Rossii, Arktogeja, Moskva 1977.
Dugin, A., Что понимать под Православием? (часть 3), arcto.ru, 1999. [accessed 01.07.2020]
Eberhard, P., Studia nad geopolityką XX wieku
Eberhardt, P., Koncepcje geopolityczne Aleksandra Dugina, „Przegląd Geograficzny" 2010, 82(2).
Glaser, M, Thomann, P.E., The concept of "Greater Eurasia": The Russian "turn to the East" and its consequences for the European Union from the geopolitical angle of analysis, „Journal of Eurasian Studies" 2022, 13(1).
Globalizm i liberalizm to cywilizacja Antychrysta, wywiad z Aleksandrem Duginem, „DoRzeczy" 2017/1, https://dorzeczy.pl/kraj/18103/Globalizm-i-liberalizm-to-cywilizacja-Antychrysta.html [accessed 26.10.2022].
Grossouvre, de H., Paris-Berlin-Moscou: la voie de l'indépendance et de la paix, L'Age d'Homme, Lousanne 2002.
Karaganov, S., From east to west or greater Eurasia, Russia in Global Affairs 2016. https://eng.global-affairs.ru/pubcol/From-East-to-West-or-Greater-Eurasia-18440 [accessed 15.10.2022].
Kuzio, T, D'Anieri, P., The Sources of Russia's Great power Politics. Ukraine and the Challenge to the European Order, E-International Relations Publishing, Bristol 2018 p. 16. https://www.e-ir.info/wp-content/uploads/2018/06/The-Sources-of-Russia%E2%80%99s-Great-Power-Politics-E-IR.pdf. [accessed 17.10.2022].
Lukin, A., What the Kremlin Is Thinking, Putin's Vision for Eurasia, "Foreign Affairs" 2014, 93(4).
Malinova, O., Russia and the West in the 2000'. Redefining Russian identity in official political discourse. In R. Taras (Ed.), Russia's identity in international relations: images, perceptions, misperceptions, Routledge, London-New York 2012.
McSweeney, B., Security, Identity and Interests: A Sociology of International Relations, Cambridge Univesity Press, Cambridge 1999.
Mearsheimer J., Lecture at Robert Schuman Centre for Advanced Studies, Florence, June 6, 2022. https://www.youtube.com/watch?v=qciVozNtCDM [accessed 18.10.2022].
Mearsheimer, J. The Tragedy of Great Power Politics. W.W. Norton & Company, London – New York 2001.
Mearsheimer, J., Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin, „Foreign Affairs" 2014, 93(5).
Moravcsik, A., Taking Preferences Seriously: A Liberal Theory of International Politics, "International Organization" 1997, 51(4).
Nowak, A., History and Geopolitics: A Contest for Eastern Europe, PISM, Warszawa 2008.
Owens, M.T., In Defense of Classical Geopolitics, „Orbis" 2015, 59(4).
Potulski, J., Współczesne kierunki rosyjskiej myśli geopolitycznej, między nauka, ideologicznym dyskursem a praktyką, Wyd Uniwersytetu Gdańskiego, Gdańsk 2010.
Slaughter, A.M., International Relations. Principal Theories. https://www.princeton.edu/~slaughtr/Articles-/722_IntlRelPrincipalTheories_Slaughter_20110509zG.pdf [accessed 25.10.2022].
Sykulski, L. *Rosja-wyspa i Wielki Limitrof". Myśl geopolityczna Wadima Cymburskiego, In. Problemy współczesnej Europy – ujęcie interdyscyplinarne*, R. Fedan, B. Petrecka, S. Dyrda-Maciałek, (Eds.), Wydawnictwo Państwowej Wyższej Szkoły Techniczno-Ekonomicznej w Jarosławiu, Jarosław 2014.
Sykulski, L., *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, In. P. Eberhardt (Ed.), *Studia nad geopolityką XX wieku*, „Prace Geograficzne" nr 242, Warszawa 2013.
Taras, R., *The power of images and the images of power: past and present identity in Russia's international relations*, In: R. Taras (ed.) *Russia's Identity in International Relations Images, Perceptions, Misperceptions, Routledge,* London - New York 2012.
Trubetskoi, N., *On the Turanian Element in Russian Culture*, "Anthropology & Archeology of Eurasia" 1998, 37(1).
Waever, O., Towards a Political Sociology of Security Studies, "Security Dialogue" 2010, 41(6). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.870.4136&rep=rep1&type=pdf [accessed 25.10.2022].
Wendt, A., Anarchy is what States Make of It: the Social Construction of Power Politics, "International Organization" 1992, 46(2).
Wiśniewski, R., Przemiany terytorialne państwa rosyjskiego – aspekt historyczno-polityczny, In. P. Eberhard (Ed.), Studia nad geopolityką XX wieku. Prace Geograficzne" nr 242, Warszawa 2013.

Mykhailo Paslavskyi[1]
Mariia Ruda[2]
Taras Boyko[3]
Serhiy Stasevych[4]

ENSURING CYBER SECURITY OF MEDICAL COMPUTER SYSTEMS IN UKRAINE: ANALYSIS OF THE PROBLEM IN A COVID-19 PANDEMIC

Streszczenie

W artykule przeanalizowano krajowe strategie cyberbezpieczeństwa i podsumowano trendy w systemach cyberbezpieczeństwa oraz treść uzasadnionych naukowo propozycji zwiększenia zdolności Ukrainy do odpowiedniego przeciwdziałania zagrożeniom w zakresie cyberbezpieczeństwa oraz rozwoju krajowej systemu cyberbezpieczeństwa. W warunkach ścisłej kwarantanny wywołanej pandemią COVID-19, dzięki możliwościom nowoczesnych systemów informatycznych i telekomunikacyjnych, znaczna część usług medycznych została przekształcona w cyfrowe środowisko online. Proces ten doprowadził jednak do potencjalnych zagrożeń związanych z wyciekiem poufnych informacji za pośrednictwem cyberprzestępców. W chwili obecnej zagadnienia cyberbezpieczeństwa medycznych systemów komputerowych są bardzo aktualne i wymagają kompleksowego i wyważonego podejścia do ich rozwiązywania. Ważnym elementem jest ochrona prawna

[1] Dr Mykhailo Paslavskyi, Ukrainian National Forestry University, Lviv, Ukraine
[2] Dr Mariia Ruda, Lviv Polytechnic National University, Lviv, Ukraine.
[3] Prof. Taras Boyko, Lviv Polytechnic National University, Lviv, Ukraine
[4] Assoc. Prof. Serhiy Stasevych, Lviv Polytechnic National University, Lviv, Ukraine.

informacji poufnych znajdujących się w medycznych systemach komputerowych. Analiza technologii cyfrowych i systemów informatycznych służących do świadczenia usług medycznych on-line wykazała, że kwestie anonimizacji danych medycznych pacjentów, ochrony urządzeń medycznych podłączonych do Internetu przed wyciekiem poufnych informacji medycznych są niezwykle istotne. Dlatego przy tworzeniu odpowiedniego oprogramowania należy przestrzegać ścisłych zasad zapewniających poufność danych przetwarzanych w medycznych systemach informatycznych. Istnieją pewne obawy dotyczące bezpieczeństwa środowisk chmurowych, które są wykorzystywane jako platformy przechowywania danych w usługach opieki zdrowotnej, dotyczące ich podatności na potencjalne cyberataki. Analiza cyberbezpieczeństwa medycznych systemów komputerowych zidentyfikowała szereg zagadnień ochrony danych, znaczenie wieloczynnikowego uwierzytelniania użytkowników, kontroli dostępu, wykorzystania skutecznych schematów szyfrowania kryptograficznego w celu skutecznej ochrony zasobów informacyjnych systemów opieki zdrowotnej w Internecie oraz zidentyfikowania obszarów do dalszych badań aby zapewnić wysokiej jakości bezpieczne usługi medyczne online.

Słowa kluczowe: cyberbezpieczeństwo, cyberincydent, incydent cyberbezpieczeństwa, bezpieczeństwo informacji i sieci, informacje poufne.

Abstract

The article examines national cybersecurity strategies and summarizes trends in cybersecurity systems and the content of scientifically sound proposals to increase Ukraine's ability to adequately counter threats in the field of cybersecurity and the development of the national cybersecurity system. Under conditions of strict quarantine due to the COVID-19 pandemic, thanks to the capabilities of modern information and telecommunication systems, a significant part of medical services has been transformed into a digital environment online. However, this process has led to the potential dangers of leaking confidential information from cybercriminals. At present, the issues of cybersecurity of medical computer systems are very relevant and require a comprehensive and balanced approach to solving them. An important component is the legal protection of confidential information, which circulates in medical computer systems. An analysis of digital technologies and computer systems for the provision of online medical services has shown that the anonymity of patients' medical data and the protection of medical devices connected to the Internet from leaks of confidential medical information are acute. Therefore, when developing appropriate software, strict rules for ensuring the confidentiality of data processed in medical information systems must be followed. It has been clarified certain security issues in cloud environments, which are used as data storage platforms in the provision of health services, regarding their vulnerability to possible cyberattacks. To increase the trust and ensure the reliable protection of confidential medical information processed in such services, it is necessary to consider all software, hardware and organizational aspects. Analysis of cybersecurity of medical computer systems revealed a number of data protection issues, the importance of multifactor user authentication, access control, the use of effective cryptographic encryption schemes to effectively protect information resources of health ecosystems on the Internet and identify areas for further research to provide quality secure medical online services.

Keywords: cybersecurity, cyber incident, cybersecurity incident, information and network security, confidential information.

Introduction

Today, each country requires its capabilities to protect the constitutional rights and freedoms of its citizens, especially in those areas of public relations where the applicability of information and communication technology (ICT) products has a decisive impact on vital services, doing business, security of all types of communications, vital activities of citizens, society and the state. In addition, the penetration of such technologies into everyday life requires new knowledge in a new environment – cyberspace, which should be expected not only a large number of services and benefits, but also the development of existing and the creation of new threats. These threats are related to the use of mechanisms of unauthorized interference with the systems and security breaches of the information they process, the constant development of the development industry and the widespread use of various malicious and vulnerable software, the use of special operations in cyberspace on critical information infrastructure etc.

Public attention to the introduction of ICT in a wide range of public relations, the growing danger of their use makes urgent the task of systematic study of the national cybersecurity system, its shortcomings, justification of directions and tasks for its modernization. Among the negative factors influencing the national cybersecurity system, it is appropriate to highlight the following: almost full import of ICT products in the presence of a sufficient number of highly qualified software developers in Ukraine; low coordination of implementation of national informatization projects; inefficient budgeting for cybersecurity; low level of awareness of the tasks and goals of cybersecurity by almost all subjects of its provision; negligence or neglect of cybersecurity requirements; low cybersecurity culture at all levels and in all spheres of public and private life.

On the other hand, today in Ukraine there are factors to ensure compliance of cyber-security with modern requirements and best international practices of EU and NATO member states. The healthcare sector has long been a major target of cybercriminals, but since the advent of the COVID-19 virus, organizations at the forefront of the pandemic have seen an increase in cybersecurity incidents and attacks. Cybersecurity in medicine is really coming to a more important place.

In the period from February to June 2020, organizations related to HIPAA, reported about 192 large-scale data leaks from the Office of Civil Rights (OCR) of the US Department of Health and Human Services – more than twice as many as were recorded for the same period in 2019.

Although the types of cyber threats, what medical organizations have encountered during the COVID-19 pandemic is not unexpected, factors such as the rapid transition to telecommuting, the expansion of telemedicine, and the additional burden on resources felt by many organizations have come together to create new challenges.

For example, in recent months, some medical organizations have temporarily relaxed firewall (Windows security) rules to facilitate additional homework, reduced the number of providers, or entered into new contracts to rapidly deploy or expand telemedicine capabilities. Although the types of cyber threats faced by medical organizations during the COVID-19 pandemic are very similar to those that occurred before COVID-19, fraudsters exploit the fears associated with the pandemic. The Internet Crime Complaints Center said it received 1200 complaints in March related to cyber attacks involving the coronavirus, far exceeding the number of complaints it received against all types of cyber fraud in 2019. The government has warned that cybercriminals are targeting health authorities, pharmaceutical companies, the scientific community, medical research organizations and local authorities, as well as others involved in national pandemic work.

In addition to trying to steal important commercial information, hackers can try to steal valuable information related to the pandemic, such as confidential research on COVID-19, or information on national and international health policies. Cunning hackers who exploit the COVID-19 crisis are a global problem. In March, the Canadian Cybersecurity Center warned of malicious hackers targeting their public healthcare sector. They attack institutions to gain unauthorized access to intellectual property, research and development related to COVID-19. The Czech Republic has also faced a series of cybersecurity incidents, including an attack on one of the largest COVID-19 testing centers, which has led to its closure and transfer of patients to other hospitals. The threat to public health and safety posed by such malicious activities has prompted the US State Department to take global action. Below are some examples of cyber threats in the COVID-19 era, as well as some practical steps what organizations can do to manage cyber risks in today's increasingly virtual environment is presented.

Analysis of the literature

Normative and legal aspects of cybersecurity systems were considered in the works of K. Alexander [1], J. Liepman [2], V. Mazurov [3], R. Aldrich [4], E. Starostina [5], M. Schmitt [6], A. Shchetilov [7], Aquiles A. Almansi [8].

Ukrainian scientists have conducted research on various aspects of cybersecurity in Ukraine: I. Doronin (concerning the state body for the formation of a unified policy in the field of cybersecurity) [9], V. Kravets (measurements of cybersecurity assessment at different levels through the global, national and sectoral cybersecurity index) [10], L. Deshko and K. Bondareva (application of the mechanisms defined by the Budapest Convention on Cybercrime, the Agreement on the Implementation of the Ukraine-NATO Trust Fund, European Union–Ukraine Association Agreement) [11], I. Zabara (conclusion of bilateral, regional and universal international agreements on information and cybersecurity), [12] R. Lukyanchuk (international cooperation with the participation of

NATO) [13], V. Buryachko, V. Bogush (quality criteria for training in the field of cybersecurity) [14], V. Gurkovsky (methodological aspect of determining the content of security as an object of public administration in a global information society) [15], V. Dovhan (public administration in e-government and reforming the system of electronic services, the essence and structure of personnel security) [16], D. Dubov (study of the terminological system and analysis of the state of formation of the national cybersecurity system and strategic aspects of cybersecurity, public-private partnership and interaction) [17],V. Petrov (formation of the national cyber security system of Ukraine, cooperation of Ukraine with NATO) [18], A. Semenchenko (state and directions of development of the national cybersecurity system) [19], etc.

Until now, specialists in our country have been sufficiently engaged in the study of certain problems of public administration of the national cybersecurity system, which has led to the urgency of conducting a comprehensive study on the mechanisms of public administration in the field of cybersecurity.

Research results

Recently, the Internet of Things (IoT) paradigm has covered more and more areas of life. A variety of digital devices, networked and connected to the Internet, form the scope of modern high-performance remote services, available anytime, anywhere. In the healthcare field, these devices can range from innovative activity meters (such as pedometers) and blood pressure and heart rate monitors to modern devices capable of monitoring specialized implants (such as subcutaneous glucose monitors, pacemakers, or advanced hearing aids). Such opportunities allow to significantly improve the quality of medical care while reducing costs [4]. Thus, real-time remote screening of patients' physiological parameters for early detection of clinical deterioration becomes possible, which improves the decision-making process regarding diagnosis and treatment.

However, improving the quality of personalized online medical services is inextricably linked to ensuring that relevant software and hardware are protected from leaks of personal medical information. As e-health services generate large arrays of disparate medical data about patients and doctors, it is vital that this private information is securely protected and inaccessible to outsiders.

Regulatory and legal aspects of medical data protection

Health data belong to a specific category of personal data and require a higher level of protection than other categories of personal data.

Therefore, health data need separate legal regulation to streamline their collection and use. Appropriate legal framework for the protection of privacy has been developed and implemented in various countries [12]. For example, in the United States, there is the

HIPAA (Health Insurance Portability and Accountability Act) [21] on the mobility and accountability of health insurance, which helps maintain confidential information about the health of state citizens. In the European Union, the General Data Protection Regulation (GDPR) imposes a serious responsibility on citizens for non-compliance with the rules of privacy at various levels, especially in health and insurance organizations, because disruption of health data can have significant negative personal and social consequences for patients and their families.

Thus, the GDPR included in the list of data related to personal data of users the following [22]:

- genetic data – personal data relating to inherited or acquired genetic traits of an individual, which provide unique information about the physiology or health of the individual and which follow, in particular, from the analysis of the biological sample of the individual;
- biometric data – personal data after special technical processing relating to physical, physiological or behavioral characteristics of an individual, which allow to conduct or confirm the unique identification of the specified individual, such as images of a human face or dactyloscopic data;
- health data – personal data related to the physical or mental health of an individual, including the provision of health care services that provide information about the state of his health.

The GDPR strictly regulates the transparency for the user of how data about him is collected and processed [22]:

- personal data must be processed legally, fairly and transparently, with a mandatory declaration of information about the purposes, methods and scope of their processing in the most accessible and understandable form;
- personal data must be collected and used exclusively for the stated purposes by the Internet resource;
- personal data must be collected in volumes that do not exceed the required amount for the stated purposes of processing;
- personal data that is inaccurate must be corrected at the first request of the user;
- retention of personal data that uniquely identifies the user must be stored for a period not exceeding the stated purpose of processing;
- personal data must be protected against unauthorized and unlawful processing, damage and destruction.

In addition, the requirements of the GDPR establish a strict procedure for the form of obtaining the user's consent to the processing of his personal data in the form of approval or in the form of intended actions of the user on Internet services. This Law also stipulates that the user's consent to the processing of personal data expires if there was no choice or there was no possibility to revoke the consent without causing any harm to the user.

In Ukraine, in order to ensure the protection of personal data, which includes health data, biometric or genetic data, there are the Laws of Ukraine 'Fundamentals of Ukrainian Legislation on Health Care' [15] and 'On Personal Data Protection'. They regulate the issues of ensuring the protection of personal data in the field of health care, the functioning of medical information computer systems, state financial guarantees of medical care, etc.

Thus, in Art. 7 of the Law of Ukraine 'On Personal Data Protection' states the prohibition of processing personal data relating to health, sexual life, biometric or genetic data. However, this does not apply to the processing of personal data when it is 'necessary for health purposes, medical diagnosis, care or treatment or the provision of medical services, the operation of an electronic health system'. Provided that such data are processed by a medical professional or another person of the health care institution "[23].

For example, during the COVID-19 pandemic, there was an urgent need in the world to collect and store a significant amount of information about the health of the population. Employers began to monitor the incidence of COVID-19 among workers, public authorities began to collect data on the movement of persons and compliance with the regime of isolation, and people increasingly began to apply to health facilities for testing for COVID-19 or antibodies [17]. Healthcare information has come to be used frequently for references that can be used to identify a patient. Ensuring the confidentiality of personally identifiable information must be assumed and strictly controlled by the state at the legislative level. This should take into account the rapid progress of information and communication technologies, which may be ahead of and not meet the standards of industry and regulatory requirements on confidentiality and health issues, and therefore the need to adjust the regulatory framework.

The growing number, scale, intensity, complexity of cyber incidents and cyber threats in the global cyberspace, which no single state is able to effectively counter, is one of the main factors that necessitates their international cooperation in cybersecurity and cyber defense, combining their forces and means to reducing the level of cyber threats to citizens, society and the state. The urgency of the problem of international cooperation is due to the growing number, types and levels of cyber threats and cyber incidents in cyberspace, large-scale and dynamic introduction of ICT in all spheres of public life, building a digital society and state, the inability of any country to solve these problems, and for Ukraine in addition - by waging a hybrid war against Russia.

This area is formally identified as a priority in a number of legislative acts of Ukraine related to the development of national security, information (digital) society, digital economy, European and Euro-Atlantic integration of Ukraine, etc. For example, the purpose of the Cyber Security Strategy of Ukraine is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state, to achieve which, among other things, it is necessary to deepen international cooperation in this area. The annual action plans provide for measures to fulfill the task [24]

of developing international cooperation in the field of cybersecurity, supporting international initiatives in this field and cooperation of Ukraine with the EU and NATO to strengthen Ukraine's capabilities in the field of cybersecurity [24], participation in confidence-building measures in cyberspace [25].

One of the basic principles of cybersecurity is defined in Article 7 of the Law on Cyber Security and is formulated as: 'international cooperation to strengthen mutual trust in the field of cybersecurity and develop common approaches to combating cyber threats, consolidation of efforts in the investigation and prevention of cybercrime, prevention of the use of cyberspace for terrorist, military and other illegal purposes'. Issues of interaction, including information on cyber incidents, cover various layers: from public policy (on the upper layer of interaction), the effectiveness of which directly affects public response, to the content of a formalized report of a cyber incident, the speed of which directly affects the implementation of effective countermeasures, neutralization and minimization of negative consequences, the possibility of the fastest recovery of the object on which the incident had a negative impact.

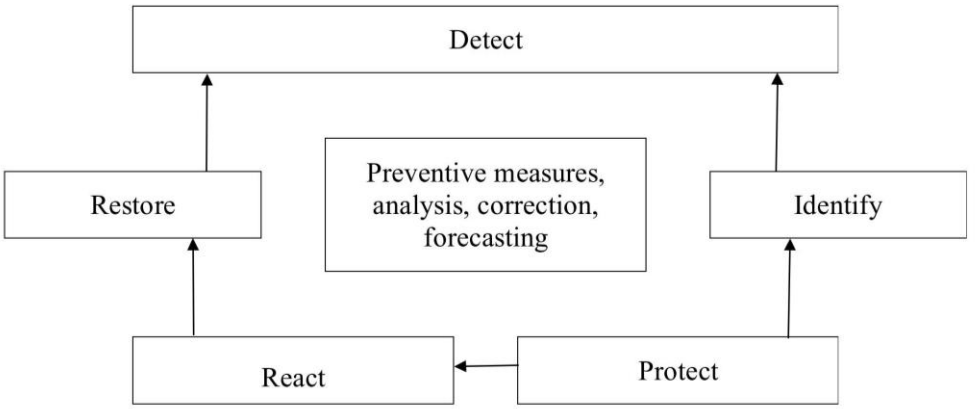


Fig. 1. The life cycle of a cyber incident

According to the stages of the life cycle (Fig. 1), the main part and importance of information work falls on the identification phase. The degree of regulation of such information affects, on the one hand, the willingness of the potential target to provide information about the cyber incident to the response team, implement a response plan to the cyber incident (if prepared in advance by the organization-object), avoid negative consequences of cyber incident, use appropriate response measures. On the other hand, it is to provide confidence that the information is provided to the response team, this team will ensure the confidentiality of such communication, inform other entities on which such an incident could potentially have a negative impact, avoid image losses by such entities.

Therefore, in the normative documents of international organizations in the field of cybersecurity, timely appropriate notification of a cyber incident under the established rules is a determining factor in the success of its neutralization and return to normal operation of the victim or readiness to effectively counter the potential victim.

The beginning of the incident	The answer	Processing time	Update
1/2 hour	3 hour	3 hours	By agreement or during the working day

Fig. 2. Example of setting a time frame for processing a cyber incident

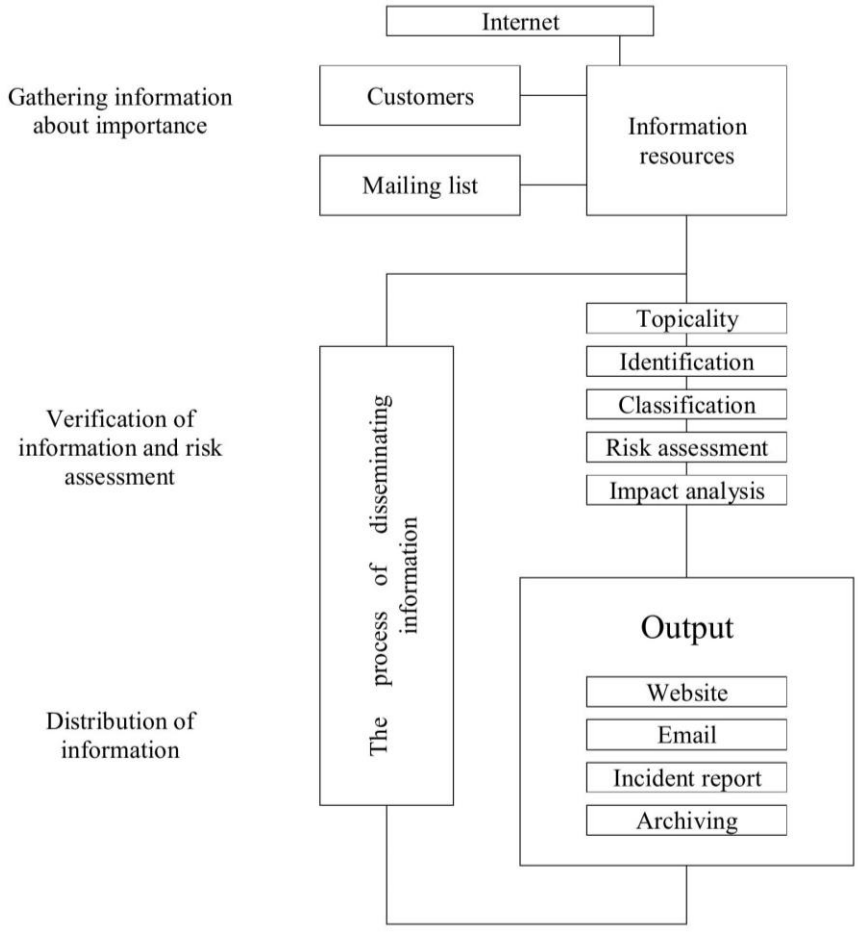


Fig. 3. An example of the scheme of the algorithm for working with information about a cyber incident

Scheme shown in Fig. 2, makes it possible to determine the importance of timely notification of a cyber incident, as the response time and further framework for its processing and neutralization may increase unjustifiably, which will affect the restoration and continued operation of the object in which the cyber incident took place.

Incident detection result: safety bulletin on risk assessment (example):

Bulletin name	.....	
Bulletin number	.....	
The affected systems	.....	
Operating system name and version	.....	
Risk	.....	High / Average / Low
Consequences / potential damage	.....	High / Average / Low
External identifiers	.....	
Vulnerability overview	.....	
Consequences	.....	
Decision	.....	
Description	.....	
Applications	.....	

Fig. 4. An example of a cyber incident report form

Figures 3-5 show examples that emphasize the importance of the content of the information message, the purpose of which is to provide exactly the information necessary to process a cyber incident.

It should be emphasized that when processing a cyber incident, there are three sources of information about it. They should be considered as overlapping in order to provide information in case of inability to use e-mail, telephone call center platform or facsimile or other means of communication. Typically, response teams need to work constantly (daily 24/7) and have the appropriate capabilities.

Currently, there are several regulations of various international organizations that establish ways to formalize and provide information about cyber incidents.

International Telecommunication Union pays due attention to the development and provides free access to a series of recommendations Rec. ITU-T 1200-1229 CYBER-SECURITY and 1500-1589 CYBERSECURITY INFORMATION EXCHANGE.

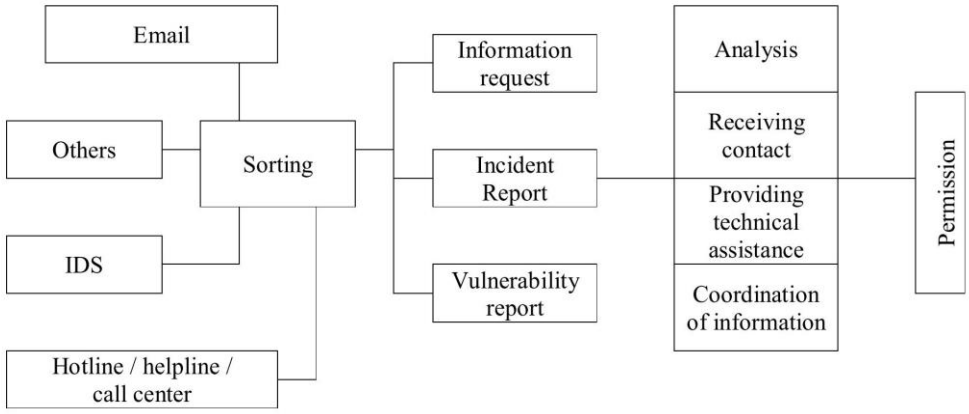


Fig. 5. Algorithm and sources for obtaining information about a cyber incident [ENISA]

Recommendation ITU-T X.1206: Vendor-neutral structure for automatic information security notification and update dissemination; ITU-T Recommendation X.1209 Capabilities and their context scenarios for cybersecurity information sharing and exchange. Recommendation X.1209 describes high-level scenarios and supporting opportunities for information sharing and cybersecurity information exchange. The purpose of its provisions is to support more effective security operations by supporting the joint exchange of information between trusted parties who jointly monitor, maintain and generally manage the security of systems and networks.

Recommendation ITU-T X.1500 Overview of cybersecurity information exchange defines a general model for exchanging information. It has the following main functions that can be used separately or together as appropriate:

- structuring cybersecurity information for exchange;
- identification of information and subjects of cybersecurity;
- establishing trust and political agreement between organizations that exchange information;
- request and response with information about cybersecurity;
- ensuring the integrity of the exchange of information on cybersecurity.

Recommendation ITU-T X.1541: Incident object description exchange format contains provisions, the application of which allows in the format of an electronic document to formalize the implementation of the description and minimize the processing time of cyber incident information.

Recommendation ITU-T X.1550 Access control models for incident exchange networks introduces existing approaches to the implementation of access control policies for incident exchange networks. This Recommendation introduces a variety of well-established access control models, sharing models, and criteria for evaluating

the effectiveness of an incident exchange network. The considered decisions based on standards, promote the implementation of different access control models in different models of cybersecurity information exchange and in different trust environments.

It should be noted that the whole set of standards in this area is still under development and only some of them are posted on the official website on the Internet.

The European Institute of Standards and Technology (ETSI) also develops and implements relevant standards. However, there is only one standard for the exchange of information on cyber incidents – ETSI TR 103 331 'CYBER; Structured threat information sharing'. It emphasizes that the exchange of information on cyber threats – often referred to as the exchange of information on threats – is one of the most important components of an organization's cybersecurity program and describes the current platform and results of structuring and sharing information on cyber threats to ensure interoperability and integration in this area.

Protection of medical personal data under COVID-2019 conditions

The global COVID-19 pandemic has rapidly changed the number of patients receiving online care. Telemedicine and online screening have become more common as a measurement (temperature, heart rate, blood pressure, oxygen saturation and respiratory rate) performed at the patient's home using biometric monitoring technologies provide convenient opportunities to collect vital signs.

This significantly reduces the risk of spreading the disease due to social distancing. Therefore, it can be argued that telemedicine is now helping to slow the spread of coronavirus disease. The World Health Organization (WHO) and the Centers for Disease Control in the United States and Europe have recognized that digital technologies and monitoring systems play an important role in maintaining public health. Studies [26] have shown that the introduction of telemedicine services significantly reduces the burden on hospitals during a pandemic, as remote medical services minimize the need for patient care.

Obviously, even after a pandemic, most users will prefer to receive online home care for remote prevention, diagnosis, advice, and even treatment as an alternative model of providing clinical services. Digital healthcare ecosystems have evolved on top of cloud platforms, IoT technology, mobile computing, artificial intelligence (AI) and machine learning (ML) for medical analytics. While such ecosystems shape the future of public and intelligent health care, the confidentiality of patients, doctors, nurses and health care providers is a matter of greater concern today than ever before. The anonymization of genomic data, the protection of medical devices connected to the Internet, from the leakage of confidential data on the health of patients require careful monitoring of confidentiality in this matter.

Approaches to the protocol and functionality of mobile software platforms for the provision of online medical services differ in different countries, taking into account the specific needs and mentality of states. Currently, the demand for high-quality software applications for this purpose is only growing. In proportion to the demand in the IT services market, there is a wide range of specialized software applications with interesting inventive solutions and new opportunities in the field of healthcare. Some of them are limited to collecting statistics of observations (demographics, symptoms, contact data) of patients and transmitting it to healthcare professionals in the relevant geographical areas for detection, reporting, active monitoring and rapid intervention in cases of COVID-19 infection. Others also have the ability to track, detect and control the distance between users via Bluetooth to limit the spread of the disease. Remote tracking, on the one hand, helps protect loved ones from unintentional infection, as it automatically detects and collects data on possible contacts with an infected person and recent trips.

However, on the other hand, this type of program implements mass surveillance, collection and use of personal data about all movements of the client, his diagnostic questionnaires, connection to an individual electronic medical card, TV sessions between patients and health care professionals.

With the consent of the user, this personal data may be used by health services to monitor and control the status of the disease in the region. Real-time patient monitoring data conducted for remote screening should be securely protected and inaccessible to outsiders. When developing appropriate software, strict regulatory rules must be followed to ensure the confidentiality of data to prevent possible violations of personal security and personal freedoms. Also, due to the interest in accessing this kind of personal data sometimes the customers of such software are special services or criminal companies. Therefore, it is important to conduct educational activities in society and control the authorized official bodies to enter the market of appropriate software to prevent abuse. Despite various technological methods, the risk of abuse cannot be completely eliminated. The dilemma between personal freedoms and public health should be considered philosophically and resolved very carefully and with the consent of society. Digital technologies thus have the means to provide the most ‘painless’ technological solutions.

Discussion of results

In general, technical regulation in Ukraine is carried out in accordance with the Laws of Ukraine ‘On Standardization’, a new edition of which has come into action from December 2020 and is more adapted to European and international legislation in this area. This Law defines the infrastructure and procedure for the development, revision and adoption of national standards, as well as the powers of standardization entities, in particular the national standardization body. The national standardization body adopts, repeals or renews

national standards, as well as coordinates the activities of technical standardization committees.

According to the website of the National Standardization Body (UkrNDNC, http://uas.org.ua/ua/), the state of standardization in the field of cybersecurity in Ukraine is characterized, first of all, by a number of such main problems as:

- there is no technical committee for standardization in the field of cybersecurity, but since 1992 technical committee (TC) TC-20 'Information Technologies' has been functioning and since 1995 TC-107 'Technical protection of information' has been functioning;
- annual programs of work on national standardization for 2020 (http://uas.org.ua/wp-content/uploads/2020/02/nakaz-38-21.02.2020-Programa-2020.pdf) and previous years, development or the adoption of national standards in the field of cybersecurity is not provided;
- TC-20 and TC-107 do not perform standardization work in the field of cybersecurity.

Thus, we can draw the following main conclusions about the state of standardization in the field of cybersecurity in Ukraine and prospects for its development based on the study and generalization of best international experience:

- subjects of standardization, which would embody the form of cooperation of interested legal entities and individuals in order to organize and perform work on international, regional, national standardization in the field of cybersecurity currently not in Ukraine;
- financing of standardization works in the field of cybersecurity in Ukraine is not carried out;
- there are no normative documents (standards) that set requirements for products, rules, procedures and processes, as well as requirements for entities in the field of cybersecurity in Ukraine;
- this area of work is possible for development only within the framework of public-private partnership in Ukraine, as well as the development and implementation of the concept and strategy of standardization in the field of cybersecurity;
- the formation of a TC in the field of cybersecurity in Ukraine in the near future is not expected, in this regard, until the work on the development and approval of draft national standards in the field of cybersecurity, including harmonized with international, it is possible and appropriate to involve other TCs, who have relevant experience in related fields. TC-20 'Information Technology', which is a member of subcommittee 27 of the Joint Committee for Standardization of the International Organization for Standardization (SC 27 JTC 1 ISO) and which ensured the adoption of a number of national standards in cryptographic protection, harmonization of national standards with international standards in electronic signatures, international cryptographic algorithms, information security management, etc., may, with its

consent and development, be involved in standardization work in the field of cybersecurity;
- the results of international standardization are characterized by the presence of a large number of standards and recommendations in the field of cybersecurity in particular, and information security in general, and the availability of reports on the effectiveness of their application, preparation of which in accordance with Ukrainian legislation is not provided. In addition, the areas of research and standardization of their results are similar in areas: artificial intelligence (AI), Internet of Things (IoT), Cloud Computing, Cryptography, Information Security and Network Security or Cybersecurity;
- lack of standardization strategy, concept and program in Ukraine leads to unsystematic research in the field of cybersecurity, chaos in decision-making on national standards, including harmonized with international ones, lack of money to organize standardization work in the field of cybersecurity. Therefore, at this stage of development of cybersecurity standardization, it would be more appropriate to implement international standards in the field of information security and network security (cybersecurity) with the appropriate degree of identity (harmonization of national standards with international ones).

The issue of security of the infrastructure for the collection, storage and transmission of medical data

The control of access to medical data transmitted between patients and health care providers is to restrict access based on the personal characteristics of all authorized persons. The concept of a reliable electronic database of medical information is central in assessing the degree of guarantee of system reliability. The logging mechanism is an important means of security. Healthcare providers may have not previous experience using remote patient care and may therefore be unfamiliar with data collection protocols and the context of the values collected. To make informed patient care decisions based on biometric data collected remotely, it is important to understand the technical solutions built into products, data collection protocols, form factors (physical size and shape), data quality considerations, and availability of verification information. The keeping of medical information protocols should be supplemented by an audit, i.e. an analysis of the registration of medical information.

There are also some security issues with possible vulnerabilities to cloud attacks that health services currently offer. They occur due to different types of insider threats (cloud provider administrators, cloud stack managers and solution administrators) and the complexity of managing authentication and access control in a multi-user mode with

a single access window (from one work computer to different employees of medical laboratories, enterprises, etc. where logins and passwords are automatically stored). Even when cloud platforms meet all regulatory requirements for data security and confidentiality, they process data that is not actually anonymous and therefore remains sensitive to identification. Therefore, cloud technology is not suitable for areas where you want to store and send data that is secret. The cloud environment itself is a fairly reliable system, but when an intruder enters it, it gains access to a huge data warehouse. Cloud service providers are constantly working to improve reliability and security: increase backup capacity to ensure reliability in the event of a jump in the case of DDOS attacks, duplicate communication channels to switch to them, strengthen identity management and access control to reduce selection risks and hacking passwords. However, SaaS service providers cannot control the correctness of the user's access organization, and when providing a PaaS service, they cannot guarantee that customers will develop their software in accordance with the established security policy on the provided platform. In addition, with the rapid influx of users of cloud services, the number of errors and information leaks from such resources increases. Therefore, to increase trust in cloud services and ensure reliable protection of important user data in such services, the formation of a high level of cybersecurity of the infrastructure must be approached with great care and take into account all software, hardware and organizational aspects. The security of medical computer information systems involves determining how to protect data, processes, and health systems from possible cyberattacks. Lack of encryption or the use of common encryption schemes, neglect of key management issues have allowed attackers to access millions of data records.

Unless appropriate cryptographic means and security measures are in place to verify integrity, this can lead to leaks of confidential information. Understanding data protection issues, multi-factor user authentication, access control, and the use of effective cryptographic encryption schemes are components for effectively protecting the information resources of health ecosystems on the Internet.

Conclusions

The study of the protection of medical information computer systems from cyber attacks has revealed key issues and areas for further research in the field of cybersecurity of telemedicine. Due to the lack of clearly defined definitions of cybersecurity at the European and international levels, the understanding of key terms varies considerably from country to country. This affects different approaches to cybersecurity strategies among countries. Lack of common understanding and approaches between countries can hinder international cooperation, the need for which is recognized by all countries.

1. Based on the analysis of the existing Coordination Procedure and the draft Joint Action Protocol, it can be noted that cybersecurity issues are addressed through the application of protection mechanisms introduced by information protection legislation and information security introduced by national standards harmonized with international ones.
2. Tasks to ensure cybersecurity are assigned to the existing units of information protection of military formations, enterprises, institutions and organizations of all forms of ownership, also formed under the legislation of Ukraine in the field of information protection, or to newly created entities – cybersecurity units. At the same time, there is no fundamental difference in the content of previously performed tasks between these bodies of interaction in terms of processing tasks both under the Coordination Procedure and the draft Protocol of Joint Actions.
3. The electronic and written notification specified in Annexes 1 and 2 to the Coordination Procedure remains a formalized document, which has a certain structure of information notification both about a cyber incident and about attempts of unauthorized actions concerning SID, which are processed in ITS.
4. The shortcomings inherent in both documents are the lack of rules for mandatory reporting on the results of measures taken at non-zero phases of interaction, resulting in a lack of understanding of the coordinator (if the Coordination Procedure applies) and the main actors of cybersecurity (when applying the draft Protocol of Joint Action) during the processing of the cyber incident.
5. In the banking system, the organization of information exchange on cyber incidents is regulated by the obligation of banks to develop and approve appropriate policies related to information security and cybersecurity. At the same time, the procedure for processing cyber incidents is not clearly spelled out.
6. The NIS Directive carefully describes the procedure, subjects and conditions of information both within the Member States and at the cross-border (within the EU) level. In Ukrainian documents (including their projects) the concept of 'single point of contact', its functions, tasks and responsibilities are not defined, the procedure for informing the competent authorities of partner countries (neighboring countries, etc.) about the possibility of the incident on these countries is not mentioned. There are also discrepancies in the time of reporting the incident (emergency): in the Interaction Procedure it is established during the day, in the draft Protocol of Joint Action – within an hour as it became known about the incident, and the NIS Directive – immediately without undue delay.
7. In Ukraine, the legislative level defines the need and priority of international cooperation in the field of cybersecurity, which it carries out both bilaterally with individual states, primarily with the United States, and with their associations (NATO and the EU). The article analyzes their experience in organizational, legal and financial mechanisms of international cooperation in the field of cybersecurity with Ukraine,

which are compared with the existing capabilities of Ukraine in this area. The analysis showed that Ukraine's bilateral international cooperation in the field of cybersecurity is currently formalized or is in the process of completing formalization only with the United States.

8. Regarding Ukraine's international cooperation in this area with NATO and the EU, despite a number of developed and implemented organizational and legal mechanisms for public administration of international cooperation, one of the main problems remains the problem of coordination of actions of cybersecurity actors, and which is the main reason for the insufficient effectiveness of public policy in this area.
9. It is proved that the effectiveness and efficiency of international cooperation in the field of cybersecurity depends on many factors, but the main ones are the coherence and coordination of actions of the main actors of cybersecurity in Ukraine and relevant international actors. It is noted that the situation is much more complicated with the coordination of international actors, who act, as a rule, not systematically for Ukraine and independently of each other, based primarily on their own interests (interests of international donors), which do not always fully meet national priorities of Ukraine, and, sometimes, even compete with each other in a particular area (industry), becoming a source of unsystematic, disordered, uncoordinated actions, creating, inter alia, a threat to the interoperability of organizational and technical systems and, consequently, significantly reduce efficiency and effectiveness of international cooperation. Repeated attempts by the state to solve this problem in Ukraine were unsuccessful, as each international donor independently, based on their personal interests, capabilities and understanding of our national interests chooses the scope (industry, region, etc.) and criteria for selecting potential performers (beneficiaries, recipients). Although there are mechanisms of self-organization and self-regulation among international donors, due to the above specifics of technical assistance they are fragmentary, informal, insufficiently motivated for donors and therefore, as a rule, ineffective and ineffective. The current state of international cooperation in the field of cybersecurity is characterized by:
   - lack of effective government policy in the organization of international cooperation in the field of cybersecurity;
   - inefficient, uncoordinated, uncontrolled and unaccounted use of received in the framework of international, including technical assistance in software and hardware to increase the level of their cyber protection;
   - insufficiently responsible attitude of the beneficiaries to the cyber security software and hardware received within the framework of technical assistance, negatively affects its international image and investment attractiveness, as well as the loss of Ukraine's ability to dynamically implement digital technologies.

10. The national cybersecurity system built on the basis of the Law does not fully ensure the proper implementation of tasks to ensure, in particular, international cooperation in the field of cybersecurity. Its basic elements must undergo a profound transformation. For example, the National Cyber Security Coordination Center should receive a new status, real authority to rebuild a modern, efficient, flexible, responsible, customer-oriented cybersecurity system. The renewed authority should include powers, in particular:

– introduction of an organizational mechanism for strategic planning of measures to implement the Cyber Security Strategy with objectives and measures defined in accordance with the objectives of the Strategy, united by a single idea, measured results and constant review of effectiveness of measures to achieve certain goals, providing specific measures for international cooperation;
– ensuring proper representation in international advisory bodies in the field of cybersecurity;
– organization of accounting, assessment of protective qualities, use and modernization (replacement) of tools and systems used to ensure cybersecurity of critical and information infrastructure;
– organization and ensuring the participation of Ukrainian teams in cyber-trainings and cyber-exercises, analysis of the gained experience and dissemination of the best received practices;
– organization of preparation and signing of international agreements with the USA, and the EU and its member states, and NATO on cooperation in the field of cybersecurity;
– constant monitoring, evaluation and implementation of advanced cybersecurity legislation of the world's leading countries and their associations, international, including European standards and recommendations.

Cybersecurity issues in the EU are clearly regulated in several documents, namely: eIDAS Regulation, NIS Directive, Cybersecurity Act, Digital Europe Program.

11. The experience of regulatory regulation in the field of network and information security of the Member States of the European Union and the EU as a whole can be implemented in Ukrainian legislation only in general and common approaches, in particular to identify Ukrainian institutions for dialogue and interaction with international partners at all levels (international, national, regional, sectoral, industry).
12. The issue of improving the effectiveness of planning reflects a certain institutional imperfection of the cybersecurity system and needs to be addressed together with other tasks with the improvement of legal, financial, organizational and staff support for the activities of cybersecurity entities.

The new version of the Cyber Security Strategy of Ukraine should be free from the shortcomings of its current version and contain more specific tasks and measures to ensure cyber security with the possibility of adjusting them to threats in cyberspace.

13. The considered problems and proposals for its solution will allow to translate the planning of cybersecurity measures in line with recent changes in the budget legislation of Ukraine on the introduction of medium-term planning, which should be the organizational basis for improving budgeting of cybersecurity measures in government agencies and in the case of their implementation in the non-budgetary sphere and other actors of cybersecurity.

Approaches and directions of improvement of national mechanisms of public administration in the field of international cooperation in the field of cybersecurity are offered and the recommendations to state bodies are proved.

References:

Bures O. Contributions of private business to the provision of security in the EU: beyond public-private partnerships // Crime, Law and Social Change. – 2017. – № 67 (3).

Complete guide to GDPR compliance. URL: https://gdpr.eu / (дата звернення: 12.02.2021).

Cyber security research and development act. URL: https://legcounsel.house.gov/Comps/Cyber%20Security%20Research%20And%20Development%20Act.pdf.

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 07.02.2013 JOIN(2013)1 URL: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Directive 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A32016L0680.

ENISA publication: National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace URL: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

Health insurance portability and accountability act. URL: https://aspe.hhs.gov/report/health-insurance porta bility-and-accountability-act-1996

HIPAA: як захищають медичні дані пацієнтів в США? URL: https://everlegal.ua/hipaa-yak-zakhy schayut - medychni-dani-patsientiv-v-ssha.

ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary URL: https://www.iso.org/ru/ standard/73906.html

ISO/IEC 27032 Information technology — Security techniques — Guidelines for cybersecurity URL: https://www.iso.org/standard/44375.html.

Korchenko O., Loginov I., Skvortsov S. Stationary systems of cyberattacks detection and prevention for cyber-protection and cyber-counterintelligence (by example USA) // Ukrainian Scientific Journal of Information Security. – 2019. – vol. 25, issue 1. P. 5-12 URL: http://jrnl.nau.edu.ua/index.php/Info-security/index.

Kosmidis, D., Nestoras, K. Telehealth and telenursing in time of COVID-19. The step of ASCLIPI. 2020. Vol. 19, № 4.

Marvell S. The real and present threat of a cyber breach demands real-time risk management // Acuity Risk Management. – 2015.

National Cyber Strategy of the United States of America URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

NIST SP 800-53 (Rev. 4) Security and Privacy Controls for Federal Information Systems and Organizations URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Primary Directive on CIS Security, AC/35-D/2004-REV3 URL: http://www.dksi.bg/NR/rdonlyres/6DC49C44-5C52-47A2-8773-6BF11C59E53C/0/Primary_CIS_SecurityAC35D2 004REV3.pdf

Public Private Partnerships (PPP) - Cooperative models URL: https://www.enisa.europa.eu/ publications/public-private-partnerships-ppp-cooperative-models.

Recommendation ITU-T X.1205 (04/2008) SERIES X: DATA NETWORKS, OPEN SYSTEM – COMMUNICATIONS AND SECURITY – Telecommunication security – Overview of cybersecurity URL: https://www.itu.int/net/ITU-R/asp/terminology-definition.asp?rlink={4B499A4A-3E11-4AE6-9B03-46FB1A662507}&lang=en

Recommendation ITU-T X.1206 A vendor-neutral framework for automatic notification of security related information and dissemination of updates URL: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=9287

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807.

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/uri=OJ:JOL_2013-_165_R_0041_01&qid=1397226946093&from=EN

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC URL: https://ec.europa.eu/futurium/ en/system/files/ged/eidas_regulation.pdf.

Regulatory framework for electronic communications in the European Union URL: https://ec.europa.eu/digital-single-market/en/news/regulatory-framework-electronic-communications-european-union

The European Union is updating its cybersecurity strategy URL: https://www.eu2017.ee/news/press-releases/european-union-updating-its-cybersecurity-strategy

Ukraine Cybersecurity Cooperation Act of 2017 URL: https://www.congress.gov/bill/115th-congress/house-bill/1997/text.

Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Задерейко О.В. Кібербезпека України: аналіз су-часного стану. Захист інформації. 2019. Т. 21. № 3. Київ: Національний авіаційний університет.

Grzegorz Zając[1]

Prawne aspekty bezpieczeństwa przewozów lotniczych i ochrony przed aktami bezprawnej ingerencji w ujęciu międzynarodowym

Legal aspects of air transport safety and security against acts of unlawful interference in the international context

Streszczenie

Celem badawczym artykułu jest omówienie prawnych uregulowań w zakresie bezpieczeństwa w transporcie lotniczym. Wykonywanie operacji lotniczych przez przewoźników oparte jest o szereg wymogów prawnych, technicznych, operacyjnych. Również porty lotnicze muszą spełniać określone normy międzynarodowe, aby mogły przyjmować i obsługiwać zarówno przewoźników lotniczych jak i pasażerów. Najważniejszym w działalności każdego podmiotu lotniczego jest wymóg bezpieczeństwa. Wykonywanie przewozów lotniczych na świecie oparte jest o międzynarodowe uzgodnienia i bilateralne umowy między państwami. W artykule autor dokonuje analizy międzynarodowego prawa lotniczego w zakresie bezpieczeństwa wykonywania przewozów lotniczych i ochrony przed aktami bezprawnej ingerencji. W szczególności analizie poddane zostaną zagadnienia międzynarodowych standardów bezpieczeństwa, zakresu stosowania aspektów bezpieczeństwa i ochrony lotnictwa w umowach dwustronnych, procedur prawnych badania wypadków lotniczych, a także omówienie instrumentów ochrony pasażerów przed przewoźnikami lotniczymi, którzy nie spełniają ‚minimalnych wymogów bezpieczeństwa.

Słowa kluczowe: bezpieczeństwo lotnicze, ochrona lotnictwa, terroryzm lotniczy, pasażer lotniczy, transport lotniczy, lotnisko

[1] Dr Grzegorz Krzysztof Zając, adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach, ORCID ID: 0000-0002-5504-5228

Abstract

The aim of the article is to discuss legal regulations in the field of safety in air transport. The performance of air operations by carriers is based on a number of legal, technical and operational requirements. Airports also have to meet certain international standards in order to serve and handle both air carriers and passengers. The most important in the activity of any entity acting in the field of aviation is the safety and security requirement. The provision of air transport in the world is based on international agreements and bilateral agreements between countries. In the article, the author analyzes international aviation law in the field of safety of air transport and protection against acts of unlawful interference. In particular, the issues of international safety standards, the scope of application of aviation safety and security aspects in bilateral agreements, legal procedures for investigating air accidents, as well as a discussion of instruments to protect passengers against air carriers that do not meet the minimum safety requirements, will be analyzed.

Keywords: aviation safety, aviation security, aviation terrorism, air passenger, air transport, airport

Podstawową kwestią w funkcjonowaniu przemysłu lotniczego jest zapewnienie bezpieczeństwa wszystkim użytkownikom i podmiotom, których dotyczy. Co niektórzy mogliby powiedzieć, że przynoszenie zysków, rentowność przedsiębiorstwa jest czynnikiem warunkującym jego istnienie. To prawda, lecz czy to będzie lotnisko, czy przewoźnik lotniczy, który nie będzie spełniał minimalnych wymogów bezpieczeństwa, to bez właściwego podejścia do bezpieczeństwa wykonywania przewozów lotniczych taki podmiot nie utrzyma się na bardzo wymagającym i wystandaryzowanym rynku lotniczym.

Każdy użytkownik chce korzystać z jak najlepszych warunków zarówno pod względem, jakości, organizacji, zakresu swojej oferty. Przy tym kwestie bezpieczeństwa są fundamentem, gdyż brak wypełnienia odpowiedniego minimum wpływa bezpośrednio na jakość usług, organizację systemu i dostępność oferty. Władze lotnicze w imieniu państwa nie dopuszczą do użytkowania danego podmiotu, jeśli nie spełni odpowiednich warunków formalnych w zakresie bezpieczeństwa. Może zdarzyć się, szczególnie w państwach mniej demokratycznych, lub w tych, w których przepisy i standardy lotnicze nie są tak rygorystycznie przestrzegane, lecz i w tych miejscach wzrasta świadomość społeczna o konsekwencjach ekonomiczno-społecznych jakie niesie ze sobą negatywny wizerunek lotniska czy przewoźnika dla całego państwa. W pierwszej kolejności to na państwie ciąży obowiązek, aby podmioty działające na rynku lotniczym spełniały odpowiednie standardy międzynarodowe, czy regionalne lub krajowe, a w drugiej kolejności to sami pasażerowie chcą korzystać z jak najbardziej bezpiecznych form transportu. Wreszcie to w interesie przewoźnika lotniczego lub portu lotniczego jest, by udostępniać i oferować usługi, które są bezpieczne, co wpływa na ich kondycję ekonomiczną.

Istnieją międzynarodowe uregulowania oraz standardy i zalecenia, które należy respektować w zakresie bezpieczeństwa. Nie wszystkie mają charakter prawno-wiążący, wiele jest zaleceń, które z racji specyfiki środka transportu należy przestrzegać we

własnym interesie oraz interesie tych, do których kierowana jest usługa. Regulacje międzynarodowe stanowią podstawę funkcjonowania całego lotnictwa cywilnego. Tym szczególnym dokumentem jest konwencja o międzynarodowym lotnictwie cywilnym (konwencja chicagowska) z 7 grudnia 1944 r. Oprócz niej, istnieją wiążące prawnie państwa członkowskie załączniki, określające standardy i zalecane praktyki postępowania. Przyjmowane są przez Radę Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO), na podstawie art. 37 konwencji. Istnieją też regionalne, bardziej szczegółowe i niekiedy bardziej restrykcyjne rozwiązania dotyczące bezpieczeństwa przewozów lotniczych w Europie, które to przyjmowane są pod auspicjami Unii Europejskiej (UE), lub Agencji Unii Europejskiej do spraw Bezpieczeństwa Lotniczego (EASA). Pozostałe regiony świata radzą sobie nieco gorzej z regionalnym ujednoliceniem przepisów, co nie oznacza, że normy bezpieczeństwa muszą odbiegać od tych europejskich. Przeciwnie, w każdym państwie obowiązują regulacje międzynarodowe, których nieprzestrzeganie stanowi naruszenie przyjętych zobowiązań i wiąże się z groźbą nałożenia sankcji.

Wykonywanie operacji lotniczych przez przewoźników oparte jest o szereg wymogów, jakie musi on spełnić. Również porty lotnicze muszą spełniać określone normy międzynarodowe, aby mogły przyjmować i obsługiwać zarówno przewoźników lotniczych jak i pasażerów. Najważniejszym w działalności każdego podmiotu jest wymóg bezpieczeństwa. Zagadnienie to rozpatrywane jest współcześnie w kontekście każdego innego obszaru, czyli bezpieczeństwo obsługi naziemnej, bezpieczeństwo obsługi pasażerów i odprawy, bezpieczeństwo w starcie i lądowaniu statków powietrznych, bezpieczeństwo żeglugi powietrznej, bezpieczeństwo techniczne i operacyjne statków powietrznych, itp.

Cel, przedmiot i metodologia badań

Bezpieczeństwo jest jednym z poważnych wyzwań współczesnego lotnictwa. W wymiarze bezpieczeństwa międzynarodowego, bo taki ma charakter lotnictwo cywilne, należy je rozpatrywać w ujęciu współpracy międzynarodowej, wspólnego rozwiązywania zbiorowych problemów oraz umiejętności budowania powszechnego zaufania[2]. Głównym celem działalności przewoźników jest osiąganie zysków poprzez jak największą liczbę przewożonych pasażerów. Mogą oni wykonywać loty na podstawie międzynarodowych uzgodnień i bilateralnych umów między państwami. Właśnie w nich znajdziemy ramy prawne dotyczące obowiązku bezpiecznego wykonywania operacji lotniczych. Przewoźnicy muszą spełnić wymogi w nich określone. Umowy wielostronne stanowią ramy prawne i organizacyjne oraz na ich podstawie dokonuje się harmonizacja przepisów i praktycznego działania podmiotów w transporcie lotniczym, w tym państw. Natomiast umowy dwustronne konkretyzują zawarte w wielostronnych umowach przepisy i stanowią

[2] K. Świerszcz, *Bezpieczeństwo państwa w czasach współczesnych w ujęciu podmiotowo-aksjologicznych wyzwań*, Przegląd Nauk o Obronności 1/2016, s. 69.

uszczegółowienie komunikacji lotniczej miedzy dwoma stronami. Z uwagi na coraz powszechniejszą uwagę na kwestie bezpieczeństwa, również w umowach dwustronnych zawiera się stosowne klauzule bezpieczeństwa tak, aby państwa w związku z wypadkiem lotniczym lub aktem terrorystycznym wymierzonym w lotnictwo wiedziały jak się zachować i łatwiej im było podjąć działania. Współpraca państw w tej płaszczyźnie jest niezwykle pożądana i konieczna.

Celem artykułu jest omówienie prawnych uregulowań w zakresie bezpieczeństwa w transporcie lotniczym. W artykule autor dokonuje analizy międzynarodowego prawa lotniczego w zakresie bezpieczeństwa wykonywania przewozów lotniczych i ochrony przed aktami bezprawnej ingerencji. Przedmiotem badań autora są zagadnienia międzynarodowych standardów bezpieczeństwa, zakresu stosowania aspektów bezpieczeństwa i ochrony lotnictwa w umowach dwustronnych, procedur prawnych badania wypadków lotniczych, a także omówienie instrumentów ochrony pasażerów przed przewoźnikami lotniczymi, którzy nie spełniają ‚minimalnych wymogów bezpieczeństwa. Autor stawia hipotezę, że o bezpieczeństwie przewozów lotniczych świadczą surowe przepisy prawne w różnych płaszczyznach wykonywania przewozów lotniczych i ich przestrzeganie przez poszczególne podmioty. W celu zweryfikowania hipotezy zostaną wykorzystane metody badawcze właściwe dla dziedziny prawa i nauk społecznych, tj. metoda dogmatyczno-prawna, metoda analizy i krytyki piśmiennictwa oraz metoda syntezy.

Artykuł stanowi syntetyczne podejście do tego złożonego zagadnienia badawczego. Autor syntetycznie ujął szerokie zagadnienie i w sposób uporządkowany dokonał analizy problemu badawczego. Temat ten stanowi rzadko poruszany materiał analityczny w literaturze.

Międzynarodowe standardy bezpieczeństwa

Zarówno porty lotnicze jak i przewoźnicy działają w oparciu o jednolite międzynarodowe normy bezpieczeństwa. Fundamentem jest konwencja chicagowska, która została przyjęta przez państwa po to, by *międzynarodowe lotnictwo cywilne mogło się rozwijać w sposób pewny i prawidłowy, a międzynarodowe służby transportu lotniczego mogły być ustanawiane na zasadzie jednakowych możliwości dla wszystkich i prowadzone w sposób właściwy i ekonomiczny*, a także biorąc pod uwagę, że *przyszły rozwój międzynarodowego lotnictwa cywilnego może przyczynić się w znacznej mierze do stworzenia i utrzymania przyjaźni i zrozumienia między narodami i ludami świata oraz że wszelkie jego nadużycie może zagrozić bezpieczeństwu powszechnemu*. Musi istnieć jeden podstawowy ład bezpieczeństwa lotniczego, by każdy działający podmiot mógł bezpiecznie wykonywać swoją działalność. Ład chicagowski opiera się zapisach konwencji oraz załącznikach i dokumentach regulujących różne aspekty bezpieczeństwa lotniczego i jest jednym z najlepiej funkcjonujących na świecie.

Nie ma jak dotąd jednej międzynarodowej definicji bezpieczeństwa lotniczego. Nie występuje ona w żadnej umowie wielostronnej, ani nie praktykuje się definiowania tej

kategorii w umowach dwustronnych. Normatywne określenie bezpieczeństwa lotniczego funkcjonuje zazwyczaj w płaszczyźnie krajowego porządku prawnego. Brak jest prawno-międzynarodowej definicji z uwagi na odmiennie postrzeganie kategorii „bezpieczeństwo" przez państwa jako pewnego systemu wartości[3]. Bezpieczeństwo w lotnictwie wiąże się z utrzymaniem określonego porządku. Na stan bezpieczeństwa lotniczego wpływa wiele czynników, gdyż jest to zagadnienie obszerne obejmujące szereg elementów nie związanych z nim bezpośrednio. Według definicji G. Zająca bezpieczeństwo lotnicze (ang. *safety*) rozumiane *jako zbiór przepisów prawnych dotyczących produkcji i utrzymania statków powietrznych oraz funkcjonowania świadczeniodawców i świadczeniobiorców w środowisku lotniczym*, natomiast ochrona lotnictwa (ang. *security*) *obejmuje ogół ram organizacyjno-prawnych oraz operacyjno-technicznych zapobiegania nielegalnym aktom wymierzonym w lotnictwo cywilne*[4].

Te dwa terminy są wzajemnie komplementarne, jako że zapewnienie właściwego poziomu bezpieczeństwa lotniczego nie może się odbyć bez przyjęcia stosownych środków i procedur zapobiegających aktom terroryzmu skierowanych w sektor lotniczy. W szerszym ujęciu na bezpieczeństwo mają wpływ również czynniki ekonomiczne (np. kwestia defragmentacji nieba (podziału), zarządzanie ruchem lotniczym (ang. *Air Traffic Management – ATM*), czy techniczno-operacyjne (np. ujednolicenie standardów technicznych, właściwy dobór slotów (przydziałów czasów na start i lądowanie samolotów w porcie lotniczym).

Zagadnienie bezpieczeństwa w lotnictwie cywilnym znajduje się w wielu dokumentach międzynarodowych, umowach wielostronnych i dwustronnych, w szczególności podstawowe przepisy znajdują się w konwencji chicagowskiej oraz w dwóch jej załącznikach: nr 17 („Ochrona lotnictwa") oraz nr 19 („Zarządzanie bezpieczeństwem").

Konwencja chicagowska powstała w czasie, kiedy trwały jeszcze działania wojenne. Rok 1944 coraz bardziej przybliżał koniec II wojny światowej, jednocześnie państwa prowadziły intensywne działania dyplomatyczne w celu uregulowania porządku międzynarodowego opartego o powszechny system bezpieczeństwa zbiorowego. W tym właśnie roku trwały prace nad kodyfikacją prawa międzynarodowego w różnych dziedzinach, np. finansowych czy lotniczych[5]. Odnośnie tej ostatniej, stan lotnictwa od przyjęcia pierwszej powszechnej międzynarodowej konwencji w tym zakresie w 1919 r. (konwencja paryska) zmienił się i potrzebne były bardziej przejrzyste zasady uwzględniające inny wymiar bezpieczeństwa.

---

[3] Szerzej o bezpieczeństwie jako systemie wartości [w:] J. Kukułka, *Bezpieczeństwo a współpraca obywatelska. Współzależności i sprzeczności interesów*, „Sprawy Międzynarodowe", 1982, nr 7, s. 34.

[4] G. Zając, *Wspólna polityka lotnicza Unii Europejskiej*, Przemyśl 2009, s. 130.

[5] W dziedzinie finansowej został utworzony tzw. System z Bretton Woods, który tworzony był przez Bank Światowy (popr. Międzynarodowego Banku Odbudowy i Rozwoju – IBRD) oraz Międzynarodowy Fundusz Walutowy – IMF.

Bezpieczeństwo przewozów lotniczych jest fundamentalną kwestią dla państw, przewoźników, portów lotniczych, pasażerów, instytucji zapewniających bezpieczeństwo żeglugi lotniczej (usługi nawigacji lotniczej), organów kontroli ruchu lotniczego. Bezpieczne środowisko musi zapewnić państwo poprzez odpowiednie zapisy w prawie międzynarodowym lotniczym. W pierwotnej wersji konwencji chicagowskiej zapis dotyczący bezpieczeństwa lotniczego był wyjątkowo ograniczony. W artykule 3 ust. d przewidziano jedynie, że przy ustanawianiu przepisów dotyczących państwowych statków powietrznych będzie uwzględnione bezpieczeństwo żeglugi cywilnych statków powietrznych. Zatem, nałożono na państwa obowiązek wdrożenia krajowych regulacji prawnych uwzględniających bezpieczeństwo transportu powietrznego, zarówno cywilnego jak i państwowego. Ten lakonicznie sformułowany przepis cedował na poszczególne państwa cały ciężar wprowadzania norm bezpieczeństwa w transporcie lotniczym. Nie przewidziano konsekwencji takiego zapisu. Dynamicznie rozwijająca się branża lotnicza ukazała szereg błędów w tym zakresie. Nie przypuszczano, że samoloty będą również używane niezgodnie z ich przeznaczeniem, tj. jako środka do zabijania lub porywania ludzi dla wymuszania okupu lub realizacji innych celów porywaczy.

W 1984 r. wprowadzono artykuł 3bis do konwencji chicagowskiej, zgodnie z którym wszystkie państwa powstrzymają się od użycia broni przeciwko statkom cywilnym w locie, tak aby nie zagrażać życiu pasażerom i załogi[6]. Każde państwo, na podstawie art. 3 bis ust.b, ma prawo zażądać lądowania statku powietrznego w wyznaczonym miejscu, jeśli istnieją uzasadnione obawy, że jest on używany do celów niezgodnych z konwencją. Państwo może nakazać stosowanie się do wszelkich poleceń załodze statku powietrznego, która ma obowiązek się do nich dostosować. W tym celu, państwa mogą również posłużyć się „wszelkimi stosownymi środkami". Gdyby w taki sposób brzmiała dyspozycja tego przepisu, to oznaczałaby ona możliwość użycia broni, czyli np. zestrzelenie statku powietrznego. Jednakże, zapis ten zawiera rozszerzenie stanowiące, że środki te muszą być zgodne z powszechnie obowiązującymi zasadami prawa międzynarodowego, w tym zasadami określonymi w art.2 Karty Narodów Zjednoczonych. Z uwagi na fakt, iż obecnie wszystkie państwa, które ratyfikowały konwencję chicagowską są członkami Narodów Zjednoczonych są zobowiązane do poszanowania praw i obowiązków wynikających z Karty oraz innych umów międzynarodowych. Dyspozycja zawarta w art.3 bis ust.a zawiera wyraźny i niebudzący wątpliwości nakaz „powstrzymania się od uciekania się od użycia broni przeciwko cywilnemu statkowi powietrznemu w locie oraz że w przypadku przechwycenia życie osób na pokładzie i bezpieczeństwo statku powietrznego nie mogą być zagrożone".

Pojawienie się w połowie XX wieku ataków terrorystycznych wymierzonych w bezpieczeństwo lotnictwa cywilnego zmusiło państwa do szybkich zmian w kierunku

[6] Artykuł 3bis został przyjęty przez Zgromadzenie ICAO w dniu 10 maja 1984 r. Zgodnie z artykułem 94 ust.a zmiana ta weszła w życie w dniu 1 października 1998 r.

ujednolicenia zasad postępowania z osobami naruszającymi bezpieczeństwo transportu lotniczego. Indywidualne podejście jest bezprzedmiotowe, gdyż lotnictwo ma charakter głównie międzynarodowy i to przewozy międzynarodowe stanowią o istocie rozwoju lotnictwa cywilnego. Dlatego też konieczne było wypracowanie wspólnych standardów i jak najszybsze wdrożenie ich w życie. W wyniku takiego działania został stworzony międzynarodowy system przeciwdziałający aktom terroryzmu lotniczego (tzw. system tokijsko-hasko-montrealski). System ten kształtowany jest w oparciu o następujące konwencje:

- konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych, podpisana w Tokio w dniu 14 września 1963 r. (konwencja tokijska),
- konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, podpisana w Hadze w dniu 16 grudnia 1970 r. (konwencja haska),
- konwencja w sprawie zwalczania bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, podpisana w Montrealu w dniu 23 września 1971 r. (konwencja montrealska).

Jednocześnie wprowadzono nowe międzynarodowe przepisy dotyczące ochrony lotnictwa poprzez przyjęcie załącznika nr 17 do konwencji chicagowskiej. Nastąpiło to stosunkowo późno, bo dopiero 22 marca 1974 r., tj. trzydzieści lat po przyjęciu samej konwencji. Szkody nie tylko osobowe, lecz również materialne, wyrządzane przez akty terrorystyczne były w tamtym okresie ogromne. Dotyczyło to przede wszystkim używania samolotu jako środka do zniszczenia określonego celu na Ziemi.

Przyjęty system stanowi ramy organizacyjno-prawno-funkcjonalne dotyczące bezpieczeństwa w międzynarodowym ruchu lotniczym. Warto tu podkreślić, że te wielostronne uregulowania dotyczą wyłącznie oddziaływania w sferze międzynarodowej, wyłączone są natomiast loty krajowe, które podlegają krajowym przepisom. Odnośnie bezpieczeństwa statków powietrznych i ochrony ich przed nielegalnym zawładnięciem, najpełniej kwestie te reguluje konwencja haska. Zawiera wyraźne określenie bezprawnego zawładnięcia statkiem powietrznym, umieszczając ten czyn w kategorii „przestępstwa". Zgodnie z jej art.1 „każda osoba, która na pokładzie statku powietrznego będącego w locie:

a) bezprawnie, przemocą lub groźbą użycia przemocy lub w każdej innej formie zastraszenia dokonuje zawładnięcia statkiem powietrznym lub przejęcia nad nim kontroli albo też usiłuje popełnić taki czyn, lub
b) współdziała z osobą, która popełnia lub usiłuje popełnić taki czyn – popełnia przestępstwo".

W tej definicji znalazły się bardzo istotne dwa elementy. Po pierwsze, jako przestępstwo zostało zakwalifikowane również usiłowanie jego popełnienia. Po drugie, niezwykle istotne jest uznanie za przestępcę także współsprawcę. Osoba taka będzie

odpowiadać w takim samym stopniu i według takich samych kryteriów jak przestępca główny. Należy nadmienić, że ściganie wspomnianych sprawców jest możliwe tylko wtedy, gdy sprawca dokonał tego na pokładzie samolotu „będącego w locie". Stąd też celowe było zamieszczenie w konwencji definicji tego terminu. Uznano, że statek powietrzny „jest w locie od chwili, gdy załadowanie zostało zakończone i wszystkie drzwi zewnętrzne zostały zamknięte, aż do chwili, gdy jedne z tych drzwi zostały otwarte w celu wyładowania". Natomiast, gdyby doszło do przymusowego lądowania to przyjmuje się, że lot trwa dopóki, dopóty właściwe władze nie przejmą odpowiedzialności za statek powietrzny oraz osoby i mienie znajdujące się na pokładzie.

W konwencji haskiej zostało poczynione jeszcze jedno ważne zastrzeżenie. Ponieważ jest to umowa międzynarodowa o charakterze wielostronnym, to ma ona zastosowanie tylko wówczas, gdy miejsce startu lub ostatecznego lądowania samolotu, na pokładzie którego popełniono przestępstwo w rozumieniu tej konwencji, jest położone poza terytorium państwa rejestracji tego statku powietrznego. Dotyczy to zarówno lotów międzynarodowych (tzw. piątej, szóstej, bądź siódmej wolności lotniczej), jak i lotów krajowych (tzw. ósmej wolności, czyli kabotażu). Takie sformułowanie traktatowe wydaje się uzasadnione, gdyż jeśli dany czyn nastąpił na pokładzie samolotu wykonującego wyłącznie lot krajowy na terytorium państwa rejestracji tego statku, to wtedy mają zastosowanie przepisy prawa wewnętrznego tegoż państwa. Wyłączeniem od tej zasady jest jedynie sytuacja, gdy sprawca lub domniemany sprawca przestępstwa znajdzie się na terytorium państwa innego niż państwo rejestracji tego statku powietrznego.

Niezależnie od miejsca przebywania sprawcy lub domniemanego sprawcy przestępstwa, państwa sygnatariusze konwencji haskiej mają obowiązek zatrzymać taką osobę. Niezwłocznie powinno podjąć się działania mające na celu wyjaśnienie wszelkich okoliczności i ustalenie faktów. Gdyby sprawca przestępstwa okazał się być obywatelem innego państwa niż to, w którym został zatrzymany, należy dokonać wobec niego ekstradycji. Zgodnie z postanowieniami konwencji może to mieć miejsce w sytuacji, gdy istnieje między dwoma państwami umowa ekstradycyjna. Jeśli jednak państwo nie chce wydać sprawcy-obywatela innego państwa, to zobowiązane jest niezwłocznie wszcząć wobec niego postępowanie karne na podstawie własnych przepisów wewnętrznych[7].

Postanowienia o bezpieczeństwie w umowach dwustronnych

Umowy dwustronne o komunikacji lotniczej są zawierane w oparciu o konwencję chicagowską (tzw. system chicagowsko-bilateralny). Przez wiele dziesięcioleci stanowiły one podstawę wykonywania przewozów lotniczych miedzy państwami. Były one bardzo

[7] Zob. szerzej w: G. Zając, *Prawnomiędzynarodowe regulacje dotyczące zwalczania terroryzmu w lotnictwie cywilnym,* [w:] „Stosunki Międzynarodowe", t. 43 nr (1-2) 2011, Wyd. Uniwersytetu Warszawskiego, Warszawa 2011, s. 105-120.

restrykcyjne, ograniczały swobodę dostępu do rynku i uczciwą konkurencję. Dopiero globalne procesy liberalizacyjne w lotnictwie zapoczątkowane w 1978 r. w USA, a potem od 1986 r., w Europie, doprowadziły do modyfikacji tych umów w kierunku bardziej otwartych, umożliwiających rozwój komunikacji lotniczej miedzy państwami. Współcześnie funkcjonują zarówno te pierwsze, jak i te drugie umowy, z przewagą tych ostatnich. Można zauważyć również w Europie, iż umowy dwustronne zostały całkowicie zniesione i zastąpione zasadą otwartego nieba europejskiego. Zgodnie z art. 149 traktatu o funkcjonowaniu Unii Europejskiej (TFUE), istnieje swoboda prowadzenia działalności między państwami członkowskimi, wobec tego dotyczy to także transportu lotniczego i nie może on podlegać jakimkolwiek ograniczeniom w związku z wykonywaniem działalności lotniczej jednego podmiotu z jednego państwa członkowskiego na terenie innego państwa członkowskiego. Wolności zapisane w podstawowych aktach normatywnych Unii Europejskiej, tj. swoboda przedsiębiorczości i zakaz dyskryminacji ze względu na przynależność państwową stanowią najwyższe wartości, na których opiera się funkcjonowanie Unii Europejskiej.

Warto przypomnieć, że w pierwszych dwustronnych umowach o komunikacji lotniczej zawieranych między poszczególnymi państwami począwszy od lat 20. ubiegłego wieku przez długie lata nie było zwyczaju wpisywania klauzul bezpieczeństwa w te umowy. Dopiero od przełomu lat 80. i 90. XX wieku dwustronne umowy uległy rozszerzeniu o artykuły dotyczące bezpieczeństwa lotniczego[8]. Stało się tak w wyniku przyjęcia stosownych konwencji traktujących o bezpieczeństwie oraz odpowiedzi na współczesne uwarunkowania w sektorze transportu lotniczego.

Można wyróżnić oddzielnie klauzule dotyczące bezpieczeństwa oraz klauzule dotyczące ochrony lotnictwa przed aktami bezprawnej ingerencji. Analizując ten pierwszy aspekt, postanowienia w umowach dwustronnych generalnie odnoszą się do procedur konsultacji lub „kontroli na ziemi", bądź jednego i drugiego elementu w stosunku do przewoźnika lotniczego. Państwa zastrzegają sobie możliwość zażądania w dowolnym czasie konsultacji w sprawie standardów bezpieczeństwa przestrzeganych przez drugie państwo dotyczących przewoźnika lotniczego wykonującego operacje między danymi państwami, a to odnośnie załóg, statków powietrznych oraz ich eksploatacji. W przypadku umów unijnych (horyzontalnych), zawierają one odniesienia do unijnych aktów prawnych w dziedzinie bezpieczeństwa lotniczego jakie musi spełnić przewoźnik z państwa trzeciego chcący wykonywać operacje na obszarze UE. Jeżeli po takich konsultacjach jedno państwo stwierdzi, że drugie w sposób nie wystarczający kontroluje spełnianie wymogów przez zarejestrowanego u siebie przewoźnika, to zostanie ono powiadomione o konieczności podjęcia niezbędnych działań dla zapewnienia tych minimalnych standardów, oraz

[8] G. Zając, *Dwustronne umowy o komunikacji lotniczej zawierane przez Polskę*, w: „Przegląd Sił Powietrznych", nr 4/06, Wyd. Dowództwo Sił Powietrznych RP, Poznań 2006, s.84-94.

zostanie zastosowany zakaz poruszania się w przestrzeni powietrznej Europy do czasu spełnienia wszystkich wygów europejskich.

W dwustronnych umowach pojawić się mogą także postanowienia o tzw. kontrolach na ziemi (*ramp inspections*) statków powietrznych zarejestrowanych w państwach trzecich. Każdy statek powietrzny eksploatowany przez przewoźnika lub przewoźników lotniczych jednej Strony może być poddany podczas pobytu na terytorium drugiej Strony inspekcji. Zgodnie z zasadą wzajemności, takie inspekcje mogą być również przeprowadzane w państwach trzecich w stosunku do przewoźników unijnych. Kontrole będą przeprowadzane przez upoważnione osoby na pokładzie samolotu i w jego otoczeniu, pod względem ważności dokumentacji statku powietrznego i jego załogi, a także widocznego stanu statku powietrznego i jego wyposażenia.

Jeśli w trakcie takiej kontroli na ziemi, lub ich serii powstaną:

a) poważne zastrzeżenia, czy dany statek powietrzny lub jego eksploatacja spełniają minimalne standardy ustanowione w tym czasie na podstawie konwencji chicagowskiej, lub
b) poważne zastrzeżenia odnośnie braku efektywnego stosowania lub przestrzegania minimalnych standardów ustanowionych na podstawie tej konwencji,

to Strona dokonująca inspekcji może stwierdzić, że wymagania, zgodnie z którymi eksploatowany jest statek powietrzny lub licencje w odniesieniu do niego, nie spełniają minimalnych standardów bezpieczeństwa ustalonych na podstawie w/w konwencji. W takiej sytuacji istnieje możliwość zakazu przelotu danym statkiem nad obszarem UE, lub możliwość rozciągnięcia zakazu na wszystkie statki powietrzne danego przewoźnika lotniczego.

W przypadku, gdyby przewoźnik odmówił dostępu do przeprowadzenia tzw. kontroli na ziemi w stosunku do statku powietrznego przez niego użytkowanego, to państwo chcące przeprowadzić taką inspekcję może bezzwłocznie zawiesić lub zmienić zezwolenie eksploatacyjne wydane temu przewoźnikowi. W umowach dwustronnych są również zapisy o tym, że gdy kompetentna władza lotnicza podejmie działania odnośnie nieprzestrzegania minimalnych standardów przez przewoźnika drugiej Strony, to natychmiast poinformuje o tym pozostałe władze lotnicze, podając przyczyny podjęcia takiego działania. Istnieje również możliwość wniesienia sprawy do Wspólnego Komitetu ustanowionego na podstawie takiej umowy.

Jeśli chodzi o zapisy dotyczące ochrony lotnictwa w umowach dwustronnych, to zawierają one odniesienia do odpowiednich konwencji w tym obszarze. Strony potwierdzają wzajemne zobowiązania dotyczące ochrony lotnictwa przed czynami bezprawnej ingerencji. W tym celu będą postępować zgodnie z konwencją chicagowską z 1944 r., konwencją tokijską z 1963 r., konwencją haską z 1970 r. oraz konwencją montrealską z 1971 r. Niekiedy dodaje się także odniesienie do protokołu montrealskiego z 1988 r. dotyczącego ochrony lotnictwa w portach lotniczych. Natomiast w dwustronnych

umowach horyzontalnych znajdują się odniesienia do aktów unijnych odnośnie zasad prawa wobec przewoźników i portów lotniczych dotyczących ochrony lotnictwa. Zwykle jeden załączników do takiej umowy enumeratywnie wymienia przyjęte ustawodawstwo unijne w tym zakresie.

Poza tym, w umowach zawieranych przez państwa członkowskie znajdują się odniesienia do postępowania zgodnie ze standardami i rekomendowanymi praktykami dotyczącymi ochrony lotnictwa ustalonymi przez ICAO i załączniki do konwencji chicagowskiej. W razie wystąpienia szczególnego zagrożenia, Strony umowy pozytywnie będą rozpatrywać prośby o zastosowanie specjalnych środków ochrony. Ponadto Strony wzajemnie zgadzają się przestrzegać przepisów wewnętrznych o ochronie.

Jednym z postanowień jest ustalenie, że Strony będą udzielały sobie nawzajem wszelkiej niezbędne pomocy w zapobieganiu czynom bezprawnego zawładnięcia cywilnymi statkami powietrznymi i innym bezprawnym czynom skierowanym przeciwko bezpieczeństwu takich samolotów, ich pasażerów i załóg, portów lotniczych i urządzeń nawigacyjnych, a także innym zagrożeniom bezpieczeństwa lotnictwa cywilnego. Przepis ten jest identyczny w dwóch różnych typach umów.

W przypadku zaistnienia lub groźby zaistnienia aktu bezprawnego zawładnięcia cywilnego statku powietrznego albo innych bezprawnych czynów skierowanych przeciwko bezpieczeństwu takiego statku, jego pasażerów i załogi, portów lotniczych lub urządzeń nawigacyjnych, Strony będą udzielały sobie nawzajem pomocy przez ułatwienie łączności oraz inne odpowiednie środki mające na celu szybkie i bezpieczne zakończenie takiego zdarzenia lub groźby jego zaistnienia.

Prawne procedury i zasady postepowania w badaniu wypadków lotniczych

Polityka państwa musi gwarantować każdemu użytkownikowi przestrzeni powietrznej i związanemu z branżą lotniczą, że dołoży wszelkich starań, by z punktu widzenia prawnego wszystkie standardy wykonywania usług lotniczych były bezpieczne. Państwo musi stworzyć mechanizmy kontroli i egzekucji braku poszanowania przyjętych rozwiązań prawnych. Muszą one być jednak jednolite w stosunku do różnych podmiotów (przewoźników lotniczych, pasażerów będących obywatelami różnych państw) z uwagi na międzynarodowy charakter lotnictwa cywilnego. Dlatego w tym celu ICAO przyjęła stosowne przepisy, by w przypadku wypadków oraz incydentów lotniczych każde państwo postępowało według jednolitych, zharmonizowanych zasad.

Bardzo ważne jest, że w międzynarodowym prawie lotniczym zostały ściśle uregulowane kwestie „wypadku lotniczego" oraz „incydentu lotniczego", a to w załączniku nr 13 do konwencji chicagowskiej. Każde państwo na świecie ma obowiązek stosować przyjęte i wdrożone procedury wynikające z tego załącznika.

Termin „wypadek lotniczy" oznacza *zdarzenie związane z użytkowaniem statku powietrznego, mające miejsce od chwili, gdy jakakolwiek osoba wchodzi na jego pokład z zamiarem wykonania lotu, do chwili, kiedy wszystkie znajdujące się na pokładzie osoby opuszczają statek powietrzny*. Jednakże zastrzeżono równocześnie, że musi to mieć związek z jedną z następujących przyczyn:

a) osoba doznała obrażeń ciała ze skutkiem śmiertelnym lub poważnego obrażenia ciała, gdyż:
   –znajdowała się na pokładzie danego statku powietrznego, lub
   – zetknęła się bezpośrednio z jakąkolwiek częścią statku powietrznego, włączając części, które oddzieliły się od danego statku powietrznego, lub
   – znajdowała się w bezpośrednim oddziaływaniu strumienia gazów wylotowych silnika odrzutowego *z wyłączeniem* tych przypadków, kiedy obrażenia ciała powstały z przyczyn naturalnych, zadanych samemu sobie lub przez inne osoby, kiedy obrażeń ciała doznali pasażerowie nie posiadający biletów, ukrywający się w miejscach, do których zwykle dostęp jest zamknięty dla pasażerów i członków załogi,
b) statek powietrzny został uszkodzony lub nastąpiło zniszczenie jego konstrukcji, w rezultacie czego:
   – naruszona została trwałość konstrukcji, pogorszeniu uległy techniczne lub aerodynamiczne charakterystyki statku powietrznego, oraz
   – wymagane jest przeprowadzenie poważnego remontu lub wymiana uszkodzonego elementu z wyłączeniem przypadków przerwy w pracy lub uszkodzenia silnika, gdy uszkodzeniu uległ tylko silnik, jego osłony lub agregaty wspomagające; lub gdy uszkodzone zostały łopaty śmigła, końcówki skrzydła, anteny, ogumienie kół, urządzenia hamowania, owiewki lub, gdy pokrycie posiada niewielkie wgniecenia albo przebicia,
c) statek powietrzny przepadł bez wieści lub znajduje się w takim miejscu, do którego dostęp jest absolutnie niemożliwy

„Incydentem", natomiast, określono każde zdarzenie, które nie doprowadziło do wypadku, ani nim nie jest, a które wpływa lub może mieć wpływ na bezpieczeństwo operacji statku powietrznego. Wyróżnić można jeszcze pośrednią kategorię, a mianowicie „poważne incydenty". Oznaczają one incydenty, których okoliczności wystąpienia wskazują na to, iż nieomal doszło do wypadku.

Incydenty zdarzają się częściej niż wypadki. Zastosowanie właściwych środków ochrony wymaga współpracy wielu instytucji, które muszą koordynować swoje decyzje i podejmowane działania. Dzięki nowoczesnym technologiom możliwy jest stały kontakt dowódcy statku powietrznego (pilotów) z innymi właściwymi organami ochrony na ziemi. Zapobieganie incydentom wymaga szybkiego wskazania i analizy sytuacji. Po pierwsze konieczna jest umiejętność identyfikacji podejrzanego zachowania. W tym celu personel

lotniczy jest odpowiednio szkolony. Po drugie, należy opisać sytuację na statku powietrznym. Chodzi o wskazanie, co się dzieje na pokładzie, oraz wykonywanie poleceń dowódcy statku powietrznego jako najważniejszej osoby. Po trzecie, należy oszacować ryzyko zagrożenia oraz jakie będzie miało konsekwencje dla innych. Wszystkich incydentów nie da się uniknąć. Jeśli zawiodą czynniki osobowe, techniczne, może dojść do wypadku.

Głównym i jedynym celem badania wypadków lotniczych i incydentów jest zapobieganie wystąpienia podobnym sytuacjom w przyszłości. Badanie prowadzi państwo, na terenie którego miał miejsce wypadek. Państwo prowadzące badania musi je prowadzić zgodnie z międzynarodowymi standardami określonymi w złączniku nr 13 do konwencji chicagowskiej. Jeśli chodzi o uczestnictwo innych państw w procesie badania wypadku, to mogą one wyznaczyć akredytowanego przedstawiciela wraz z towarzyszącymi mu doradcami. Badanie musi być zakończone sporządzeniem raportu końcowego. Wcześniej państwo prowadzące badanie jest zobowiązane do przedstawienia raportu wstępnego, do którego uwagi może wnieść państwo, które otrzyma później raport końcowy. Raport końcowy musi być wysłany przez państwo prowadzące badanie do następujących adresatów: państwo zlecające badanie, państwo rejestracji, państwo operatora, państwo konstruktora, państwo producenta, państwo wyrażające zainteresowanie w związku z ofiarami śmiertelnymi, oraz państwo przekazujące informacje, zasadnicze oprzyrządowanie lub delegujące ekspertów.

Terminologia zaproponowana w międzynarodowych regulacjach odnośnie incydentów i wypadków została transponowana do porządków krajowych poszczególnych państw. Niektóre porozumienia regionalne również przejęły do wewnętrznego zastosowania podobne rozwiązania np. Unia Europejska. Należy zatem zauważyć, że została dokonana harmonizacja przepisów dotyczących badania wypadków lotniczych, gdyż ma to fundamentalny wpływ na bezpieczeństwo całego środowiska lotniczego. Dzięki temu nie ma ryzyka, iż państwo błędnie zinterpretuje określone zdarzenie i w konsekwencji wyciągnie błędne wnioski. Zapobiega temu także wypracowana ujednolicona procedura związana z dochodzeniem i badaniem przyczyn i okoliczności zdarzenia.

Prawo UE w obszarze lotnictwa cywilnego obejmuje również aspekt badania wypadków lotniczych, choć jest on niemal identyczny i wzorowany na międzynarodowych regulacjach. Aktualnie w Unii Europejskiej obowiązują regulacje z 2010 r. (rozporządzenie nr 996/2010 z dnia 20 października 2010 r.)[9]. Pierwszą regulacją w tym zakresie na obszarze Unii Europejskiej była dyrektywa nr 80/1266/EC w 1980 r. w sprawie współpracy i wzajemnej pomocy między państwami członkowskimi w dziedzinie badania wypadków lotniczych[10]. Kolejną była dyrektywa nr 94/56 z dnia 21 listopada 1994 r.

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 996/2010 z dnia 20 października 2010 r. w sprawie badania wypadków i incydentów w lotnictwie cywilnym oraz zapobiegania im oraz uchylające dyrektywę 94/56/WE, (Dz.U. UE, L 295, 12.11.2010, s.36-50).

[10] Dz.U. WE, L 375 z 31 grudnia 1980 r., s. 32.

ustanawiająca podstawowe zasady regulujące postępowanie w dochodzeniu przyczyn wypadków i zdarzeń w lotnictwie cywilnym[11]. Obecnie obowiązujące przepisy nawiązują do dyrektywy z 1994 r.

Szeroko zdefiniowane zostało pojęcie „wypadku" z odniesieniem również do wypadku bezzałogowego statku (drona). Ta stosunkowo nowa w prawie lotniczym kategoria dotyczy bezzałogowych statków powietrznych[12]. Jest przedmiotem aktualnych analiz i regulacji prawnych, to uznaje się, że konieczne jest uregulowanie kwestii wypadków z udziałem tych maszyn. Zgodnie z art. 2 ust. 1 rozporządzenia UE 996/2010 wypadek to *zdarzenie związane z eksploatacją statku powietrznego,* w przypadku załogowego statku powietrznego odbywa się od momentu wejścia na pokład statku powietrznego jakiejkolwiek osoby z zamiarem odbycia lotu aż do opuszczenia pokładu przez te osoby, lub, w przypadku bezzałogowego statku powietrznego, odbywa się od momentu, gdy statek powietrzny jest gotowy do ruchu w celu wykonania lotu aż do czasu jego zatrzymania na koniec lotu i wyłączenia układu napędowego, w którym:

a) osoba znajdująca się na pokładzie statku powietrznego poniosła śmierć lub odniosła poważne obrażenia w następstwie:
   – przebywania na pokładzie statku powietrznego, lub
   – bezpośredniego kontaktu z jakąkolwiek częścią statku powietrznego, włączając części, które zostały od statku powietrznego odłączone, lub
   – bezpośredniego działania podmuchu silnika statku powietrznego,
   – z wyjątkiem przypadków, kiedy obrażenia są skutkiem przyczyn naturalnych, samookaleczenia lub zostały zadane przez inne osoby, lub kiedy osoba doznała obrażeń, ukrywając się poza obszarami zwykle dostępnymi dla pasażerów lub członków załogi; lub
b) statek powietrzny doznaje uszkodzenia lub doszło do zniszczenia jego elementu konstrukcyjnego w stopniu zagrażającym jego wytrzymałości konstrukcyjnej, osiągom lub właściwościom sterowniczym i w normalnych okolicznościach niezbędna byłaby poważna naprawa lub wymiana uszkodzonego elementu, z wyjątkiem niesprawności lub uszkodzeń silnika, w przypadku kiedy uszkodzenie ogranicza się do samego silnika (w tym jego osłon lub akcesoriów), śmigieł, końcówek skrzydeł, anten, sond, łopatek, opon, hamulców, kół, owiewek, paneli, klap podwozia, wycieraczek, poszycia statku powietrznego (takich jak małych wgnieceń lub dziur) lub niewielkich uszkodzeń łopat wirnika nośnego, łopat wirnika ogonowego, podwozia oraz tych spowodowanych przez grad lub zderzenie z ptakiem (w tym dziur w osłonie anteny radiolokatora); lub
c) statek powietrzny zaginął lub dostęp do niego jest całkowicie uniemożliwiony.

[11] Dz.U. WE, L 319 z 12 grudnia 1994 r., s. 14.

[12] Szerzej o terminologii bezzałogowych statków powietrznych w: R. Ivančík, P. Nečas, *Theoretical and Terminological View of Unmanned Aircraft*, INCAS BULLETIN, Volume 14, Issue 3/ 2022, s.147-156.

Nowe przepisy precyzują wzajemne prawa i obowiązki UE, Komisji Europejskiej oraz EASA. Zgodnie z art.15 rozporządzenia wzmocniono prawa ofiar wypadków lotniczych i ich rodzin, a w stosunku do osób uczestniczących w wypadku zapewniona została większa anonimowość. Wzmocniono również europejską organizację EASA poprzez zagwarantowanie udziału jej przedstawiciela w badaniu zdarzeń lotniczych, zgodnie z art.8 rozporządzenia 996/2010. Uznano bowiem, że EASA posiada podobne uprawnienia jak państwo, gdyż realizuje w imieniu swoich państw członkowskich funkcje i zadania państwa konstruktora, państwa producenta oraz państwa rejestracji w związku z zatwierdzaniem projektu. EASA od momentu powołania jej w 2002 r. przyczyniła się do zwiększenia poziomu bezpieczeństwa lotów jako inicjator wielu projektów aktów normatywnych w tym obszarze.

Uzupełnieniem powyższych regulacji jest rozporządzenie nr 376/2014 z dnia 3 kwietnia 2014 r. w sprawie zgłaszania i analizy zdarzeń w lotnictwie cywilnym dotycząca zgłaszania wszelkich zdarzeń w lotnictwie cywilnym[13]. Głównym celem jej jest wymiana informacji i wprowadzenie procedury dobrowolnego i obowiązkowego zgłaszania zdarzeń w lotnictwie cywilnym, które narażają lub mogłyby narazić na niebezpieczeństwo statek powietrzny, znajdujące się w nim osoby, lub osoby trzecie, sprzęt lub urządzenia, dotyczące eksploatacji statku powietrznego, czy wszelkich innych informacji związanych z szeroko rozumianym bezpieczeństwem lotniczym.

Reżim instytucjonalno-prawny w zakresie badania wypadków lotniczych na terenie Unii Europejskiej ustanowiony w oparciu o rozporządzenie 996/2010 oraz rozporządzenie nr 376/2014 znacznie przyczynił się do ograniczenia ryzyka występowania wypadków oraz spowodował daleko idące zmiany w kompleksowym podejściu do bezpieczeństwa lotnictwa cywilnego. Przewozy pasażerskie są bardzo bezpieczne, co widać ze statystyk, że na ponad 30 milionów lotów tylko kilka rocznie zdarza się wypadków śmiertelnych w Europie w ostatnim czasie. W ogólnej liczbie wypadków śmiertelnych na świecie dostrzec należy tendencję spadkową wypadków w przewozach pasażerskich.

Nowa regulacja jest kompatybilna w stosunku do międzynarodowych postanowień zawartych w załączniku nr 13 do konwencji chicagowskiej. Przyjęcie nowego rozporządzenia w miejsce dotychczasowej dyrektywy było podyktowane również tym, że pojawiły się nowe bezzałogowe statki powietrzne, które również powodowały wypadki. W związku z rozwojem zaawansowanych systemów technologicznych konieczna stała się nowa regulacja obejmująca dotąd nieregulowane dziedziny, jak bezzałogowe statki powietrzne. Deklaracja ryska z 2015 r. stanowi solidne potwierdzenie przez państwa ją

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 376/2014 z dnia 3 kwietnia 2014 r. w sprawie zgłaszania i analizy zdarzeń w lotnictwie cywilnym oraz podejmowanych w związku z nimi działań następczych, zmiany rozporzą-dzenia Parlamentu Europejskiego i Rady (UE) nr 996/2010 oraz uchylenia dyrektywy 2003/42/WE Parlamentu Europej-skiego i Rady i rozporządzeń Komisji (WE) nr 1321/2007 i (WE) nr 1330/2007, Dz.U. UE, L 122, 24.4.2014, p. 18-43. Przed wprowadzeniem przedmiotowego rozporządzenia funkcjonowała dyrektywa 2003/42/WE z 2003 r. w tym samym przedmiocie, która znacząco przyczyniła się do wzrostu bezpieczeństwa lotnictwa w Europe i zmniejszenia liczby wypadków, co zaowocowało przyjęciem kompleksowych rozwiązań w postaci omówionego wyżej rozporządzenia w 2014 r.

podpisujące, że należy wdrożyć ramy prawne i zapewnić bezpieczne funkcjonowanie bezzałogowych statków powietrznych w Europie[14]. Coraz bardziej zaawansowane technologicznie bezzałogowe statki powietrzne oraz ich systemy wymagają bardziej wszechstronnej wiedzy oraz zasobów, niż miało to miejsce jeszcze na przełomie tysiącleci, w zakresie badania wypadków lotniczych. Dotychczas nie wypracowano jeszcze jednych wspólnych europejskich regulacji w tej kwestii, a obecne jedynie krajowe rozwiązania w niektórych państwach próbują wychodzić naprzeciw oczekiwaniom użytkowników.

Badanie wypadków lotniczych służy zapobieganiu w przyszłości podobnym sytuacjom. Ustalenie przyczyn i okoliczności takiego wypadku oraz wskazanie odpowiednich rozwiązań przyczynia się do opracowania lepszych metod i standardów szkolenia, a także udoskonalenia stanu technicznego statków powietrznych i urządzeń lotniczych. Uwzględniając również fakt, iż lotnictwo nie ma wymiaru wyłącznie lokalnego, czy krajowego, a funkcjonuje w płaszczyźnie międzynarodowej, to badanie wypadków lotniczych musi charakteryzować się ujednoliconymi normami. Harmonizacja przepisów i spójna wykładnia procedur w skali globalnej pozwala szybko wprowadzać zalecane rozwiązania i uniknąć występowania mnogości przepisów obniżających poziom bezpieczeństwa lotów. Lotnictwo międzynarodowe jest tą dziedziną, która wymaga współpracy i wymiany doświadczeń.

Bezpieczeństwo przewozów pasażerów

Zapewnienie bezpieczeństwa społeczeństwu należy do podstawowych obowiązków państwa Odpowiednie jego organy zajmują się określonymi kategoriami bezpieczeństwa. Takie instytucjonalne ujęcie roli bezpieczeństwa państwa pozwala na stwierdzenie, że za bezpieczeństwo w ruchu lotniczym swoich pasażerów odpowiada nie tylko przewoźnik lotniczy, czy port lotniczy, lecz nade wszystko państwo poprzez swoje organy. Pasażer czuje się bezpiecznie w ruchu lotniczym nie tylko dlatego, że zapewnia mu to umowa z przewoźnikiem, wysokie poczucie bezpieczeństwa, czy jakość usług. Państwo prowadząc swoją politykę bezpieczeństwa lotniczego gwarantuje wszystkim pasażerom, że korzystanie z ruchu lotniczego jest w pełni bezpieczne. W tym celu państwo spełnia rolę nie tylko regulacyjną, którą wykonują określone podmioty, lecz folę kontrolną (nadzorującą), polegającą na kontroli przestrzegania wszelkich procedur bezpieczeństwa podróżnych.

Punktem wyjścia zapewnienia pasażerom bezpieczeństwa w ruchu lotniczym jest zasada ogólnego bezpieczeństwa w lotnictwie określona w art. 3 ust. d, oraz art. 44 konwencji chicagowskiej. Państwo nadzoruje przestrzeganie bezpieczeństwa przez wszystkie podmioty związane z działalnością lotniczą.

[14] Deklaracja ryska w sprawie zdalnie sterowanych statków powietrznych (dronów): „Wyznaczając przyszłość lotnictwa", Ryga, 6.03.2015.

Wszystkie kategorie pasażerów (rozpoczynający lot, transferowi, tranzytowi) są co do zasady poddawani kontroli bezpieczeństwa na lotnisku w celu uniemożliwienia im wniesienia do stref zastrzeżonych lotniska oraz na pokład statku powietrznego przedmiotów zabronionych. W Europie pasażerowie transferowi i tranzytowi mogą być zwolnieni z procedur kontroli bezpieczeństwa, jeśli dotyczy to lotu w ramach Unii Europejskiej (szerzej też Europejskiego Obszaru Gospodarczego i Szwajcarii) przylatują z jednego z państw członkowskich, lub jeśli przylatują z państwa trzeciego, w którym procedury bezpieczeństwa są zgodne z procedurami europejskimi. Ponadto, pasażerowie tranzytowi mogą być zwolnieni z kontroli bezpieczeństwa również w sytuacji, gdy pozostają na pokładzie statku powietrznego lub nie mają kontaktu z pasażerami odlatującymi, z wyjątkiem tych, którzy odlatują tym samym statkiem powietrznym. Podobnie jest w stosunku do bagażu wyżej wymienionych pasażerów.

Pasażerowie korzystają z ochrony w wielu płaszczyznach działalności lotniczej. Ich bezpieczeństwo opiera się o takie zasady jak: informacja o przewoźniku wykonującym faktycznie lot, procedury związane z bagażem, bezpieczeństwo w sytuacji odwołania lotu, czy opóźnienia, lub odmowy wejścia na pokład, i wiele innych. Nie ma jednolitych międzynarodowych standardów ochrony pasażerów, lecz w przypadku europejskiej polityki lotniczej ustanowiono szereg rozwiązań korzystnych dla pasażera, których celem jest zapewnienie bezpieczeństwa podróży każdemu użytkownikowi.

Dotychczasowy rozwój międzynarodowego prawa lotniczego w ramach systemu chicagowskiego nie uwzględniał kwestii ochrony praw pasażerów lotniczych. W konwencji montrealskiej z 1999 r. określone zostały zasady odpowiedzialności przewoźnika za szkodę wynikłą w razie śmierci lub uszkodzenia ciała pasażera, uszkodzenie bagażu lub ładunku oraz granice odszkodowania[15]. Pasażer ma gwarancję od państwa, że poruszanie się w przestrzeni powietrznej jest bezpieczne. Natomiast bezpieczeństwo związane jakością podróży, tj. kwestia bagażu, czy praw w zakresie odwołania, opóźnienia lotu, czy odmowy wejścia na pokład, pozostają w sferze regulacji oddolnych.

W Europie można powiedzieć, że ten stan jest całkowicie uregulowany, i państwa oraz organy UE mają instrumenty realizacji polityki ochrony praw pasażerów lotniczych i dbania o ich bezpieczeństwo w tych aspektach. Pasażerowie w Europie, ale również na całym świecie, mają możliwość korzystania z nowego instrumentu bezpieczeństwa w lotnictwie cywilnym jakim jest tzw. „czarna lista" przewoźników. Jest to unijny wykaz rozporządzenia nr 2111/2005 wszystkich przewoźników lotniczych na świecie spoza Europy, którzy nie spełniają międzynarodowych i europejskich norm bezpieczeństwa oraz/lub określonych statków powietrznych poszczególnych przewoźników, które budzą

[15] Konwencja o ujednoliceniu niektórych zasad dotyczących międzynarodowego przewozu lotniczego (Konwencja montrealska) z dnia 28.05.1999 r. sporządzona w Montrealu, Dz.U. WE, L 194, 18.7.2001.

duże zastrzeżenia co do ich stanu technicznego[16]. Każdy może sprawdzić, czy przewoźnik nie jest wpisany na taką listę. Wpisanie na nią świadczy o braku spełnianiu minimalnych wymogów bezpieczeństwa według europejskich norm. To ważna informacja dla wszystkich pasażerów na świecie, gdyż znajdują się na niej przewoźnicy z różnych państw, a to ułatwi pasażerom w tych państwach na identyfikację potencjalnie niebezpiecznych maszyn i przewoźników. „Czarna lista" jest dla bezpieczeństwa pasażerów swoistym przewodnikiem. Dzięki niej osoba, która jeszcze nie rozpoczęła podróży samolotem będzie poinformowana o bezpieczeństwie danego przewoźnika. „Czarna lista" jest także przestrogą dla tych, którzy wybierają się w podróż samolotem po państwach trzecich, aby mieli na uwadze brak spełnienia wysokich standardów bezpieczeństwa określonego przewoźnika i jego maszyn. Swobodnie zaś można korzystać z transportu lotniczego wykonywanego w obrębie UE, bowiem przewoźnicy nie gwarantujący bezpieczeństwa lotu są pozbawieni możliwości wkraczania w unijną przestrzeń powietrzną[17].

Podsumowanie

W wyniku przedstawionych analiz cel pracy, jakim była analiza międzynarodowego prawa lotniczego w zakresie bezpieczeństwa wykonywania przewozów lotniczych i ochrony przed aktami bezprawnej ingerencji, został zrealizowany. Zweryfikowana i potwierdzona została także hipoteza badawcza, że o bezpieczeństwie przewozów lotniczych świadczą srogie przepisy prawne w różnych płaszczyznach wykonywania przewozów lotniczych i stopień ich przestrzegania przez poszczególne podmioty. Bezpieczeństwo przewozów lotniczych jest gwarantowane zarówno przez podmioty pozapaństwowe, jakimi są przewoźnicy lotniczy, czy porty lotnicze, a także nade wszystko w wymiarze instytucjonalno-organizacyjnym przez organy państwa, które stale nadzorują i monitorują przestrzeganie określonych procedur, norm i zaleceń.

Bibliografia:

Dyrektywa nr 80/1266/EC w 1980 r. w sprawie współpracy i wzajemnej pomocy między państwami członkowskimi w dziedzinie badania wypadków lotniczych, Dz.U. WE, L 375 z 31 grudnia 1980 r.

Dyrektywa nr 94/56 z dnia 21 listopada 1994 r. ustanawiająca podstawowe zasady regulujące postępowanie w dochodzeniu przyczyn wypadków i zdarzeń w lotnictwie cywilnym, Dz.U. WE, L 319 z 12 grudnia 1994

Ivančík R., Nečas P., *Theoretical and Terminological View of Unmanned Aircraft*, INCAS BULLETIN, Volume 14, Issue 3/ 2022

Konwencja o ujednoliceniu niektórych zasad dotyczących międzynarodowego przewozu lotniczego (Konwencja montrealska) z dnia 28.05.1999 r. sporządzona w Montrealu, Dz.U. WE, L 194, 18.7.2001

Konwencja o zwalczaniu bezprawnego zawładnięcia statkami powietrznymi, podpisana w Hadze w dniu 16 grudnia 1970 r. (konwencja haska)

[16] Rozporządzenie nr 2111/2005 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2005 r. w sprawie ustanowienia unijnego wykazu przewoźników lotniczych podlegających zakazowi wykonywania przewozów w ramach Unii Europejskiej i informowania pasażerów korzystających z transportu lotniczego o tożsamości przewoźnika lotniczego wykonującego przewóz oraz uchylające art. 9 dyrektywy 2004/36/WE, Dz.U. L 344 z 27.12.2005, s. 15-22.

[17] G. Zając, *Funkcjonowanie*…, op.cit., s. 347.

Konwencja w sprawie przestępstw i niektórych innych czynów popełnionych na pokładzie statków powietrznych, podpisana w Tokio w dniu 14 września 1963 r. (konwencja tokijska)

Konwencja w sprawie zwalczania bezprawnych czynów skierowanych przeciwko bezpieczeństwu lotnictwa cywilnego, podpisana w Montrealu w dniu 23 września 1971 r. (konwencja montrealska)

Kukułka J., *Bezpieczeństwo a współpraca obywatelska. Współzależności i sprzeczności interesów*, „Sprawy Międzynarodowe", 1982, nr 7

Rozporządzenie nr 2111/2005 Parlamentu Europejskiego i Rady z dnia 14 grudnia 2005 r. w sprawie ustanowienia unijnego wykazu przewoźników lotniczych podlegających zakazowi wykonywania przewozów w ramach Unii Europejskiej i informowania pasażerów korzystających z transportu lotniczego o tożsamości przewoźnika lotniczego wykonującego przewóz oraz uchylające art. 9 dyrektywy 2004/36/WE, Dz.U. L 344 z 27.12.2005

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 376/2014 z dnia 3 kwietnia 2014 r. w sprawie zgłaszania i analizy zdarzeń w lotnictwie cywilnym oraz podejmowanych w związku z nimi działań następczych, zmiany rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 996/2010 oraz uchylenia dyrektywy 2003/42/WE Parlamentu Europejskiego i Rady i rozporządzeń Komisji (WE) nr 1321/2007 i (WE) nr 1330/2007, Dz.U. UE, L 122, 24.4.2014

Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 996/2010 z dnia 20 października 2010 r. w sprawie badania wypadków i incydentów w lotnictwie cywilnym oraz zapobiegania im oraz uchylające dyrektywę 94/56/WE, (Dz.U. UE, L 295, 12.11.2010

Świerszcz K., *Bezpieczeństwo państwa w czasach współczesnych w ujęciu podmiotowo-aksjologicznych wyzwań*, Przegląd Nauk o Obronności 1/2016

Zając G., *Dwustronne umowy o komunikacji lotniczej zawierane przez Polskę*, w: „Przegląd Sił Powietrznych", nr 4/06, Wyd. Dowództwo Sił Powietrznych RP, Poznań 2006

Zając G., *Prawnomiędzynarodowe regulacje dotyczące zwalczania terroryzmu w lotnictwie cywilnym,* [w:] „Stosunki Międzynarodowe", t. 43 nr (1-2) 2011, Wyd. Uniwersytetu Warszawskiego, Warszawa 2011

Zając G., *Wspólna polityka lotnicza Unii Europejskiej*, Przemyśl 2009

Bogusław Węgliński[1]

Odbudowa ruchu lotniczego z Portu im. Mikołaja Kopernika we Wrocławiu w 2022 r. Od pandemii, przez wojnę na Ukrainie do normalności

Streszczenie

W artykule przedstawiono proces odbudowy poszczególnych segmentów ruchu lotniczego w porcie lotniczym Wrocław SA w roku 2022. Rok ten wydaje się być prognostykiem powrotu wrocławskiego portu na ścieżkę wzrostu, po której kroczył przez pierwsze dwie dekady tego tysiąclecia. Potwierdzają ten proces wyniki innych portów lotniczych w Polsce i Europie.

Słowa kluczowe: ruch lotniczy, port lotniczy Wrocław.

Abstract

The article presents the process of rebuilding individual segments of air traffic at Wrocław SA airport in 2022. This year seems to herald the return of the airport of Wrocław to the growth path it followed for the first two decades of this millennium. This process is confirmed by the results of other airports in Poland and Europe

Keywords: air traffic, airport in Wroclaw.

Wstęp

W artykule poddałem analizie funkcjonowanie portu lotniczego we Wrocławiu w 2022 r. Odniosłem się do powodów drastycznego spadku liczby pasażerów spowodowanego wybuchem pandemii COVID-19 w 2020 r., prześledziłem także próby odbudowy ruchu

[1] Dr Bogusław Węgliński, adiunkt, Dolnośląska Szkoła Wyższa we Wrocławiu, ORCID ID: 0000-0002-6587-8231.

w roku 2021 i bieżącym w najważniejszych jego segmentach. Wydaje się że rok 2022 jest zarówno w porcie we Wrocławiu, jak i innych lotniskach w Polsce i Europie przełomowym rokiem na drodze do powrotu na ścieżkę wzrostu. Obserwując wyniki cząstkowe z polskich lotnisk, wiele z nich już w tej chwili notuje miesięczne wyniki wyższe od tych z roku 2019.

W artykule przeprowadziłem analizę dokumentów dotyczących rozwoju ruchu lotniczego we wrocławskim porcie. Ważnym elementem była także poparta obecnością na briefingach przy okazji zdecydowanej większości opisywanych wydarzeń analiza aktualnych wydarzeń z życia lotniska we Wrocławiu. W przypadku dostosowania nieużywanego terminala lotniskowego do funkcji schronienia dla uchodźców, przeprowadziłem wywiad z osobą odpowiedzialna za realizację tego projektu, a także wykonałem dokumentację fotograficzną w budynku. Ze względu na to, że wątek dotyczący adaptacji „starego" terminala do nowej funkcji był wątkiem pobocznym w artykule, materiały nie zostały użyte.

W artykule postawiłem hipotezę, że port lotniczy we Wrocławiu sprawnie wraca w 2022 r. na ścieżkę szybkiego wzrostu, po której kroczył przez ponad 2 dekady. Postawiłem sobie następujące pytania badawcze:

1. Jak głęboki regres ruchu lotniczego spowodował wybuch pandemii w 2020 r.?
2. Jak wyglądały próby odbudowy ruchu w latach 2020-2021?
3. Jaki wpływ na proces odbudowy ruchu lotniczego w roku 2022 miał wybuch wojny na Ukrainie?
4. Jaką rolę pełnił Port Lotniczy Wrocław SA w czasie największego nasienia napływu uchodźców z Ukrainy?
5. Jakie inwestycje w infrastrukturze lotniczej w porcie planowane są na najbliższe lata?

Rozwinięcie

Rok 2022 ma szansę stać się przełomowym rokiem w procesie odbudowy rynku lotniczych przewozów pasażerskich w Polsce. Ucierpiał on mocno w wyniku pandemii, która wybuchła w początkach roku 2020. Autorzy projektu dokumentu regulującego funkcjonowanie rynku lotnictwa cywilnego w UE zwracają uwagę, że spadek popytu na loty sięgał w kwietniu 2020 roku 89%[2].

Należy zauważyć, że mimo tworzenia wspólnej polityki bezpieczeństwa lotnictwa cywilnego na poziomie Unii Europejskiej,[3] decyzje w sprawie ograniczenia ruchu podejmowane były na poziomie państw członkowskich. To potwierdza wiodącą rolę

[2] Komisja Europejska. Wniosek Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie Rady (EWG) nr 95/93 w odniesieniu do tymczasowego złagodzenia zasad wykorzystywania czasów na start i lądowanie w portach lotniczych Wspólnoty w związku z kryzysem związanym z pandemią COVID-19, Bruksela, dnia 12.07.2022 r. COM(2022) 334 final, s. 2.

[3] B. Węgliński, Zagrożenie terroryzmem we współczesnym świecie a system bezpieczeństwa państwa. Wrocław 2016, s. 237-246.

państw w kreowaniu polityki bezpieczeństwa, także na poziomie lotnictwa cywilnego[4]. Wspominając tamte dni w naszym kraju, destrukcyjny wpływ epidemii koronawirusa na rynek lotniczy w Polsce potwierdziło rozporządzenie Prezesa Rady Ministrów z dnia 13 marca 2020 r. w sprawie zakazów w ruchu lotniczym.[5] W dokumencie tym ogłoszono zakaz lądowania w polskich portach lotniczych samolotów pasażerskich powracających z pasażerami z lotów zagranicznych. Pozostawiono wyjątki dla lotów organizowanych na zlecenie Prezesa Rady Ministrów, otwarto też jednocześnie ścieżkę zwolnienia z opłat lotniskowych dla lotów wykonywanych w celu niesienia pomocy humanitarnej i medycznej.[6]Konsekwencja odwołania lotów międzynarodowych było zawieszenie przez PLL Lot siatki połączeń krajowych.[7] Swoje loty krajowe zawiesił także Ryanair.[8]

PLL Lot rozpoczęły, jako jedyny przewoźnik na terenie Polski loty mające na celu powrót uwięzionych poza granicami polskich obywateli. Transport przylatujących do Warszawy pasażerów wewnątrz kraju wspierało PKP Inter City oraz zapewniający transport autobusowy Polonus.[9] Po kilku tygodniach ich funkcjonowania podsumowano wyniki akcji #LOTdoDomu. Michał Dworczyk, minister- Szef Kancelarii Prezesa Ministrów powiedział: *Operacja #LOTdoDomu powstała z potrzeby pomocy rodakom, których strategiczna i podyktowana bezpieczeństwem publicznym decyzja o zamknięciu granic kraju pozostawiła daleko od domu. Skala tego wyjątkowego projektu była ogromna, praca wielowymiarowa, a do tego technicznie i dyplomatycznie bardzo skomplikowana. Uruchomiona została specjalna podstrona umożliwiająca rejestrację zapotrzebowania na loty, równocześnie rozpoczęło się planowanie pierwszych połączeń i organizacja ich zaplecza. Liczba zgłoszeń rosła lawinowo w każdym dniem sprawiając, że skala projektu przybrała niespotykany dotąd rozmiar. Zrealizowane na zlecenie Kancelarii Prezesa Rady Ministrów 388 operacji lotniczych do 71 destynacji z misją pomocy dla ponad 54 tys. obywateli Polski jest największym repatriacyjnym przedsięwzięciem w historii Polski, od czasu II wojny światowej. Wielkie podziękowania i wyrazy uznania za ciężką pracę należą się wszystkim zaangażowanym instytucjom publicznym oraz wykonawcy – spółce PLL LOT* [10].

Od 1 czerwca 2020 r. uruchomiono w Polsce część połączeń krajowych, jednak ich częstotliwość związana z dalszym brakiem lotów międzynarodowych realizowanych przez PLL LOT była bardzo ograniczona. Terminale dostosowano do nowych wymagań sanitarnych, wprowadzono między innymi odstępy między siedzeniami w sali odlotów, czy kontrolę temperatury przy wejściu do budynku. (fot nr 1).

---

[4] G. Zając, *Contemporary political, legal and economic aspects of aviation safety*. [w:] International Journal of Social Science and Economic Research, vol. 5 issue:9, September 2020, s. 2477.

[5] Rozporządzenie Prezesa Rady Ministrów z dnia 13 marca 2020 r. w sprawie zakazów w ruchu lotniczym. (Dz.U poz. 436/2020).

[6] Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze, Dz.U. poz. 1580/2019, art. 76.1.

[7] https://www.tokfm.pl/Tokfm/7,171710,25790151,lot-wszystkie-polaczenia-zawieszone-od-15-do-28-marca.html [dostęp 10.10.2020].

[8] https://corporate.ryanair.com/news/grupa-ryanair-odwoluje-wszystkie-loty-z-do-z-polski-od-niedzieli-15-marca-do-wtorku-31-marca/?market=pl [dostęp 10.10.2020].

[9] Dybiński R. 20.03.2020, MI: Polonus i PKP Intercity dołączają do akcji #LOTdoDomu; https://www.rynek-lotniczy.pl/mobile/mi-polonus-i-pkp-intercity-dolaczaja-do-akcji-lotdodomu-8145.html [dostęp 10.10.2020].

[10] https://dlapilota.pl/wiadomosci/pll-lot/pll-lot-54-tys-polakow-wrocilo-do-kraju-w-ramach-operacji-lotdodomu [dostęp 10.10.2020].

Fot. 1. Zdjęcie hali odlotów na lotnisku we Wrocławiu z 01.06.2020

Źródło: fotografia ze zbiorów autora

Ograniczenia w innych krajach europejskich wyglądały podobnie[11].

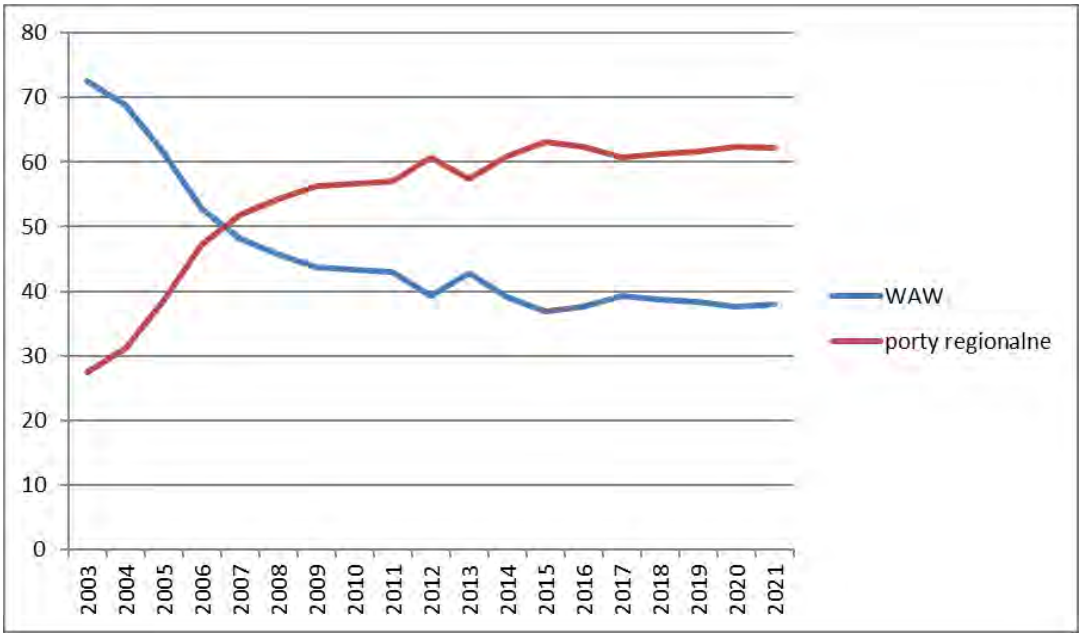
W kolejnych miesiącach ruch lotniczy powoli liberalizowano, a skalę zmian w liczbie pasażerów obsługiwanych w polskich portach lotniczych w latach 2019-2021 ilustruje tabela 1.

Tab. 1. Liczba pasażerów obsługiwanych w polskich portach lotniczych w latach 2019-2021 (w mln)

Lotnisko	2019	2020	2021
WAW	18,84	5,74	7,74
KRK	8.4	2,59	3,07
GDN	5,36	1,7	2,15
KTW	4,84	1,44	2,33
WRO	3,54	1,00	1,42
WMI	3,1	0,87	1,46
POZ	2,37	0,65	1,05
RZE	0,77	0,23	0,26
SZZ	0,58	0,19	Ok. 0,15
LUZ	0,36	0,12	0,11
BZG	0,41	0,12	Ok. 0,12
LCJ	0,24	0,07	0,07
SZY	0,15	0,06	0,05
IEG	0,03	0,02	0,02
Razem	49,01	14,55	19,73

Źródło: Opracowanie własne na podstawie Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2019-2021, ULC, Warszawa, marzec 2022.

[11] G. Zając, *Kryzys lotniczy w związku z Coronavirusem* [w:] Przegląd komunikacyjny 11/2020, s. 13-14



Wykres 1. Procentowy udział MPL im. Chopina i portów regionalnych w liczbie pasażerów obsługiwanych na lotniskach w Polsce w latach 2003-2020

Źródło: opracowanie własne na podstawie: ULC, Analiza rynku transportu lotniczego w Polsce w latach 2004-2006, Warszawa, wrzesień 2008, s. 17; Analiza rynku transportu lotniczego w Polsce w latach 2004-2007, Warszawa 2009, s. 20, Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu regularnym i czarterowym w polskich portach lotniczych w latach 2008-2010, Warszawa 2011; Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2010-2012, Warszawa 2013; Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2014-2016, Warszawa 2017; Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2015-2017, Warszawa 2018, Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2016-2018; Warszawa 2019, Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2017-2019, Warszawa 2021;Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2018-2020, Warszawa 2021.

Pandemia COVID-19 spowodowała nienotowany wcześniej spadek liczby pasażerów korzystających z polskich lotnisk. Wpływ, jaki na wyniki portów w naszym kraju miał globalny kryzys ekonomiczny, który rozpoczął się w końcu 2008 r. i wpływał na sytuację na rynku lotniczy także w roku 2009, był nieporównywalny do katastrofy z roku 2020. Ten z I dekady naszego wieku spowodował spadek rzędu 8%[12], z niecałych 21 mln w 2008 r. do prawie 19 mln w roku kolejnym. Już w roku 2010 liczba pasażerów wróciła nieomal do poziomu z roku 2008[13], aby w kolejnych latach rosnąć aż do roku 2020. Dopiero w tym roku liczba pasażerów spadła do 14,5 mln z rekordowych 49 mln

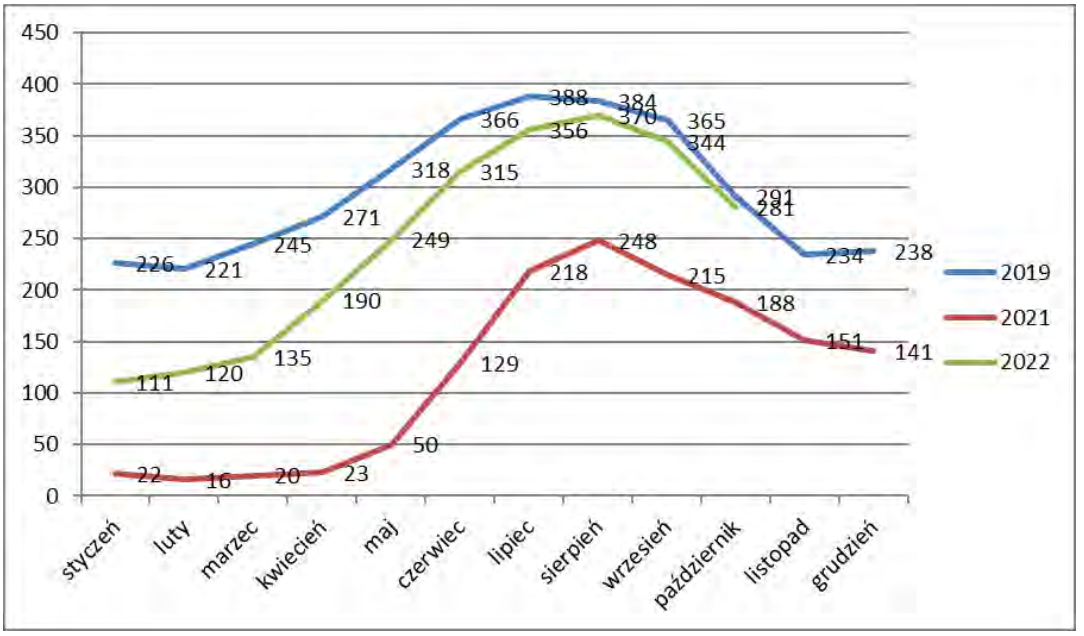
[12] B. Węgliński, *Przewozy krajowe w Polsce. Polskie lotnictwo komunikacyjne w roku 2010*. [w:] P. Mickiewicz, B. Węgliński(red.) *„Otwarte niebo" nad Dolnym Śląskiem*, Wrocław 2011 s.131-132.

[13] ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu regularnym i czarterowym w polskich portach lotniczych w latach 2008-2010, Warszawa 2011.

odnotowanych w roku 2019. Tym razem, mimo powolnej odbudowy siatki i liczby pasażerów, na wyniki porównywalne z potokami pasażerskimi z roku 2019 trzeba było czekać w większości portów do roku 2022.

Mimo tego, że jeszcze w roku 2003 na lotnisku Chopina w Warszawie obsłużono ponad 72% ogółu pasażerów korzystających z portów lotniczych w Polsce, (wykres 1) szybki rozwój portów regionalnych w latach kolejnych zmienił tą proporcje na korzyść tych właśnie. Od kilkunastu lat to porty regionalne wiodą prym w łącznej liczbie odprawionych pasażerów przekraczając 60% tej liczby.

Jednym z portów regionalnych, który idealnie wpisuje się w opisywany proces rozwoju i wzrostu znaczenia regionalnych lotnisk w Polsce jest Port Lotniczy im Mikołaja Kopernika we Wrocławiu. Podobnie, jak w innych portach, proces wzrostu liczby pasażerów został zakłócony w roku 2009, a potem załamał się w roku 2020[14]. Proces odtwarzania ruchu w roku 2021, kiedy ruch ograniczany był przez ograniczenia związane z kolejnymi falami epidemii trudno uznać za doskonały, choć wyniki w miesiącach wakacyjnych świadczyły o oczekiwaniach pasażerów i potrzebie poczucia normalności. (wykres 2).



Wykres 2. Porównanie liczby pasażerów obsłużonych w latach: 2019, 2021 i miesiącach styczeń-październik 2022 na lotnisku we Wrocławiu

Źródło: https://airport.wroclaw.pl/lotnisko/statystyki/ruch-pasazerski/ [dostęp 10.02.2020]; https://airport.wroclaw.pl/lotnisko/statystyki/ruch-pasazerski/ [dostęp 07.11.2022].

[14] https://airport.wroclaw.pl/lotnisko/statystyki/ruch-pasazerski/ [dostęp 10.11.2022].

O znaczącej odbudowie ruchu można powiedzieć dopiero w roku 2022, choć zakłócona została ona przez kolejne zagrożenie, którym była inwazja wojsk rosyjskich na Ukrainę, która zaczęła się 24 lutego. Z dnia na dzień zawieszono wszystkie połączenia łączące Wrocław z kilkoma miastami w tym kraju. Siatka połączeń tworzyła się przez lata i była odpowiedzią na rosnącą liczbę Ukraińców pracujących we Wrocławiu i w regionie. Loty na kijowskie lotnisko w Żulianach rozpoczął listopadzie 2016 roku Wizzair, proponując 2 loty w tygodniu[15]. Od sezonu letniego 2017 ofertę węgierskiego przewoźnika wzbogaciły połączenia do Lwowa[16]. W sezonie letnim 2018 były to już 3 loty w tygodniu do Kijowa, a do Lwowa można było polecieć na pokładzie Airbusów Wizzair 4 razy w tygodniu[17]. Od rozkładu zimowego 2018/2019 swoje 3 loty tygodniowo na kijowskie lotnisko Boryspol ogłosił Ryanair[18]. Siatka połączeń Wrocławia z Ukrainą powoli rosła, a jej zawartość w rozkładzie letnim 2021 i zimowym 2021/2022 pokazują tabele 2 i 3.

Tabela 2 Loty z Wrocławia na Ukrainę w dniach 8-14.08.2021 (Rozkład letni)

dzień	Kierunek/ przewoźnik	Kierunek/ przewoźnik	Kierunek/ przewoźnik	Kierunek/ przewoźnik
Niedziela 08.08.2021				
Poniedziałek 09.08.2021	Kijów Boryspol/ Ryanair	Lwów/ Ryanair	Lwów/ Wizzair	Charków/ Wizzair
Wtorek 10.08.2021	Kijów Żuliany/ Wizzair	Odessa/ Ryanair		
Środa 11.08.2021	Kijów Boryspol/ Ryanair	Lwów/ Ryanair		
Czwartek 12.08.2021	Kijów Żuliany/ Wizzair	Zaporoże/ Wizzair		
Piątek 13.08.2021	Lwów/ Ryanair	Lwów/ Wizzair	Charków/ Wizzair	
Sobota 14.08.2021	Kijów Żuliany/ Wizzair	Odessa/ Ryanair		

Źródło: badanie własne rozkładu lotów w PL Wrocław SA przeprowadzone w dniach 08-14 08.2021.

Jak widać, ofertę Wizzair wzbogaciły połączenia do Charkowa i Zaporoża, a Ryanair latał w tym rozkładzie dodatkowo do Lwowa i Odessy. Ponieważ przed wybuchem wojny mieszkało we Wrocławiu nie mniej niż 100 tys. mieszkańców Ukrainy[19], w rozkładzie zimowym można było polecieć na Ukrainę 16 razy w ciągu tygodnia. Prawdopodobną rozbudowę siatki w rozkładzie letnim przerwał wybuch wojny. Warto odnotować, że siatka połączeń z rozkładu zimowego pozwalała szacować liczbę obsługiwanych na kierunkach

[15] Informacja prasowa PL Wrocław z dnia 19.07.2016.
[16] Informacja prasowa PL Wrocław z dnia 18.01.2017.
[17] B. Węgliński, K. Natalli, *Rozwój regionalnych portów lotniczych w Polsce Wpływ na gospodarkę i bezpieczeństwo społeczne oraz regionalne.* Oficyna Wydawnicza Atut, Wrocław 2019, s. 191-192.
[18] Informacja prasowa PL Wrocław z dnia 23.03.2018.
[19] Szagdaj Nadia (26.07.2022), Ilu Ukraińców mieszka we Wrocławiu? Stanowią oni już niemal 25% wszystkich mieszkańców, https://gazetawroclawska.pl/ilu-ukraincow-mieszka-we-wroclawiu-stanowia-oni-juz-niemal-25-proc-wszystkich-mieszkancow /ar/c1-16526591 [dostęp 10.11.2022].

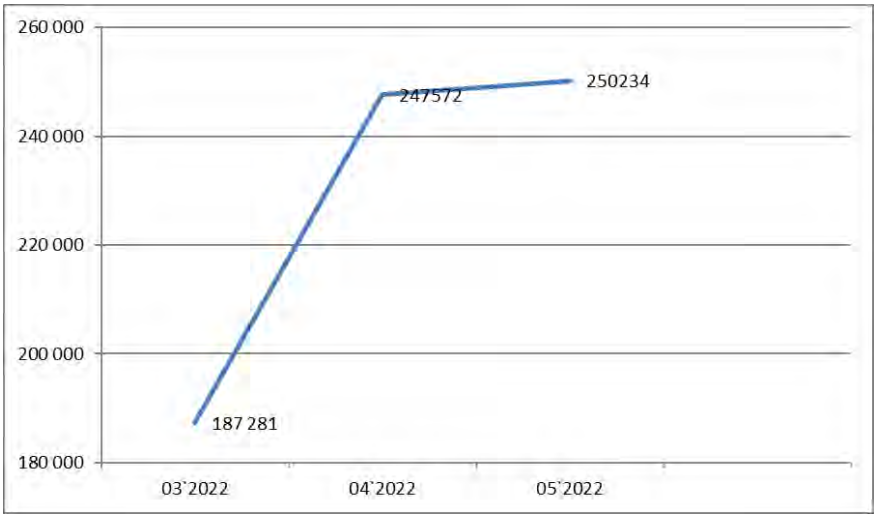
ukraińskich pasażerów na nie mniej niż 5 tys. tygodniowo, czyli ok. 20 tys. miesięcznie. To oczywiście postawiło przewoźników przed koniecznością dokonania szybkich zmian w ofercie po wybuchu wojny. Napiszę o tym w dalszej części tekstu.

Tabela 3. Loty z Wrocławia na Ukrainę w dniach 6-12.02.2022 (rozkład zimowy)

dzień	Kierunek/ przewoźnik	Kierunek/ przewoźnik	Kierunek/ przewoźnik
Niedziela 06.02.2022	Kijów Boryspol/ Ryanair	Charków/ Wizzair	
Poniedziałek 07.02.2022	Kijów Boryspol/ Ryanair	Lwów/ Wizzair	Odessa/ Ryanair
Wtorek 08.02.2022	Kijów Żuliany/ Wizzair	Lwów/ Ryanair	
Środa 09.02.2022	Kijów Boryspol/ Ryanair	Charków/ Wizzair	
Czwartek 10.02.2022	Kijów Żuliany/ Wizzair	Lwów/ Wizzair	
Piątek 11.02.2022	Kijów Boryspol/ Ryanair	Lwów/ Wizzair	Odessa/ Ryanair
Sobota 12.02.2022	Kijów Żuliany/ Wizzair	Lwów/ Ryanair	

Źródło: Badanie własne rozkładu lotów w PL Wrocław SA przeprowadzone w dniach 06-12 02.2022.

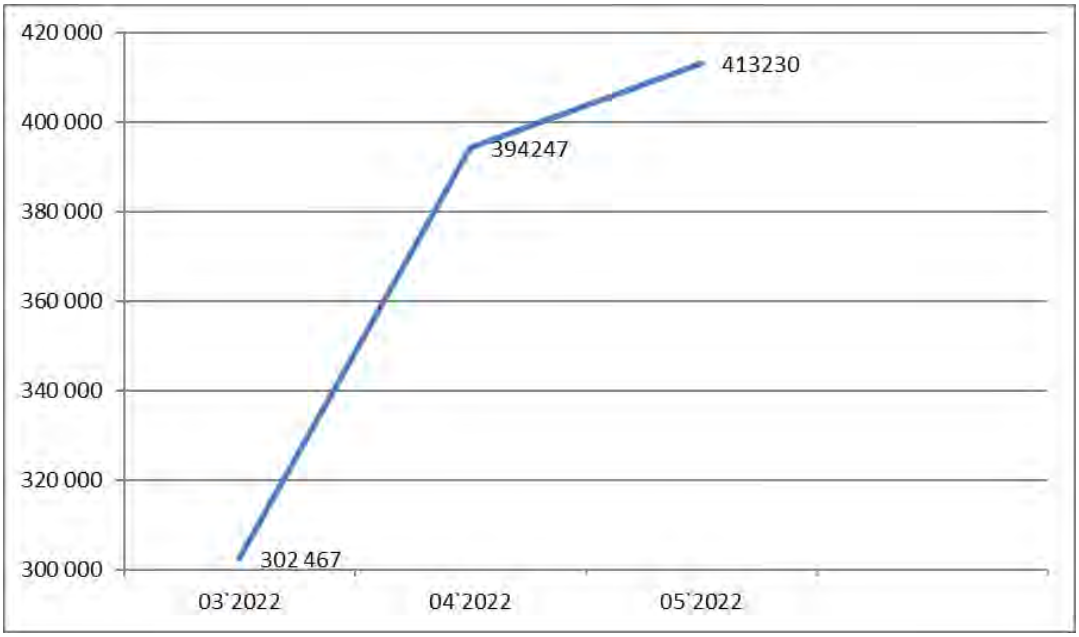
Kolejnym, nico zaskakującym wydarzeniem w działaniach portu lotniczego we Wrocławiu w roku 2022 wydarzeniem był fakt wykorzystania jego infrastruktury na potrzeby uchodźców z Ukrainy. Fala uciekinierów składających się głównie z kobiet z dziećmi i osób starszych zaczęła docierać do Wrocławia na przełomie lutego i marca. Liczbę Ukraińców we Wrocławiu w miesiącach marzec-maj 2022 ilustruje wykres 3.



Wykres 3. Liczba Ukraińców we Wrocławiu w miesiącach marzec-maj 2022.

Źródło: opracowanie własne na podstawie: Miejska gościnność. Szacunek liczby Ukraińców w miastach UMP w miesiącach marzec, kwiecień, maj 2022 r. Aktualizacja raportu Miejska gościnność: wielki wzrost, wyzwania i szanse. Raport o uchodźcach z Ukrainy w największych polskich miastach z kwietnia 2022 r., Unia Metropolii Polskich, Warszawa, lipiec 2022, s. 67.

Pamiętać należy, że liczby z wykresu to zarówno uchodźcy, jak i osoby, które mieszkały we Wrocławiu przed wybuchem wojny. Jeśli dodamy do tego Ukraińców, którzy przebywali na terenie aglomeracji wrocławskiej, którą tworzy Wrocław i otaczające go 41 gmin, wykres wygląda następująco:



Wykres 4. Liczba Ukraińców we Wrocławiu i aglomeracji wrocławskiej w miesiącach marzec-maj 2022

Źródło: opracowanie własne na podstawie: Miejska gościnność. Szacunek liczby Ukraińców w miastach UMP w miesiącach marzec, kwiecień, maj 2022 r. Aktualizacja raportu Miejska gościnność: wielki wzrost, wyzwania i szanse. Raport o uchodźcach z Ukrainy w największych polskich miastach z kwietnia 2022 r. Unia Metropolii Polskich, Warszawa, lipiec 2022, s. 68.

Centralnym miejscem koordynacji pomocy w tym okresie był Dworzec Główny we Wrocławiu. Podsumowując w kwietniu tego roku działania na największym z wrocławskich dworców, wojewoda dolnośląski Jarosław Obremski powiedział: *W szczytowym momencie przyjechało ponad 7200 osób dziennie. To było 7 marca. W tej chwili to między 500 a 700 osób dziennie, czyli mniej niż 10 procent*[20]. Liczbę uchodźców, którzy przewinęli się przez Wrocław Główny przekroczyła 100 tys. osób, a zgodnie ze sobą współpracujące w tej kwestii służby podległe wojewodzie i prezydentowi miasta poszukiwały miejsc, gdzie można było ulokować większe grupy uchodźców. Mimo otwartych serc Polaków i ich ofiarności nie wszystkich uciekinierów udało się ulokować

[20] M. Rajfur, (13.04.2022). Ponad 100 tys. uchodźców przeszło przez Dworzec Główny we Wrocławiu. Najwięcej to 7 tys. dziennie. Gazeta Wrocławska. https://gazetawroclawska.pl/ponad-100-tys-uchodzcow-przeszlo-przez-dworzec-glowny-we-wroclawiu-najwiecej-to-7-tysiecy-dziennie/ar/c1-16277051 [dostęp 10.11.2022]

w domach polskich rodzin. Niektórzy zamieszkać musieli w adaptowanych do tego celu pomieszczeniach. Jednym z miejsc zaproponowanych do przygotowania jako miejsca zakwaterowania dla uchodźców stał się, używany od wiosny 2012 tylko do celów gospodarczych i lotów General Aviation „stary" terminal wrocławskiego portu. Budynek jest oddalony od „nowego" będącego w użyciu o niecałe 2 kilometry. Budynek dostosowano do nowej funkcji w rekordowym czasie ok. 30 godzin[21]. Planowano zakwaterowanie 200 uchodźców, a najpoważniejszym brakiem wyposażenia była niewystarczająca liczba natrysków, których nie przewidziano w pełniącym zupełnie inną funkcję budynku. Braki nadrobiono przez dostawienie przed terminalem kontenera sanitarnego z 6 prysznicami, a po udostępnieniu dostępu i wybiciu nowych otworów drzwiowych uchodźcy mogli skorzystać także z dwóch, istniejących w budynku natrysków, które znajdowały się w używanej wcześniej przez Straż Graniczną części terminala. Pierwsi uchodźcy dotarli do swojego tymczasowego domu 11 marca 2022, a wydarzeniu towarzyszyła konferencja prasowa, w której wzięli udział Wojewoda Dolnośląski, prezydent Wrocławia i prezes Portu Lotniczego Wrocław S.A. (fot. 2).

Fot 2. Konferencja prasowa z udziałem wojewody dolnośląskiego, prezydenta Wrocławia i prezesa portu lotniczego we Wrocławiu (11.03.2022)

Źródło: Zdjęcie z zasobów archiwalnych autora.

Funkcjonowanie terminalu jako miejsca schronienia możliwe było dzięki sprawnej i ofiarnej współpracy wielu służb będących w gestii władz centralnych i samorządowych, a także poświęceniu rzeszy wolontariuszy pomagających w tym okresie. Pracujący przy dostosowaniu i nietypowym sposobie użytkowania terminalu pracownicy portu lotniczego

[21] J. Malinowski, W dobę przygotowali stary terminal lotniska na przyjęcie uchodźców. Jest też miejsce dla ukraińskich samolotów. https://wroclaw.wyborcza.pl/wroclaw/7,35771,28211427,w-dobe-przygotowali-stary-terminal-lotniska-na-przyjecie-uchodzcow.html [dostęp 11.11.2022].

z całą pewnością zdali kolejny trudny egzamin w swoim życiu, tym razem z empatii i poświęcenia.

Jak sygnalizowałem we wcześniejszym fragmencie artykułu, przewoźnicy, którzy nie mogli kontynuować lotów na Ukrainę dosyć szybko podjęli decyzję o spożytkowaniu wolnych rotacji którymi dysponowali. Ryanair już wcześniej sygnalizował otwarcie połączenia na główne lotnisko Sztokholmu – Arlandę[22] oraz do Treviso i Turynu[23]. Wizzair zaproponował od sierpnia loty na El Prat – główne lotnisko Barcelony, do Tirany i na Rodos[24]. Wszystkie nowe kierunki miały być obsługiwane 2 razy w tygodniu. Ofertę węgierskiego przewoźnika uzupełniło również dwukrotne w tygodniu połączenie do Dubrownika[25].

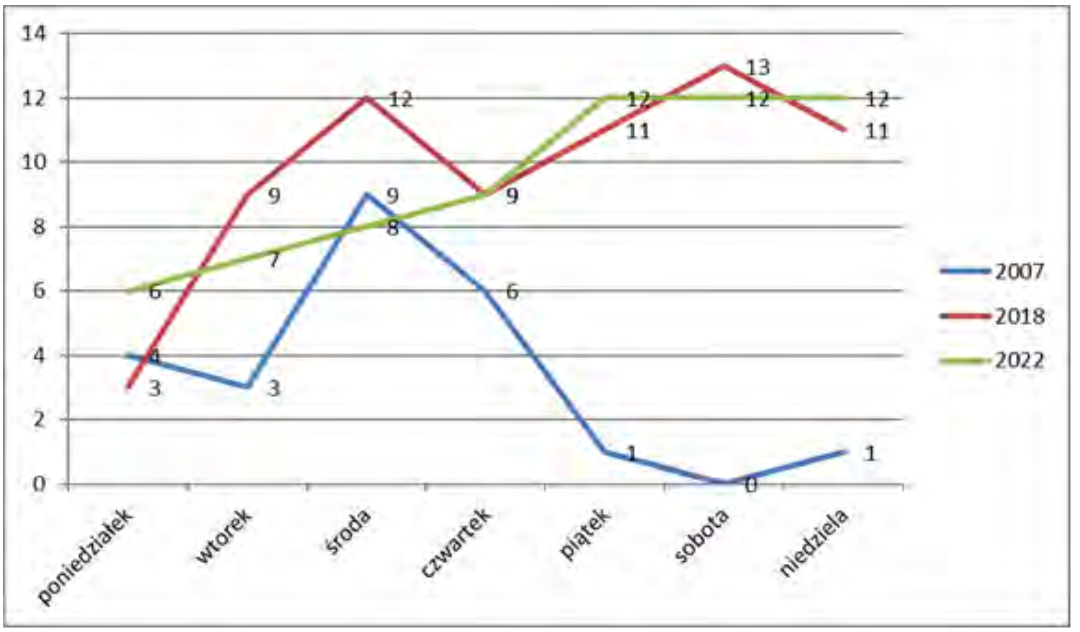
We wrocławskim porcie pojawiły się też samoloty nowego przewoźnika. Loty do Oslo-Gardermoen zaproponował Norwegian, który po dwóch nieudanych próbach w przeszłości w końcu uruchomił to połączenie.

Powoli odbudowywali swoją ofertę także przewoźnicy sieciowi: *w sezonie letnim pasażerowie wrocławskiego lotniska mają do dyspozycji około 95 rejsów tygodniowo do hubów przesiadkowych, w tym do największych w Europie, umożliwiających przesiadkę do samolotów na trasach międzykontynentalnych. Lufthansa oferuje codziennie trzy rejsy do Frankfurtu oraz dwa do Monachium, a linie Eurowings od dwóch do sześciu połączeń tygodniowo do Düsseldorfu. Samolot linii KLM codziennie poleci na trasie Wrocław – Amsterdam. Listę kierunków międzynarodowych uzupełniają Kopenhaga (SAS, rejsy trzy razy w tygodniu) oraz Zurych (SWISS, dwa razy w tygodniu). Na bardzo popularnej krajowej trasie do Warszawy, obsługiwanej przez PLL LOT, pasażerowie będą mieli do dyspozycji 6 rejsów dziennie*[26].

Jak informowano w maju, *po przerwie do rozkładu lotów w maju wróciły cztery połączenia – Gdańsk (od 1 maja), Zadar i Sztokholm-Skavsta (od 2 maja) oraz Larnaka (od 3 maja)*[27]. Jednocześnie powoli rozpoczynał się sezon czarterowy. Jak zauważył Cezary Pacamaj, członek zarządu Portu lotniczego Wrocław S.A.: *8 kierunków greckich, 4 hiszpańskie, 3 włoskie, 3 tureckie, po 2 w Egipcie, Tunezji i Bułgarii oraz Tirana w Albanii – tak wygląda oferta połączeń czarterowych z Wrocławia na lato 2022. – mamy szeroki wachlarz kierunków tradycyjnie cieszących się ogromnym powodzeniem. Propozycje biur podróży są różnorodne, co też sprzyja zainteresowaniu ze strony podróżnych. Wszystko to pokazuje, że połączenia czarterowe odbudowują się w bardzo szybkim tempie. Podróżni czekają na tę ofertę i chętnie z niej korzystają. Widać to było już w ubiegłorocznych statystykach*[28].

[22] Informacja prasowa PL Wrocław z dnia 16.11.2021.
[23] Informacja prasowa PL Wrocław z dnia 11.03.2022.
[24] Informacja prasowa PL Wrocław z dnia 07.04.2022.
[25] Informacja prasowa PL Wrocław z dnia 21.04.2022.
[26] Informacja prasowa PL Wrocław z dnia 11.03.2022.
[27] Informacja prasowa PL Wrocław z dnia 13.05.2022.
[28] Informacja prasowa PL Wrocław z dnia 11.03.2022.

Wykres nr 4 zawiera zestawienie liczby odprawianych w ciągu tygodnia lotów czarterowych w miesiącach letnich w roku 2007, 2018 i 2022. Wynika z niego, że liczba lotów w roku 2022 praktycznie zrównała się z tą z roku 2018 (69 do 68 na korzyść roku 2018), który był drugim w historii rokiem z najwyższą liczbą pasażerów czarterowych oscylującą w granicach 500 tys. Lepszy był tylko rok 2019, kiedy z czarterów we Wrocławiu skorzystało nieomal 550 tys. pasażerów.[29]



Wykres 5. Porównanie liczby lotów czarterowych w miesiącach letnich lat: 2007, 2018 i 2022 na lotnisku we Wrocławiu

Źródło: Opracowanie własne na podstawie: B. Węgliński, *Polacy w Europie latających narodów – rozwój połączeń międzynarodowych z Miedzynarodowego Portu Lotniczego we Wrocławiu*, [w:] G. Tokarz (red.) *Europa narodów*, Wrocław 2008, s. 360 i B. Węgliński, K. Natalli, *Rozwój regionalnych portów lotniczych w Polsce. Wpływ na gospodarkę i bezpieczeństwo społeczne oraz regionalne.* Wrocław 2019, s. 192-193; Badanie własne rozkładu lotów w PL Wrocław SA przeprowadzone w dniach 19-25.07.2022.

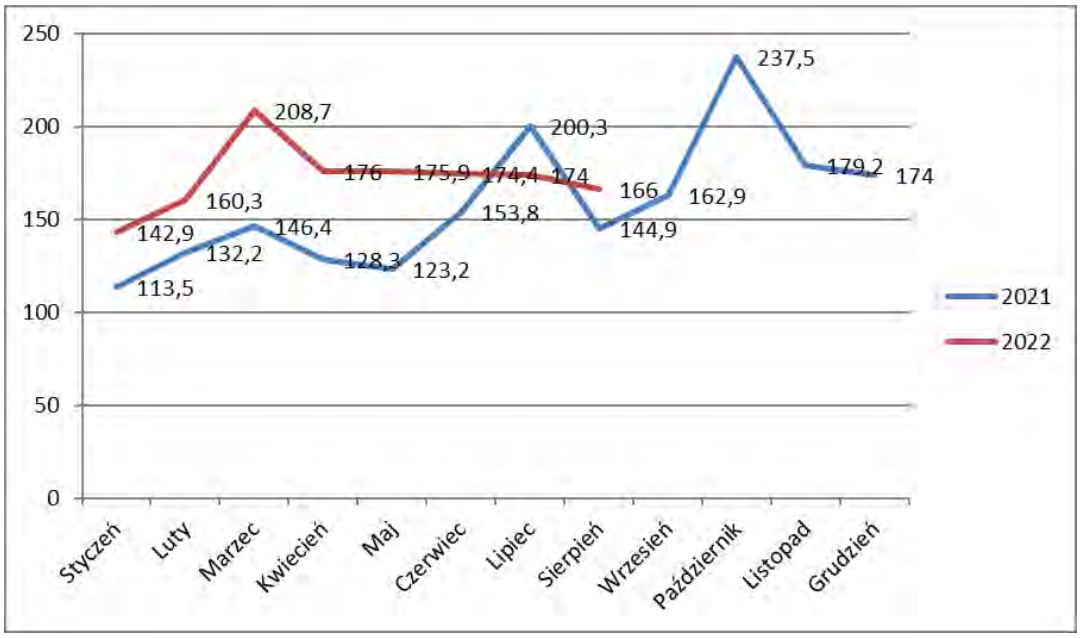
Na początku sierpnia w bazie Wizzair we wrocławskim porcie pojawił się drugi samolot[30]. Było to drugie, po sezonie letnim 2018, kiedy zdublowano liczbę maszyn po raz pierwszy rozwinięcie możliwości operacyjnych dolnośląskiej bazy przewoźnika[31]. Nowością zapowiadaną na zimowy rozkład lotów jest realizowane przez Ryanair połączenie do Porto[32]. Dariusz Kuś zauważył, że: *Pierwszy raz w historii w zimowym rozkładzie znalazły się codzienne rejsy z Wrocławia do Dublina obsługiwane przez linie*

[29] https://airport.wroclaw.pl/lotnisko/statystyki/ruch-pasazerski/ [dostęp 11.11.2022].
[30] Informacja prasowa PL Wrocław z dnia 08.08.2022.
[31] B. Węgliński, K. Natalli, op.cit, s. 187.
[32] Informacja prasowa PL Wrocław z dnia 16.09.2022.

Ryanair (do tej pory było to sześć lotów w tygodniu). Wzrośnie również liczba rejsów tego przewoźnika do Malagi (od 14 grudnia będą to dwa rejsy w tygodniu), do Gdańska (z dwóch do trzech lotów tygodniowo) i do Wenecji-Treviso – tu również loty będą realizowane trzy razy w tygodniu (we wtorki, piątki i niedziele). Te zmiany pozwolą nam zwiększyć liczbę operacji w tygodniu nawet o 13% w stosunku do 2019 r. Ten wynik stawia nas zdecydowanie powyżej średniej dla sześciu największych lotnisk Ryanaira w Polsce, które mają łączny wzrost o 6,7%[33].

W przypadku linii sieciowych widać reakcję Lufthansy na rosnący popyt na połączenia do Frankfurtu – będą je obsługiwały Embraery 190 oferujące 25% więcej miejsc od CRJ900. W czwartki i piątki pojawił się też dodatkowy, 3. w ciągu dnia lot do Monachium[34].

Cieszy także ruch cargo, który związany jest z obsługą centrum dystrybucyjnego Amazon we Wrocławiu, (wykres nr 5).



Wykres 6. Ładunki cargo odprawiane bezpośrednio na pokładach samolotów na lotnisku we Wrocławiu w roku 2021 i w miesiącach styczeń-wrzesień 2022

Źródło: https://airport.wroclaw.pl/lotnisko/statystyki/cargo/ [dostęp 11.11.2022]

Pozwala to na oczekiwanie wyniku będącego prawdopodobnie na podium historycznych wyników towarów przewożonych bezpośrednio na pokładach samolotów z wrocławskiego portu. Władze lotniska szacują, że rok 2022 będzie dużym krokiem na drodze do odbudowy ruchu z rekordowego do tej pory roku 2019. Liczba obsłużonych

[33] Informacja prasowa PL Wrocław z dnia 27.09.2022.
[34] Informacja prasowa PL Wrocław z dnia 28.10.2022.

pasażerów prawdopodobnie przekroczy 2,7 mln[35], a oferta przewoźników niskokosztowych zbliża się, lub nawet już przewyższa oferowanie z roku 2019. Ruch czarterowy odbudowuje się równie sprawnie, słabsza wydaje się oferta połączeń sieciowych – wynika to z ogólnoeuropejskich obserwacji. Firmy korzystające z linii tradycyjnych odkryły niestety w czasie pandemii całą gamę aplikacji do spotkań online. Dariusz Kuś odnosi się do tej sytuacji jednoznacznie: jednak trzeba pamiętać, że korporacje nadal w dużym stopniu pracują zdalnie, liczba podróży służbowych, choć rośnie, to wciąż jest ograniczona, a domeną tradycyjnych linii lotniczych jest głównie ruch biznesowy[36].

Przełom trzeciego i czwartego kwartału był także we wrocławskim porcie bogaty w zapowiedzi inwestycji w infrastrukturę. Najpierw Ryanair zapowiedział rozbudowę swojej bazy technicznej o kolejny hangar oferujący dwa miejsca do obsługi technicznej samolotów[37]. Tym samym o 100% wzrośnie przepustowość tej działającej od 2017 r. bazy,[38] a zatrudnienie w dobrze płatnej branży znajdzie do 2024 r. ok. 200 mechaników lotniczych.

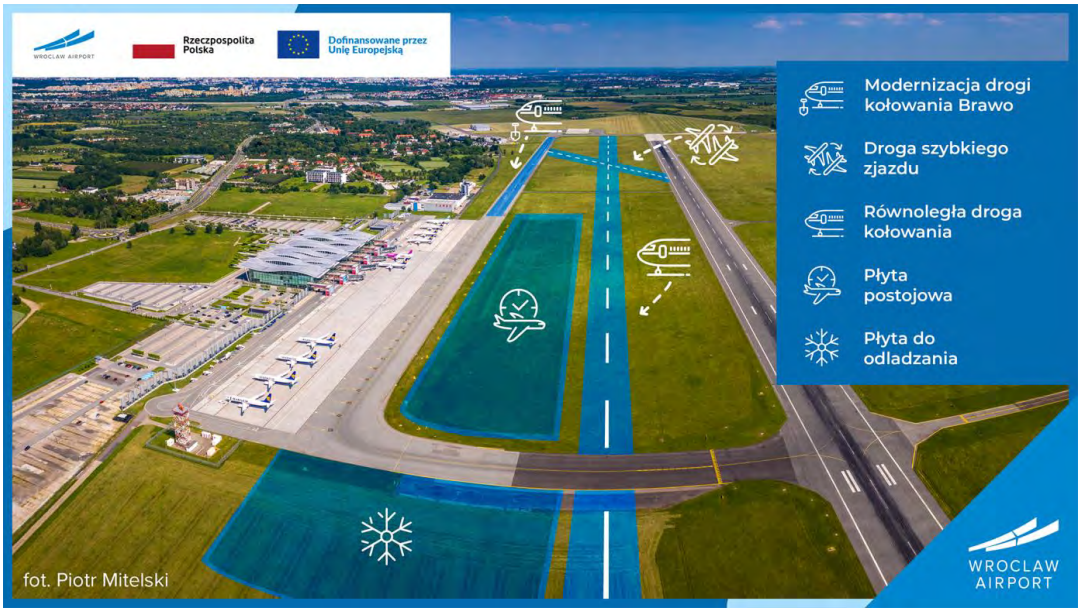
Znacznie ważniejsze wiadomości ogłoszono jednak na konferencji prasowej 25 października. Do 2025 r. wrocławski port wzbogaci się o:

- dodatkową płytę postojową, która będzie stanowiła „lustrzane odbicie" istniejącej płyty postojowej przy terminalu pasażerskim. Znajdzie się tam 12 miejsc dla samolotów kodu C takich jak Airbus 320 czy Boeing 737. (IV kwartał 2023-IV kwartał 2024); •
- dodatkową drogę kołowania, która umożliwi wykonywanie operacji lotniczych samolotów wojskowych bez wstrzymywania ruchu samolotów pasażerskich. (II kwartał 2024-II kwartał 2025);
- drogę szybkiego zjazdu, umożliwiającą szybsze opuszczenie przez samolot pasa startowego. (II kwartał 2024-II kwartał 2025);
- Nową płytę do odladzania samolotów zlokalizowaną po zachodniej stronie lotniska (obecna płyta znajduje się po stronie wschodniej).(II kwartał 2025-IV kwartał 2025);

  W ramach projektu przebudowana zostanie również istniejąca droga kołowania, (II kwartał 2025-IV kwartał 2025)[39].

Inwestycja ma kosztować ok. 350 mln zł, a połowa tej kwoty stanowi dofinansowanie z funduszy Unii Europejskie[40]. Umiejscowienie poszczególnych elementów rozbudowy pokazuje fotografia 3.

[35] Informacja prasowa PL Wrocław z dnia 21.10.2022.
[36] M.Walków,(17.09.2022) "Trochę się nauczyliśmy od Ryanaira". Prezes lotniska mówi o tym, na czym zarabiają dziś regionalne porty lotnicze, https://www.money.pl/gospodarka/troche-sie-nauczylismy-od-ryanaira-prezes-lotniska-mowi-o-tym-na-czym-zarabiaja-dzis-regionalne-porty-lotnicze-6813005312383712a.html [dostęp 11.11.2022].
[37] Informacja prasowa PL Wrocław z dnia 07.09.2022.
[38] B. Węgliński, K. Natalli, op.cit, s. 182.
[39] Informacja prasowa PL Wrocław z dnia 24.10.2022.
[40] *Ibidem.*



Fot. 3 Plany rozbudowy infrastruktury lotniska we Wrocławiu

Źródło: materiały prasowe Portu Lotniczego Wrocław SA z 24 października 2022.

Realizacja projektu pozwoli na poprawę pełnionej przez infrastrukturę lotniskową funkcji militarnej, co w połączeniu z planami armii USA budowy we Wrocławiu bazy przeładunkowej zwiększy zdolności obronne naszego państwa i ułatwi kooperację z sojusznikami z NATO[41]. Licząc na możliwości cywilnego wykorzystania infrastruktury, najistotniejsze wydają się: budowa nowej, dużej płyty postojowej pozwalającej zdecydowanie zwiększyć możliwości operacyjne lotniska oraz budowa płyty do odladzania.

Z radością można powitać także budowę nowej drogi kołowania i remont starej. Zaskakujące wydaje się budowanie ścieżki szybkiego zejścia tylko na podejściu do progu 11, a nie z obu stron drogi startowej. Z pewnością ma to jakieś uzasadnienie, którego nie widać od razu. Nie zmienia to faktu, że realizacja inwestycji pozwoli wrocławskiemu lotnisku na rozpoczęcie kolejnego etapu rozwoju we wszystkich wymiarach jego działalności.

Zakończenie

W artykule udało mi się potwierdzić postawioną we wstępie hipotezę o powrocie wrocławskiego portu do wyników pozwalających na optymizm w kolejnych latach. Liczba pasażerów odprawiana w miesiącach letnich i jesienią nieznacznie odbiega od osiąganych

[41] A. Zwoliński (15.08.2020), Będzie amerykańska baza wojskowa we Wrocławiu. Dziś zawarto umowę, https://gazetawroclawska.pl/bedzie-amerykanska-baza-wojskowa-we-wroclawiu-dzis-zawarto-umowe/ar/c1-15129521 [dostęp 11.11.2022].

w 2019 r. rekordów. Jak odnotowałem w artykule występuje pewna dysproporcja w tempie odbudowy poszczególnych segmentów rynku i o ile w przewozach niskokosztowych oferowanie jest zbliżone, a w przypadku Ryanair przewyższa to z roku 2019, o tyle prędkość przywracania ruchu przez przewoźników tradycyjnych jest zdecydowanie niższa. W przypadku lotów czarterowych także można powiedzieć o szybkiej normalizacji. Odnosząc wyniki lotniska z Wrocławia do osiągnięć innych polskich lotnisk można uznać, że nie odbiegają one od nich procentowo w znaczny sposób. Obserwując aktualizowane na bieżąco prognozy IATA dotyczące tempa odbudowy runku do poziomu sprzed pandemii, utrzymywany jest przez to stowarzyszenie termin roku 2024[42]. Po zakończeniu wojny na Ukrainie można liczyć także po odbudowie infrastruktury lotnisk w tym kraju na szybki powrót połączeń z Polski. Myślę, że popyt będzie nawet większy, bo w Polsce zostanie prawdopodobnie część Ukraińców, którzy przybyli w 2022 r. z falą uchodźców, a potencjalnymi pasażerami będą także Polacy, których połączyły z przebywającymi w naszym kraju uciekinierami relacje towarzyskie i emocjonalne. Prawdopodobnie swój potencjał potwierdziły także połączenia, które przewoźnicy uruchomili w roku 2022 w zastępstwie tras ukraińskich. Pozwolą one płynnie poszerzyć ofertę siatek połączeń, pod warunkiem posiadania wystarczającej liczby samolotów. Obaj niskokosztowi przewoźnicy operujący z Wrocławia SA jednak w procesie dynamicznej rozbudowy floty, co powinno ten proces znacznie ułatwić. Patrząc na zapowiadany rozwój infrastruktury we wrocławskim porcie można uznać, ze położy on solidny fundament pod szybki rozwój w kolejnych latach, kiedy rozważać można będzie ewentualną rozbudowę infrastruktury terminala.

Bibliografia

Czubiński R., (09.09.2022), Mikosz: Lotnictwo wraca na ścieżkę rozwoju; https://www.rynek-lotniczy.pl/wiadomosci/mikosz-lotnictwo-wraca-na-sciezke-rozwoju-15462.html [dostęp 12.11.2022]
Dybiński R. (20.03.2020), MI: Polonus i PKP Intercity dołączają do akcji #LOTdoDomu;
https://corporate.ryanair.com/news/grupa-ryanair-odwoluje-wszystkie-loty-z-do-z-polski-od-niedzieli-15-marca-do-wtorku-31-marca/?market=pl – [dostęp 10.10.2020].
https://dlapilota.pl/wiadomosci/pll-lot/pll-lot-54-tys-polakow-wrocilo-do-kraju-w-ramach-operacji-lotdodomu [dostęp 10.10.2020].
https://www.rynek-lotniczy.pl/mobile/mi-polonus-i-pkp-intercity-dolaczaja-do-akcji-lotdodomu-8145.html [dostęp 10.10.2020].
https://www.tokfm.pl/Tokfm/7,171710,25790151,lot-wszystkie-polaczenia-zawieszone-od-15-do-28-marca.html [dostęp 10.10.2020].
Informacja prasowa PL Wrocław z dnia 07.04.2022.
Informacja prasowa PL Wrocław z dnia 07.09.2022.
Informacja prasowa PL Wrocław z dnia 08.08.2022.
Informacja prasowa PL Wrocław z dnia 11.03.2022.
Informacja prasowa PL Wrocław z dnia 13.05.2022.
Informacja prasowa PL Wrocław z dnia 16.09.2022.
Informacja prasowa PL Wrocław z dnia 16.11.2021.
Informacja prasowa PL Wrocław z dnia 18.01.2017.

[42] R. Czubiński, (09.09.2022), Mikosz: *Lotnictwo wraca na ścieżkę rozwoju*; https://www.rynek-lotniczy.pl/wiadomosci/mikosz-lotnictwo-wraca-na-sciezke-rozwoju-15462.html [dostęp 12.11.2022].

Informacja prasowa PL Wrocław z dnia 19.07.2016.
Informacja prasowa PL Wrocław z dnia 21.04.2022.
Informacja prasowa PL Wrocław z dnia 21.10.2022.
Informacja prasowa PL Wrocław z dnia 23.03.2018.
Informacja prasowa PL Wrocław z dnia 24.10.2022.
Informacja prasowa PL Wrocław z dnia 27.09.2022.
Informacje prasowe Portu Lotniczego Wrocław SA.
Komisja Europejska. Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenie Rady (EWG) nr 95/93 w odniesieniu do tymczasowego złagodzenia zasad wykorzystywania czasów na start i lądowanie w portach lotniczych Wspólnoty w związku z kryzysem związanym z pandemią COVID-19, Bruksela, dnia 12.7.2022 r. COM(2022) 334 final.
Kubas K., *Wpływ pandemii na rynek transportu lotniczego*, Journal of Translogistics, 2020, s. 169-177.
Malinowski, J. (11.03.2022). W dobę przygotowali stary terminal lotniska na przyjęcie uchodźców. Jest też miejsce dla ukraińskich samolotów. https://wroclaw.wyborcza.pl/wroclaw/7,35771,28211427,w-dobe-przygotowali-stary-terminal-lotniska-na-przyjecie-uchodzcow.html.
Rajfur M. (13.04.2022). Ponad 100 tys. uchodźców przeszło przez Dworzec Główny we Wrocławiu. Najwięcej to 7 tys. dziennie. Gazeta Wrocławska.https://gazetawroclawska.pl/ponad-100-tys-uchodzcow-przeszlo-przez-dworzec-glowny-we-wroclawiu-najwiecej-to-7-tysiecy-dziennie/ar/c1-16277051.
Rozporządzenie Rady Ministrów z dnia 13 marca 2020 r. w sprawie zakazów w ruchu lotniczym Dz.U. poz. 436/2020.
Szagdaj N. (26.07.2022), Ilu Ukraińców mieszka we Wrocławiu? Stanowią oni już niemal 25 proc. wszystkich mieszkańców, https://gazetawroclawska.pl/ilu-ukraincow-mieszka-we-wroclawiu-stanowia-oni-juz-niemal-25-proc-wszystkich-mieszkancow/ar/c1-16526591.
ULC Analiza rynku transportu lotniczego w Polsce w latach 2004-2007, Warszawa wrzesień 2009.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu regularnym i czarterowym w polskich portach lotniczych w latach 2008-2010, Warszawa 2011.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2010-2012, Warszawa 2013.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2014-2016, Warszawa 2017.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2015-2017, Warszawa 2018.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2016-2018; Warszawa 2019.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2017-2019, Warszawa 2021.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2018-2020, Warszawa 2021.
ULC Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w czwartym kwartale lat 2019-2021, Warszawa 2022.
ULC Analiza rynku transportu lotniczego w Polsce w latach 2004-2006, Warszawa, wrzesień 2008.
Unia Metropolii Polskich. Miejska gościnność. Szacunek liczby Ukraińców w miastach UMP w miesiącach marzec, kwiecień, maj 2022 r. Aktualizacja raportu Miejska gościnność:wielki wzrost, wyzwania i szanse. Raport o uchodźcach z Ukrainy w największych polskich miastach z kwietnia 2022 r.; Warszawa, lipiec 2022.
Ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze*, Dz.U. poz. 1580/2019.
Walków M., (17.09.2022) "Trochę się nauczyliśmy od Ryanaira". Prezes lotniska mówi o tym, na czym zarabiają dziś regionalne porty lotnicze, https://www.money.pl/gospodarka/troche-sie-nauczylismy-od-ryanaira-prezes-lotniska-mowi-o-tym-na-czym-zarabiaja-dzis-regionalne-porty-lotnicze-68130053123837-12a.html [dostęp 11.11.2022].
Węgliński B., *Zagrożenie terroryzmem we współczesnym świecie a system bezpieczeństwa państwa*. Wrocław 2016.
Węgliński B., *Polacy w Europie latających narodów – rozwój połączeń międzynarodowych z Miedzynarodowego Portu Lotniczego we Wrocławiu*, [w:] G. Tokarz (red.) *Europa narodów*, Wrocław 2008.
Węgliński B., *Przewozy krajowe w Polsce. Polskie lotnictwo komunikacyjne w roku 2010*. [w:] Mickiewicz P., Węgliński B. (red.), „Otwarte niebo" nad Dolnym Śląskiem, Wrocław 2011.

Węgliński B., Natalli K., *Rozwój regionalnych portów lotniczych w Polsce Wpływ na gospodarkę i bezpieczeństwo społeczne oraz regionalne.* Wrocław 2019.

Zając G., *Contemporary political, legal and economic aspects of aviation safety*. [w:] International Journal of Social Science and Economic Research, vol. 5 issue:9, September 2020, s. 2417-2435.

Zając G., *Kryzys lotniczy w związku z Coronavirusem* [w:] Przegląd komunikacyjny 11/2020,s.13-18.

Zwoliński A., (15.08.2020), Będzie amerykańska baza wojskowa we Wrocławiu. Dziś zawarto umowę, https://gazetawroclawska.pl/bedzie-amerykanska-baza-wojskowa-we-wroclawiu-dzis-zawarto-umowe-/ar/c1-15129521 [dostęp 11.11.2022].

Beata Służalska[1]

Jarosław Służalski[2]

Zarządzanie sprywatyzowaną częścią zadań dotyczących zapewnienia bezpieczeństwa i porządku publicznego

Streszczenie

Artykuł ma na celu przybliżenie problematyki udziału komercyjnych podmiotów ochronnych, w procesach zarządzania sprywatyzowaną częścią bezpieczeństwa lokalnego. Autorzy dokonując analizy głównych zadań wykonywanych przez pracowników ochrony fizycznej, dochodzą do wniosku, że w sprywatyzowanym sektorze bezpieczeństwa skupiony został ogromny potencjał osobowy i techniczny, uzbrojenie i wyposażenie, a także wiedza i umiejętności przekazywane pracownikom ochrony w procesie ich edukacji. Właściwe aktywowanie tego potencjału, wpłynąć może znacząco na poprawę stanu bezpieczeństwa w jego wymiarze personalnym i strukturalnym.

Słowa kluczowe: komercyjna ochrona, współpraca, bezpieczeństwo, zarządzanie.

Summary

The article aims to present the issues of the participation of commercial security entities in the management processes of the privatized part of local security. The authors, analyzing the main tasks performed by physical security personnel, come to the conclusion that the privatized security sector concentrates enormous personnel and technical potential, armaments and equipment, as well as knowledge and skills transferred to security personnel in the process of their education. Proper activation of this potential may significantly improve the security situation in its personnel and structural terms.

Keywords: commercial protection, cooperation, security, management.

[1] Dr Beata Służalska, adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.

[2] Dr Jarosław Służalski, adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.

Poziom skuteczności realizacji zadań z zakresu zarządzania kryzysowego wyznaczony jest nie tylko poprzez efektywność działań organów i formacji rządowych oraz samorządowych, ukierunkowanych na zwalczanie zagrożeń, ale także przez gotowość wszystkich obywateli do wspierania tych działań. Zapewnienie bezpieczeństwa, staje się wspólną płaszczyzną odpowiedzialności zarówno Sił Zbrojnych RP, jak również innych instytucji działających w ramach systemu bezpieczeństwa wewnętrznego kraju. Do tych ostatnich, oprócz formacji powołanych przez państwo, zaliczyć można prywatne przedsiębiorstwa ochronne.

O strukturze i treści niniejszego artykułu decydować będą odpowiedzi na następujące pytania:

1) Jakie są głównych zadania podejmowane przez pracowników ochrony w obszarze przestrzeni miejskich?
2) Jaki jest wpływ organów struktur państwowych na funkcjonowanie komercyjnego sektora bezpieczeństwa?
3) Jakie są zasady nadzoru i kontroli państwa nad specjalistycznymi uzbrojonymi formacjami ochronnymi?
4) W jakim obszarze i na jakich zasadach może dojść do stworzenia zintegrowanego systemu zarządzania bezpieczeństwem przestrzeni miejskich, z udziałem prywatnych formacji ochrony osób i mienia?

Ważnym efektem badań, stanie się bez wątpienia analiza krytyczna zarządzania sprywatyzowaną częścią bezpieczeństwa i porządku publicznego.

Rozpoczynając rozwiązanie zasygnalizowanych problemów, odniesiono się do głównych regulacji prawnych wyznaczających obszar działania prywatnego sektora ochrony osób i mienia. Jego funkcjonowanie, legislacyjnie, uzasadnia ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia[3]. Jest ona również podstawowym aktem prawnym, pozwalającym, w sposób profesjonalny, organizować komercyjne instytucje ochronne.

Do 27 marca 1998 r., czyli do zakończenia *vacatio legis* powyższej ustawy, nie było szczegółowego aktu prawnego tej rangi, regulującego kwestie ochrony komercyjnej. Zabezpieczenie przestrzeni miejskich, w tym ludzi i mienia, odbywało się na zasadach ogólnych, a zleceniodawca czynności ochronnych mógł powierzyć pracownikom ochrony zadania, do jakich sam miał uprawnienia[4]. Przepisy nie pozwalały również na stosowanie przez pracowników ochrony środków przymusu bezpośredniego i broni palnej. Brak tego typu regulacji doprowadził, w połowie lat dziewięćdziesiątych, do licznych nadużyć, które

[3] Ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia* (Dz.U. z 1997 r., Nr 114, poz. 740, z zm.).

[4] Wśród nich, największe znaczenie dla funkcjonowania prywatnego sektora ochrony miały przepisy ustawy o działalności gospodarczej, ale także przepisy Kodeksu Karnego, dotyczące obrony koniecznej, stanu wyższej konieczności, przepisy Kodeksu Postępowania Karnego, określające prawo do ujęcia sprawcy przestępstwa na gorącym uczynku lub w pościgu bezpośrednio po popełnieniu przestępstwa oraz przepisy kodeksu cywilnego odnoszące się do ochrony posesyjnej, przysługującej posiadaczowi rzeczy.

zostały opisane w raporcie Najwyższej Izby Kontroli z 1997 r.[5] Raport ten spowodował zwiększenie zainteresowań komercyjną ochroną osób i mienia i zainicjował podjęcie prac nad nową ustawą. Regulacje w niej zawarte zapoczątkował proces prywatyzacji bezpieczeństwa. Państwowe struktury ochronne, pewien zakres swych zadań przekazały koncesjonowanym firmom ochrony osób i mienia, a także szkołom i placówkom oświatowym, kształcącym pracowników ochrony. Z pewnością przełomowym zdarzeniem, które, do czasów wejścia w życie ustawy o ochronie osób i mienia nie miało miejsca w prawodawstwie polskim było nadanie pracownikom ochrony prawa do użycia i wykorzystania broni palnej. Ale to już historia. Obecnie, najważniejszą sprawą jest umiejscowienie prywatnych struktur ochronnych w systemie zarządzania bezpieczeństwem zarówno na poziomie ogólnokrajowym, jaki i lokalnym. Mając na uwadze doniosłość powyższego stwierdzenia, określono zakres czynności ochronnych, wykonywanych przez kwalifikowanych pracowników ochrony oraz odniesiono go do głównych regulacji prawnych.

Ostatecznie, problematykę komercyjnej ochrony osób i mienia, określiły: wspomniana ustawa o ochronie osób i mienia i ustawa o bezpieczeństwie imprez masowych[6].

Rysunek 1. przedstawia szczegółowy zakres regulacji obydwu ustaw oraz szereg rozporządzeń regulujących czynności, podejmowane w zakresie komercyjnej ochrony.

Pierwsza z ustaw dotyczy w szczególności obszarów, obiektów i urządzeń, podlegających obowiązkowej ochronie, zasad tworzenia i funkcjonowania wewnętrznych służb ochrony, zasad prowadzenia działalności gospodarczej w zakresie ochrony osób i mienia oraz zasad transportowania broni, amunicji, materiałów wybuchowych, uzbrojenia, urządzeń i sprzętu wojskowego. Wykonywanie zadań, z zakresu ochrony osób i mienia uregulowane zostało także w rozporządzeniach Rady Ministrów[7] oraz Ministra Spraw Wewnętrznych i Administracji[8]. Przedmiotem regulacji drugiej ustawy stały się:

---

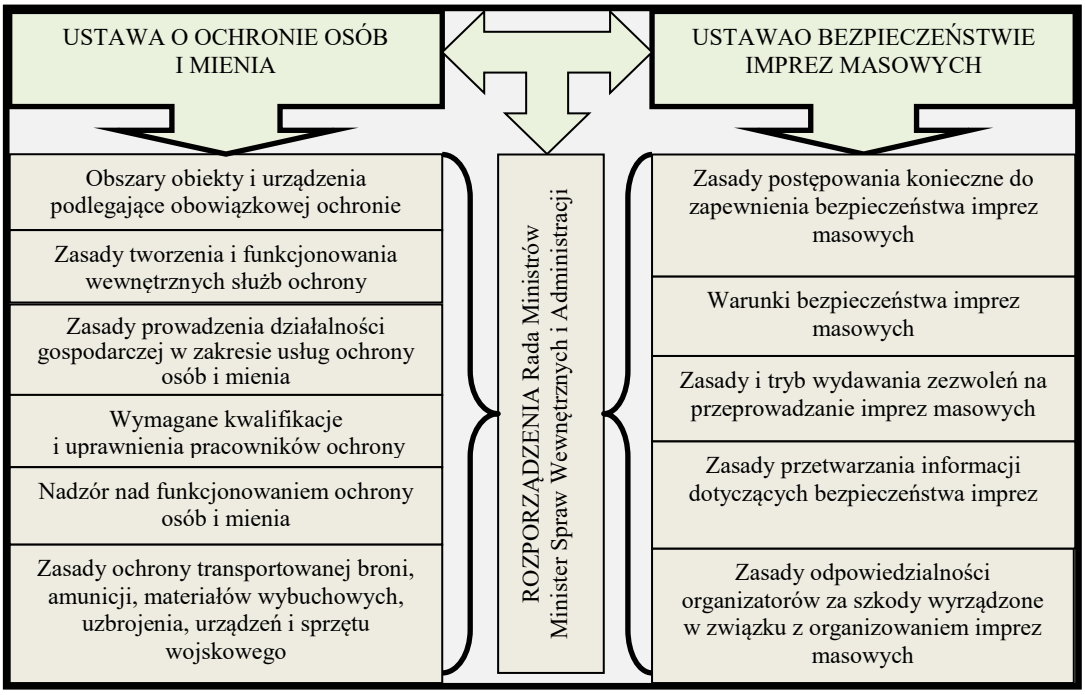
[5] A. Misiuk, *Administracja porządku i bezpieczeństwa publicznego. Zagadnienia prawno-ustrojowe*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008, s. 169.

[6] Ustawa z dnia 20 marca 2009 r. *o bezpieczeństwie imprez masowych* (Dz.U. z 2009 r., nr 62, poz. 504).

[7] Głównymi rozporządzeniami Rady Ministrów, dotyczącymi ochrony osób i mienia jest Rozporządzenie Rady Ministrów z dnia 19 grudnia 2013 r. *w sprawie szczegółowego trybu działań pracowników ochrony* (Dz.U. 2013 poz. 1681).

[8] Podstawowymi rozporządzeniami Ministra Spraw Wewnętrznych i Administracji, dotyczących ochrony osób i mienia są: Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 listopada 1998 r. *w sprawie wewnętrznych służb ochrony* (Dz.U. z 1999 r. nr 4 poz. 31); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 9 września 1998 r. *w sprawie rodzajów obiektów, w których mogą być stosowane paralizatory elektryczne* (Dz.U. nr 120 poz. 780), Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 grudnia 1998 r. *w sprawie szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją, jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi)* (Dz.U. nr 161 poz. 1108); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 października 2011 r. *w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji* (Dz.U. 2011 nr 245 poz. 1462); Rozporządzenie Ministra Spraw Wewnętrznych z dnia 16 grudnia 2013 r. *w sprawie dokumentowania działalności gospodarczej w zakresie usług ochrony osób i mienia* (Dz.U. 2013 poz. 1739); Rozporządzenie Ministra Spraw Wewnętrznych z dnia 18 grudnia 2013 r. *w sprawie wymagań w zakresie szkoleń i kursów potwierdzających przygotowanie teoretyczne i praktyczne w zakresie wyszkolenia strzeleckiego, samoobrony, technik interwencyjnych oraz znajomości przepisów prawa związanych z wykonywaniem ochrony osób i mienia* (Dz.U. 2013 poz. 1688); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 stycznia 2016 r. *w sprawie szczegółowej tematyki, formy oraz czasu trwania kursu doskonalącego umiejętności kwalifikowanych pracowników ochrony fizycznej* (Dz.U. 2016 poz. 103); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 lipca 2016 r. *w sprawie*

zasady postępowania konieczne do zapewnienia bezpieczeństwa imprez masowych; warunki bezpieczeństwa imprez masowych; zasady i tryb wydawania zezwoleń na przeprowadzanie imprez masowych; zasady przetwarzania informacji dotyczących bezpieczeństwa imprez masowych, w tym danych osobowych; zasady odpowiedzialności organizatorów za szkody wyrządzone w związku ze zorganizowaniem imprez masowych.



Rys. 1. Ochchrona osób i mienia – podstawowe regulacje prawne

Źródło: J. Służalski, B. Służalska – opracowanie własne, na podstawie ustawy o ochronie osób i mienia oraz ustawy o bezpieczeństwie imprez masowych.

Działania komercyjnych formacji ochronnych, związane z zapewnianiem bezpieczeństwa przestrzeni miejskich, uzależnione są ściśle, z określoną w ustawie o ochronie osób i mienia, kategorią obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie. Obligatoryjnemu zabezpieczeniu podlegają również imprezy masowe, charakteryzujące się współczynnikami wyznaczonymi przez ustawę o bezpieczeństwie imprez masowych. Jednakże najważniejszym zadaniem, związanym z bezpieczeństwem infrastruktur miejskich, a tym samym życia i zdrowia ludzkiego, jest

wzoru wniosku o udzielenie lub zmianę koncesji na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia (Dz.U. 2016 poz. 1217); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 czerwca 2017 r. *w sprawie legitymacji pracowników ochrony* (Dz.U. 2017 poz. 1307); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 czerwca 2017 r. *w sprawie legitymacji wydawanych pracownikom wewnętrznej służby ochrony* (Dz.U. 2017 poz. 1306); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 1 marca 2022 r. zmieniające rozporządzenie *w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (Dz.U. 2022, poz. 495).

zapewnienie fizycznej i technicznej ochrony obszarów, obiektów i urządzeń. Ustawa o ochronie osób i mienia klasyfikuje je, ujmując w pięciu kategoriach: ważne dla obronności państwa, interesu gospodarczego, bezpieczeństwa publicznego, innych ważnych interesów państwa oraz obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej. (art. 5, ust. 1 i 2).

W obszarze działań, podejmowanych przez Wewnętrzne Służby Ochrony (WSO)[9] lub Specjalistyczne Uzbrojone Formacje Ochronne (SUFO)[10], na rzecz zabezpieczenia obiektów ważnych ze względu na obronność państwa, znajdują się: zakłady produkcji specjalnej oraz zakłady, w których prowadzone są prace naukowo-badawcze lub konstruktorskie w zakresie takiej produkcji, zakłady produkujące, remontujące i magazynujące uzbrojenie, urządzenia i sprzęt wojskowy, a także magazyny rezerw strategicznych. W zakresie interesu gospodarczego państwa, obowiązkowej ochronie podlegają zakłady mające bezpośredni związek z wydobyciem surowców mineralnych o strategicznym znaczeniu dla państwa, porty morskie i lotnicze oraz banki i przedsiębiorstwa wytwarzające, przechowujące bądź transportujące wartości pieniężne, w znacznych ilościach. Obowiązkowej ochronie, ze względu na bezpieczeństwo publiczne, podlegają zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania obszarów miejskich, których zniszczenie lub uszkodzenie może spowodować zagrożenie dla życia i zdrowia ludzi oraz środowiska. Są to w szczególności: elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków. Obowiązkowemu zabezpieczeniu przez Specjalistyczną Uzbrojoną Formację Ochronną, w ramach przedstawianej kategorii, podlegają także: zakłady stosujące, produkujące lub magazynujące, w znacznych ilościach, materiały jądrowe, źródła i odpady promieniotwórcze, materiały toksyczne, odurzające, wybuchowe bądź chemiczne o dużej podatności pożarowej lub wybuchowej, rurociągi paliwowe, linie energetyczne i telekomunikacyjne, zapory wodne i śluzy oraz inne urządzenia, znajdujące się w otwartym terenie, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia lub zdrowia ludzi, środowiska albo spowodować poważne straty materialne. W zakresie ochrony innych ważnych interesów państwa podlegają: zakłady o unikalnej produkcji gospodarczej, obiekty i urządzenia telekomunikacyjne, pocztowe oraz telewizyjne i radiowe, muzea i inne obiekty, w których zgromadzone są dobra kultury narodowej, a także archiwa państwowe. W skład infrastruktury krytycznej wchodzą następujące systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia

[9] Wewnętrzne Służby Ochrony to uzbrojone i umundurowane zespoły pracowników przedsiębiorców lub jednostek organizacyjnych, powołane do ich ochrony (art. 2, ust. 8 ustawy z 22 sierpnia 1997 r. *o ochronie osób i mienia*).

[10] Specjalistyczne Uzbrojone Formacje Ochronne (SUFO) to Wewnętrzne Służby Ochrony oraz przedsiębiorcy, którzy uzyskali koncesję na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia, posiadający pozwolenie na broń na okaziciela, wydane na podstawie odrębnych przepisów (art. 2 ust 7 ustawy z 22 sierpnia 1997 r. *o ochronie osób i mienia*).

w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[11].

Powyższa lista ma charakter otwarty, dający się uzupełniać w miarę pojawiania się nowych form zagrożeń bezpieczeństwa ludzi i mienia oraz infrastruktury istotnej dla funkcjonowania państwa. Podstawowym celem obowiązkowej ochrony, jest zapewnienie należytego funkcjonowania elementów infrastruktury krytycznej tzn. instytucji, przedsiębiorstw, instalacji, dróg, rurociągów itp., szczególnie ważnych dla obronności państwa, a także bezpieczeństwa publicznego i interesu gospodarczego. Szczegółowy wykaz zagrożonych obszarów, obiektów i urządzeń sporządzają: Prezes Narodowego Banku Polskiego, Krajowa Rada Radiofonii i Telewizji, ministrowie, kierownicy urzędów centralnych i wojewodowie. Tryb ustanawiania obowiązkowej ochrony, realizowany jest w dwóch etapach. W pierwszym etapie uprawnione osoby szczebla centralnego typują, spośród podległych im jednostek organizacyjnych, te które wymagają ochrony obowiązkowej. W drugim etapie wyciągi z tych wykazów przesyłane są do właściwych terytorialnie wojewodów. Wojewodowie uzupełniają je o podległe im obiekty, wymagające obowiązkowej ochrony i umieszczają w prowadzonej przez siebie ewidencji[12]. Zgodnie z art. 5 ust. 6 ustawy o ochronie osób i mienia, wojewoda, w drodze decyzji administracyjnej, może również umieścić w ewidencji, znajdujące się na terenie województwa obszary, obiekty i urządzenia innych podmiotów, niż wymienione powyżej.

Minister Spraw Wewnętrznych i Administracji, na wniosek organów sporządzających wykazy obiektów przeznaczonych do obowiązkowej ochrony, może wprowadzić, dla jednostek organizacyjnych im podległych lub przez nie nadzorowanych, regulamin ogólnych warunków i trybu wykonania zabezpieczeń. Warunkiem bezwzględnym, jest konieczność uzgodnienia planu ochrony przez kierownika zarządzającego obszarami, obiektami i urządzeniami podlegającymi obowiązkowej ochronie, z właściwym terytorialnie komendantem wojewódzkim Policji. Ponadto, zadania realizowane w celu zapewnienia ochrony tych obszarów, obiektów i urządzeń, wykonywać mogą wyłącznie osoby posiadające wpis na listę kwalifikowanych pracowników ochrony fizycznej[13]. Wspomniany powyżej plan ochrony[14], stanowi podstawowy dokument, niezbędny do podjęcia kompleksowej ochrony obszarów, obiektów i urządzeń ważnych dla obronności, bezpieczeństwa publicznego oraz interesów gospodarczych państwa.

---

[11] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. 2007 Nr 89 poz. 590 z poźn. zm.).

[12] Por.: S. Kulczyński, *Ochrona obiektów*, Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'Chikara, Lublin 2006, s. 12.

[13] Szerzej: *Ochrona osób i mienia*, (red.) M. Enerlich, TNOiK, Toruń 2003.

[14] Plan ochrony powinien spełniać następujące warunki: uwzględniać charakter produkcji lub rodzaj działalności jednostki; zawierać analizę stanu potencjalnych zagrożeń i aktualnego stanu bezpieczeństwa jednostki; podawać ocenę aktualnego stanu ochrony jednostki; zawierać dane, dotyczące specjalistycznej uzbrojonej formacji ochronnej, a w tym: stan etatowy, rodzaj oraz ilość uzbrojenia i wyposażenia, sposób zabezpieczenia broni i amunicji; zawierać dane, dotyczące rodzaju zabezpieczeń technicznych. Szerzej o planie ochrony w: *Metodyka uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie*, Warszawa 2016.

Z przeglądu kategorii obiektów podlegających obowiązkowej ochronie wynika, że większość z nich zlokalizowana jest w obszarach przestrzeni zurbanizowanej, ma więc decydujący wpływ na funkcjonowanie przestrzeni miejskich. Działania, które podejmowane są przez komercyjne formacje ochronne, determinują stan bezpieczeństwa ludzi, mienia i środowiska naturalnego. Uzasadniona jest więc dyspozycja art. 48 ustawy o ochronie osób i mienia, nakładająca sankcję karną na kierowników jednostek organizacyjnych, którzy wbrew obowiązkowi, nie zapewniają fizycznej lub technicznej ochrony[15]. Kontrowersyjną i niezgodną z pragmatyką działań, jest możliwość rozłącznego zastosowania ochrony fizycznej i technicznej. Obydwie formy ochrony (fizyczna i techniczna) powinny się wzajemnie uzupełniać. Sygnały alarmowe, generowane przez techniczne systemy zabezpieczeń, prowadzić muszą do fizycznej interwencji pracowników ochrony, a działania pracowników ochrony powinny być wspierane współczesną techniką z zakresu zabezpieczeń elektronicznych. Niemożliwe jest prowadzenie skutecznej ochrony tylko przy pomocy jednej z jej form. Słuszny jest więc wniosek, że pomimo ustawowego podziału komercyjnych działań ochronnych na dwie kategorie: bezpośrednią ochronę fizyczną i zabezpieczenie techniczne, najbardziej efektywną formą zabezpieczenia jest połączenie obu form w jednolity system.

Ogół powierzonych zadań oraz nadanych uprawnień[16] pracownikom Specjalistycznych Uzbrojonych Formacji Ochronnych, powoduje potrzebę umiejscowienia tych podmiotów w systemie zarządzania bezpieczeństwem i porządkiem publicznym.

[15] Ustawodawca, dla osób naruszających dyspozycję tej normy prawnej, przewiduje karę grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch.

[16] Główne uprawnienia pracowników ochrony określa rozdział 6 ustawy o ochronie osób i mienia. W myśl jego zapisów, pracownik ochrony, w granicach chronionych obiektów i obszarów, ma prawo do: ustalania uprawnień do przebywania na obszarach lub w obiektach chronionych oraz legitymowania osób, w celu ustalenia ich tożsamości; wezwania osób do opuszczenia obszaru lub obiektu w przypadku stwierdzenia braku uprawnień do przebywania na terenie chronionego obszaru lub obiektu albo stwierdzenia zakłócania porządku; ujęcia osób, stwarzających bezpośrednie zagrożenie dla życia lub zdrowia ludzkiego, a także dla chronionego mienia, w celu niezwłocznego oddania tych osób Policji; stosowania środków przymusu bezpośredniego (siła fizyczna, w postaci technik: obrony, obezwładniania, transportowych, kajdanki zakładane na ręce, pałka służbowa, pies służbowy, przedmiot przeznaczony do obezwładniania osób na pomocą energii elektrycznej, ręczny miotacz substancji obezwładniających), w przypadkach określonych w ustawie z dnia 24 maja 2013 r. *o środkach przymusu bezpośredniego i broni palnej* (Dz.U. z 2022 r. poz. 1416). użycia lub wykorzystani broni palnej, w granicach chronionych obiektów i obszarów, w przypadku konieczność odparcia bezpośredniego, bezprawnego zamachu na:
a) życie, zdrowie lub wolność uprawnionego lub innej osoby,
b) ważne obiekty, urządzenia lub obszary,
c) mienie, który stwarza jednocześnie bezpośrednie zagrożenie życia, zdrowia lub wolności uprawnionego lub innej osoby, a także, konieczności przeciwstawienia się osobie:
d) niepodporządkowującej się wezwaniu do natychmiastowego porzucenia broni, materiału wybuchowego lub innego niebezpiecznego przedmiotu, którego użycie może zagrozić życiu, zdrowiu lub wolności uprawnionego lub innej osoby,
e) która usiłuje bezprawnie odebrać broń palną uprawnionemu lub innej osobie uprawnionej do jej posiadania, oraz
f) zaalarmowanie lub wezwanie pomocy,
g) oddanie strzału ostrzegawczego,
h) zniszczenia lub unieruchomienia bezzałogowego statku powietrznego, w przypadkach określonych w ustawie z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz.U. z 2020 r. poz. 1970, z 2021 r. poz. 784, 847 i 1898 oraz z 2022 r. poz. 655).
Pracownik ochrony poza granicami chronionych obiektów i obszarów ma prawo do użycia i wykorzystania broni palnej w przypadku:
a) konieczność odparcia bezpośredniego, bezprawnego zamachu na bezpieczeństwo konwoju lub doprowadzenia,
b) zaalarmowania lub wezwania pomocy,
c) oddania strzału ostrzegawczego.

Konieczne stało się również wypracowanie mechanizmów nadzoru oraz kontroli państwowej nad zadaniami i uprawnieniami, powierzonymi komercyjnym firmom ochrony osób i mienia.

Rysunek 2. przedstawia główne organy struktur państwowych i ich wpływ na funkcjonowanie komercyjnego sektora bezpieczeństwa. Wyszczególnia jednocześnie obszary współpracy prywatnych struktur ochronnych z formacjami państwowymi i samorządowymi, predestynowanymi do ochrony ludności. Treści przedstawione na rysunku stanowić mogą bazę wyjściową do określenia płaszczyzn, w oparciu o które można podjąć próbę stworzenia zintegrowanego systemu zarządzania bezpieczeństwem, z udziałem struktur państwowych, samorządowych i prywatnych.

Ustawa o ochronie osób i mienia, w rozdziale 7, określiła zasady nadzoru nad SUFO oraz kontroli stanu ochrony obszarów, obiektów i urządzeń przez nie zabezpieczanych. Ogólnie czynności nadzorczo-kontrolne, można podzielić na leżące w dyspozycji: Ministra Spraw Wewnętrznych, Komendanta Głównego Policji, komendanta wojewódzkiego Policji oraz komendanta komisariatu Policji. Nadzór Komendanta Głównego Policji odnosi się do Specjalistycznych Uzbrojonych Formacji Ochronnych oraz przedsiębiorców, którzy uzyskali koncesję na prowadzenie działalności gospodarczej w zakresie usług ochrony osób i mienia oraz posiadają pozwolenie na broń na okaziciela, tzw. świadectwo broni (art. 2 pkt 7 ustawy). Nie dotyczy natomiast przedsiębiorców, którzy nie posiadają świadectwa broni. Ta kategoria przedsiębiorców podlega jedynie kontroli zarządzanej przez organ koncesyjny[17].

Rys. 2. Specjalistyczne uzbrojone formacje ochronne, nadzór – kontrola – współpraca

Źródło: J. Służalski, B. Służalska – opracowanie własne.

[17] Por.: W. Kotowski, *Ochrona osób i mienia. Komentarz praktyczny*, Difin, Warszawa 2004, s. 302.

Nadzór nad SUFO, ze strony Komendanta Głównego Policji**,** reguluje art. 43 ustawy o ochronie osób i mienia, z zastrzeżeniem, że kontrolę, na podległych sobie terenach, sprawuje Minister Obrony Narodowej; może ją prowadzić również Żandarmeria Wojskowa. Natomiast Komendant Główny Straży Granicznej sprawuje nadzór nad SUFO, w zakresie wykonywania zadań związanych z kontrolą bezpieczeństwa, przeprowadzaną w krajowych portach lotniczych.

W ramach zarządzania sprywatyzowaną częścią zadań obszaru bezpieczeństwa, Komendant Główny Policji kontroluje zasady i sposoby realizacji zadań ochrony osób i mienia, sposób użycia i wykorzystania przez pracowników SUFO środków przymusu bezpośredniego i broni palnej oraz posiadanie przez pracowników ochrony specjalistycznych kwalifikacji. Nadzór Komendanta Głównego Policji nad sposobem realizacji zadań ochrony osób i mienia polega przede wszystkim na kontroli organizacji i zasad działania, uzbrojenia, wyposażenia oraz współpracy z innymi formacjami oraz służbami. Kontroli podlega również zgodność aktualnego stanu ochrony jednostki z planem ochrony. Na podstawie pisemnego upoważnienia, wydanego przez Komendanta Głównego Policji, wyznaczony funkcjonariusz Policji ma prawo wstępu na teren obszaru i obiektów, w których jest prowadzona ochrona, a także do siedziby przedsiębiorcy prowadzącego firmę. Ma on również prawo żądać wyjaśnień i udostępnienia, bądź wglądu w dokumentację ochronną. W razie stwierdzenia uchybień, osoba kontrolująca, wydaje pisemne zalecenia w celu usunięcia nieprawidłowości i dostosowania działalności SUFO do przepisów prawa.

Znaczący wpływ na funkcjonowanie prywatnego sektora ochrony osób i mienia ma również komendant wojewódzki Policji. W zakresie jego uprawnień znalazło się m.in. opiniowanie decyzji organu koncesyjnego w sprawach udzielenia oraz cofnięcia koncesji na prowadzenie działalności gospodarczej w zakresie ochrony osób i mienia. Wydaje on również decyzję dotyczącą utworzenia Wewnętrznych Służb Ochrony, a także uzgodnienia planu ochrony.

Komendant wojewódzki Policji jest organem właściwym w sprawie wydawania wpisu na listę kwalifikowanych pracowników ochrony fizycznej. Wydaje również pozwolenia na broń na okaziciela Wewnętrznym Służbom Ochrony oraz przedsiębiorcom posiadającym koncesje na prowadzenie działalności w zakresie usług ochrony osób i mienia. Komendant komisariatu Policji wydaje natomiast opinię kandydatom na kwalifikowanego pracownika ochrony fizycznej.

Jak wynika z powyższych ustaleń, Policja sprawuje nadzór i kontrolę nad funkcjonowaniem prywatnego sektora ochrony w Polsce. Do grona instytucji nadzorczych należy również Ministerstwo Spraw Wewnętrznych i Administracji. Sprawuje ono nadzór nad wydawaniem, wykonaniem oraz cofnięciem koncesji[18].

[18] Szerzej: P. Kubiński, *Działalność gospodarcza w zakresie ochrony osób i mienia i jej koncesjonowanie*, Wolters Kluwer, Warszawa 2008.

Jak słusznie zauważa Z. Nowicki – pracownik ochrony spotkać się może z kontrolą swej działalności w każdym miejscu i czasie.

Kontroli dokonywać może osoba reprezentująca organ koncesyjny, tj. pracownik Departamentu Zezwoleń i Koncesji MSWiA, a także działający z jego upoważnienia przedstawiciel innego organu państwowego, który specjalizuje się w kontroli danego rodzaju działalności, na przykład funkcjonariusz Policji, pracownik stacji sanitarno-epidemiologicznej, funkcjonariusz straży pożarnej, pracownik służby zatrudnienia itp.[19].

Niezaprzeczalnym staje się fakt, że bezpieczeństwo przestrzeni zurbanizowanej zależy również od precyzyjnie określonych zasad współpracy prywatnych podmiotów ochrony osób i mienia z głównymi formacjami bezpieczeństwa, powołanymi przez państwo i organy samorządu terytorialnego.

Współdziałanie formacji, wymaga określenia precyzyjnych zasad podziału kompetencji i opracowania skutecznych algorytmów postępowania, w sytuacjach typowych oraz wzmożonego zagrożenia ludności i miejskiej infrastruktury krytycznej.

Rys. 3. przedstawia obecny stan prawny oraz sygnalizuje potrzebę wprowadzenia zmian umożliwiających podejmowanie przez SUFO samodzielnej współpracy z formacjami struktur państwowych i samorządowych.

Pomimo ponad dwudziestopięcioletniego funkcjonowania, na rynku polskim, koncesjonowanych agencji ochrony osób i mienia oraz ponad dwustu pięćdziesięciu tys. pracowników ochrony[20], fragmentarycznie i bardzo ogólnie określone zostały zasady współpracy SUFO z formacjami państwowymi i samorządowymi.

Zasady te reguluje rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 grudnia 1998 r. w sprawie określenia szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją, jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi)[21].

Współpracę, o której mowa w rozporządzeniu, podejmuje kierownik jednostki chronionej przez SUFO z właściwym terytorialnie komendantem Policji, kierownikiem jednostki ochrony przeciwpożarowej, komendantem Straży Gminnej oraz szefem Obrony Cywilnej.

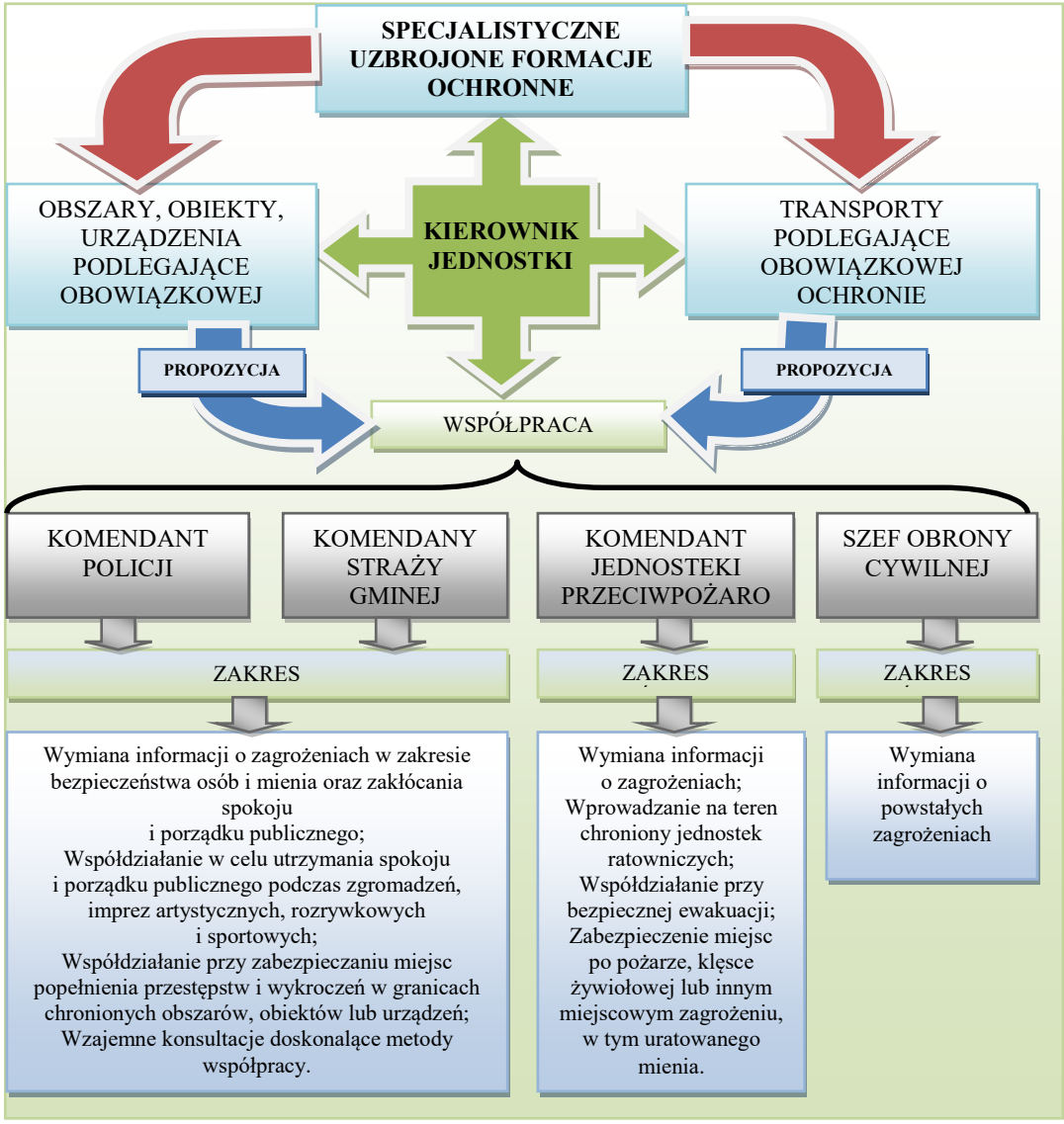
Wynika stąd, że SUFO nie mają wystarczających podstaw prawnych do podejmowania współpracy z formacjami wymienionymi w rozporządzeniu. Pozostaje im jedynie działanie wykonawcze, czyli realizacja ustaleń na szczeblu kierownik jednostki chronionej – komendant.

---

[19] Por.: Z.T. Nowicki, *Ochrona osób i mienia. Podstawy organizacyjno-prawne*, TNOiK, Toruń 1999, s. 256.

[20] www.10zl.org.

[21] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 18 grudnia 1998 r. *w sprawie określenia szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją, jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi)* (Dz.U. Nr 161, poz. 1108).



Rys. 3. Stan obecny w zakresie współpracy sufo z państwowymi i samorządowymi formacjami ochronnymi oraz proponowane zmiany

Źródło: J. Służalski, B. Służalska – opracowanie własne.

Pomimo pojawiających się wątpliwości, co do możliwości nawiązywania bezpośredniej współpracy SUFO z Policją i innymi formacjami bezpieczeństwa, jest ona zarówno merytorycznie, jak i prawnie, w pełni uzasadniona (propozycja umieszczona na rysunku 3.). Dziwi zatem i niepokoi fakt, że wyszczególnione, rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 grudnia 1998 r. w sprawie szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją,

jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi), ogólne zasady współpracy, nie powodują utworzenia zintegrowanego systemu zarządzania sprywatyzowaną częścią zadań z zakresu bezpieczeństwa i porządku publicznego. Przecież dopiero harmonijne współdziałanie tych instytucji, dostosowanie środków i metod pracy do nowych wyzwań i zagrożeń wpłynąć może na zwiększenie poziomu bezpieczeństwa przestrzeni miejskich. Potrzebne jest holistyczne, zintegrowane i długofalowe myślenie o bezpieczeństwie, pozwalające na pełne wykorzystanie dostępnych sił i środków, nie tylko formacji państwowych i samorządowych, ale także komercyjnych. Aby to się ziściło, konieczna jest instytucja organizująca i zarządzająca wspólnymi działaniami ochronnymi. Stąd też naczelnym wyzwaniem dla bezpieczeństwa zarówno na poziomie ogólnopaństwowym, jak i lokalnym, jest stworzenie zintegrowanego systemu zarządzania – systemu kierowania siłami i środkami, będącymi w dyspozycji również prywatnych formacji ochronnych. W nich to bowiem skupiony został, na przestrzeni kilkudziesięciu lat, ogromny potencjał osobowy i techniczny, uzbrojenia i wyposażenia, a także – a może przede wszystkim – wiedzy i umiejętności przekazywanych pracownikom ochrony w procesie ich edukacji. Właściwe aktywowanie tego potencjału, wpłynąć może znacząco na poprawę stanu bezpieczeństwa w jego wymiarze personalnym i strukturalnym.

Kolejnym powodem, dla którego istnieje potrzeba skierowania większego wysiłku poznawczego na kwestię zarządzania komercyjnym sektorem ochrony osób i mienia jest konwój wartości pieniężnych. Analiza tych czynności ochronnych, uwidacznia skalę i zakres udziału firm ochrony osób i mienia w zapewnianiu bezpieczeństwa ekonomicznego obywateli i podmiotów gospodarczych. W zdecydowanej większości banków, poza Narodowym Bankiem Polskim i niektórymi Bankami Spółdzielczymi, które konwojują wartości pieniężne, z wykorzystaniem własnych Wewnętrznych Służb Ochrony, usługi te zleca się podmiotom zewnętrznym[22]. Konwój wartości pieniężnych, wykonywany przez SUFO, ma bezpośredni wpływ na funkcjonowanie gotówkowego obrotu na terenie całej Polski. Jest on rozumiany jako wyspecjalizowana forma ochrony mienia, realizowana przez odpowiednio dobraną, posiadającą wewnętrzną strukturę, grupę konwojową, która przemieszcza się po określonej trasie i działa w trakcie realizowania konwoju, zgodnie z wypracowaną i ustaloną taktyką[23]. Konwój wartości pieniężnych, innych przedmiotów wartościowych i niebezpiecznych, powinien spełnić dwa wymagania. Po pierwsze oddziaływać prewencyjnie, czyli poprzez organizację i wyposażenie grup konwojowych, ewentualny zamach na transportowane wartości czynić wysoce ryzykownym

[22] Por.: W. Stawski, Odpowiedzialność podmiotu koncesjonowanego za transport wartości pieniężnych w świetle praktyki. Zob.: http://neostrada.digitalart.pl

[23] Por.: J. Karabin, T. Kowalczyk, *Konwojowanie. Vademecum pracownika ochrony*, Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'Chikara, Lublin 2006, s. 13.

i w konsekwencji mało opłacalnym. Po drugie odeprzeć zamach na konwój oraz bezpiecznie wyprowadzić osoby transportujące oraz mienie ze strefy zagrożonej[24].

Nie wdając się w szczegóły organizacji i zasad funkcjonowania transportu wartości oraz formy obowiązkowej ochrony obszarów, obiektów i urządzeń wykonywanej przez koncesjonowane przedsiębiorstwa ochronne oraz Wewnętrzne Służby Ochrony, należy stwierdzić, że dotyczą one bezpośrednio bezpieczeństwa ekonomicznego obywateli oraz bezpieczeństwa i porządku publicznego na terenie miast. Zatem, w ujęciu ogólnym, zakresem swym obejmują czynności ochronne, tożsame z realizowanymi przez inne podmioty i formacje państwowe, statutowo predestynowane do ochrony życia i zdrowia ludzkiego a także mienia. Stąd też konieczność współdziałania nie budzi wątpliwości. Przedmiotem współpracy komercyjnych służb ochrony z organami państwowymi stać się powinno, takie wykorzystanie rozwiązań organizacyjno-prawnych i zasobów technicznych, pozostających w ich dyspozycji, aby w sposób optymalny zapewnić ochronę życia, mienia oraz dziedzictwa materialnego i kulturowego, przed skutkami przestępstw, klęsk żywiołowych, awarii technicznych i innych społecznie negatywnych zjawisk[25]. Większość z wymienionych zadań stanowić może wspólną płaszczyznę kooperacji formacji państwowych i prywatnych.

Specjalistyczne Uzbrojone Formacje Ochronne oraz agencje ochrony osób i mienia, mogą stanowić również część podsystemu niemilitarnego, który w istotny sposób będzie wpływał na funkcjonowanie podsystemu militarnego, szczególnie w zakresie wspomagania mobilizacyjnego i operacyjnego rozwinięcia sił zbrojnych, uruchamiania zaopatrywania struktur państwowych, ochrony stanowisk kierowania i zapewnienia bezpieczeństwa obywateli[26].

Analiza zarządzania prywatnym sektorem bezpieczeństwa nie byłaby pełna, gdyby, choć ogólnie, nie zostały poruszone kwestie ochrony imprez masowych. Czynności ochronne, podejmowane w zakresie zabezpieczania imprez masowych, stanowią najbardziej rozpowszechnioną formę działań, podejmowanych przez formacje prywatne. Imprezy masowe stanowią również, najbardziej prawdopodobne miejsce potencjalnych zamachów terrorystycznych. Wielkie grupy ludzi, zebranych na niewielkich stosunkowo obiektach, które mogą ulec zniszczeniu w wyniku podłożenia jednego ładunku wybuchowego, to idealny cel dla terrorystów samobójców[27].

Błędnym jest przekonanie, że za bezpieczeństwo podczas imprez masowych odpowiada Policja. Podejmuje ona czynności dopiero w przypadku, gdy działania służb porządkowych okazują się nieskuteczne. A zatem, to na organizatorze tego typu imprez

[24] Szerzej: W. Stawski, *Organizacja konwoju*, Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'Chikara, Lublin 1999, s. 12.
[25] Por.: E. Ura, *Prawne zagadnienia ochrony osób i mienia*, Fosze, Rzeszów 1998, s. 128.
[26] Por.: T. Barański, R. Szklarek, *Specjalistyczne uzbrojone formacje ochronne a bezpieczeństwo państwa* [w:] *Zarządzanie bezpieczeństwem narodowym*, (red.) Ł. Sułkowski, A. Marjański, SWSZPIZ, Łódź 2009, s. 137.
[27] Por.: K. Liedel, *Od Redaktora naczelnego*. Terroryzm, nr 4/2008, s. 1.

spoczywa obowiązek zapewnienia bezpieczeństwa w granicach i czasie jej odbywania. Musi on zadbać o właściwą liczbę[28] odpowiednio przeszkolonej i wyposażonej służby porządkowej[29] i informacyjnej[30]. Dodatkowo, na organizatorze ciąży obowiązek spełnienia wymogów określonych w przepisach prawa, w szczególności w przepisach prawa budowlanego, sanitarnego oraz ochrony przeciwpożarowej. Organizator powołuje również kierownika do spraw bezpieczeństwa oraz zapewnia pomoc medyczną i organizuje zaplecze higieniczno-sanitarne. W jego gestii jest zagwarantowanie właściwej łączności między podmiotami biorącymi udział w zabezpieczeniu imprezy oraz przygotowanie dróg ewakuacji i drogi umożliwiającej dojazd służb ratowniczych. Zapewnia on również podstawowy sprzęt ratowniczy i gaśniczy. Ponadto, na organizatorze spoczywa obowiązek udostępnienia uczestnikom imprezy regulaminu oraz opracowania instrukcji postępowania w przypadkach powstania pożaru lub innego miejscowego zagrożenia, w czasie i miejscu organizowanej imprezy.

Problematyka, związana z zapewnieniem bezpieczeństwa podczas imprez masowych, została określona przede wszystkim w ustawie z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych[31] oraz rozporządzeniu Rady Ministrów z dnia 23 marca 2010 r. w sprawie wymogów, jakie powinni spełniać kierownik do spraw bezpieczeństwa, służby porządkowe i służby informacyjne[32]. Zgodnie z przywoływaną ustawą, głównym zadaniem służb porządkowych jest zapewnienie bezpieczeństwa podczas imprezy masowej. Obowiązek ten realizowany jest przy pomocy nadanych tym służbom uprawnień. Do podstawowych z nich należy: sprawdzanie uprawnień osób do przebywania na imprezie masowej, legitymowanie, przeglądanie zawartości bagażu i odzieży, wydawanie poleceń porządkowych oraz ujęcie osób stwarzających bezpośrednie zagrożenie. Służby porządkowe mają prawo stosować środki przymusu bezpośredniego w postaci siły fizycznej, kajdanek oraz ręcznych miotaczy gazu. Powyższe środki mogą być użyte w sytuacji zagrożenia dóbr powierzonych ochronie, odparcia ataku na członka służb porządkowych i informacyjnych lub inną osobę oraz niewykonania poleceń porządkowych.

[28] Liczbę służb porządkowych i informacyjnych wyznacza proporcja do przewidywanej liczby osób, mogących brać udział w imprezie. I tak na 300 osób przypadać musi nie mniej, niż 10 członków służb i na każde następne 100 osób – 1 pracownik służb. Przy czym, nie mniej, niż 20% ogólnej liczby służb stanowią członkowie służby porządkowej. W przypadku, gdy mamy do czynienia z imprezą o podwyższonym ryzyku (prawdopodobieństwo wystąpienia aktów przemocy i agresji), liczba służb do uczestników imprezy wynosi odpowiednio: 15 członków służb na 200 uczestników oraz 2 na każde następne 100. Przy czym nie mniej niż 50% ogólnej liczby członków służb, stanowią służby porządkowe.

[29] Służba porządkowa – należy przez to rozumieć osoby, podlegające kierownikowi do spraw bezpieczeństwa, wyznaczone przez organizatora, wpisane na listę kwalifikowanych pracowników ochrony fizycznej, o której mowa w art. 26 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 2018 r. poz. 2142 i 2245 oraz z 2019 r. poz. 1495) (art. 3 ust. 13 ustawy o bezpieczeństwie imprez masowych).

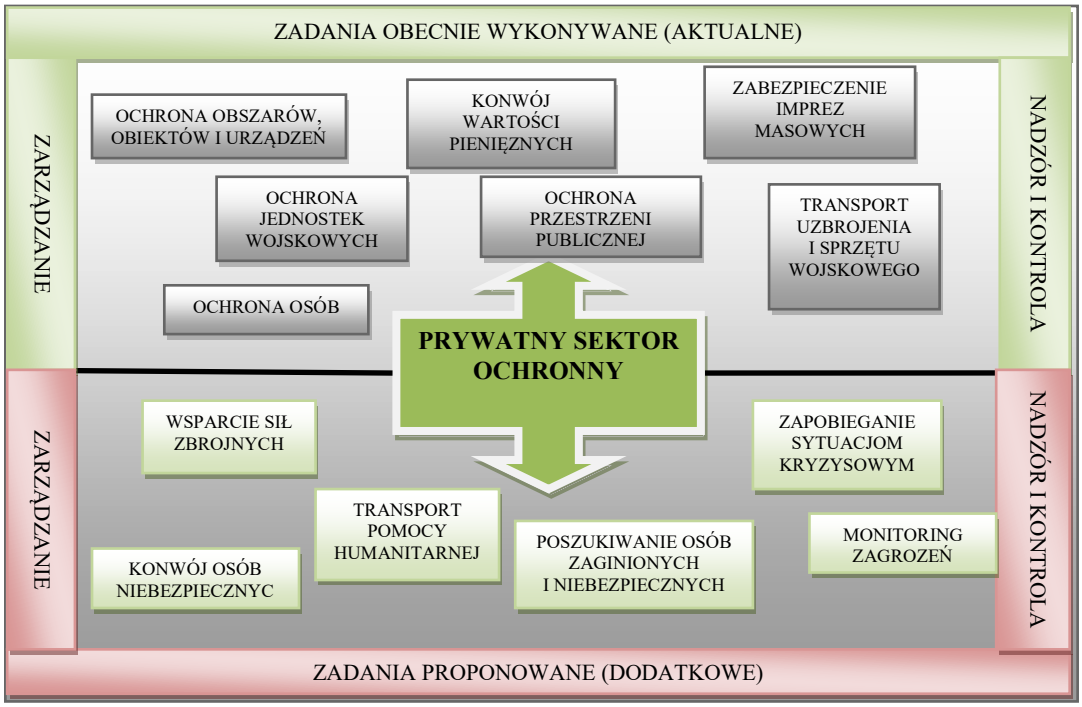
[30] Służba informacyjna – należy przez to rozumieć osoby, podlegające kierownikowi do spraw bezpieczeństwa, wyznaczone przez organizatora, w tym spikera zawodów sportowych (art. 12, ust 12 ustawy o bezpieczeństwie imprez masowych).

[31] Ustawa z 20 marca 2009 r. *o bezpieczeństwie imprez masowych* (Dz.U. Nr 62, poz. 504).

[32] Rozporządzenie Rady Ministrów z 23 marca 2010 r. w sprawie wymogów, jakie powinni spełniać kierownik do spraw bezpieczeństwa, służby porządkowe i służby informacyjne (Dz.U. 2010 Nr 52 poz. 308).

Zarządzanie sprywatyzowaną częścią zadań, dotyczących bezpieczeństwa i porządku publicznego, uwzględniać powinno szereg czynności ochronnych, które obecnie wykonują kwalifikowani pracownicy ochrony fizycznej. Jednakże, biorąc pod uwagę ogromny potencjał tkwiący w sprywatyzowanym sektorze bezpieczeństwa, należy dążyć do jego aktywowania i rozszerzenia komercyjnych czynności ochronnych na inne obszary występowania zagrożeń.

Podsumowaniem, i jednocześnie odpowiedzią na ostatnie pytanie postawione na wstępie, niech będzie rysunek 4.



Rys. 4. Sprywatyzowany sektor ochrony, zadania wykonywane i proponowane

Źródło: B. Służalska, J. Służalski – opracowanie własne.

Rysunek 4. przedstawia płaszczyzny, które mogą wyznaczać możliwe kierunki tworzenia i doskonalenia zintegrowanego systemu zarządzania bezpieczeństwem, w jego wymiarze sprywatyzowanym. Oprócz obecnie wykonywanych zadań przez pracowników ochrony osób i mienia, wskazano na nim także czynności, które mogą być realizowane przez prywatne instytucje ochronne. Wymagają one wprowadzenia skutecznych form zarządzania oraz nadzoru i kontroli państwowej, wywierających pozytywny wpływ na profesjonalizację komercyjnych struktur ochronnych.

Obowiązujące obecnie przepisy, dotyczące ochrony osób i mienia oraz zabezpieczenia imprez masowych, bywają różnie oceniane. Od zagorzałej krytyki

zwolenników bezpieczeństwa, gwarantowanego przez struktury państwowe, po euforię rzeczników prywatyzacji porządku i bezpieczeństwa publicznego. Należy jednak przyznać, że sprywatyzowana część sektora ochrony osób i mienia funkcjonuje, w sposób uregulowany prawnie, od ponad ćwierć wieku, przyczyniając się skutecznie do ochrony wartości ważnych dla bezpieczeństwa państwa i obywateli. Stanowi ona również istotne wsparcie sił policyjnych podczas realizacji zadań ochrony osób i mienia, a także infrastruktury krytycznej państwa. Należy również pamiętać, że warunkiem koniecznym, dla zapewnienia skutecznej obrony Polski, jest dobrze zorganizowane współdziałanie i efektywna integracja potencjału militarnego i pozamilitarnego z odpowiednio przygotowaną administracją i gospodarką oraz zorganizowanym i przygotowanym do obrony społeczeństwem[33]. Stąd też działania zmierzające do poprawy efektywności zarządzania sprywatyzowaną częścią zadań ochronnych stanowią wielkie wyzwanie, nie tylko dla właścicieli koncesjonowanych firm ochrony osób i mienia, ale przede wszystkim dla decydentów w sprawach bezpieczeństwa – w skali lokalnej i całego kraju.

Bibliografia

Barański T., Szklarek R., *Specjalistyczne uzbrojone formacje ochronne a bezpieczeństwo państwa* [w:] Zarządzanie bezpieczeństwem narodowym, (red.) Ł. Sułkowski, A. Marjański, SWSZPIZ, Łódź 2009.

Karabin J., Kowalczyk T., *Konwojowanie. Vademecum pracownika ochrony*, Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'Chikara, Lublin 2006.

Kubiński P., Działalność gospodarcza w zakresie ochrony osób i mienia i jej koncesjonowanie, Wolters Kluwer, Warszawa 2008.

Kulczyński S., *Ochrona obiektów*, Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'Chikara, Lublin 2006.

Liedel K., *Od Redaktora naczelnego*. Terroryzm, nr 4/2008.

Metodyka uzgadniania planów ochrony obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, Warszawa 2016.

Misiuk A., *Administracja porządku i bezpieczeństwa publicznego. Zagadnienia prawno-ustrojowe*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008.

Nowicki Z.T., *Ochrona osób i mienia. Podstawy organizacyjno-prawne*, TNOiK, Toruń 1999.

Ochrona osób i mienia, (red.) M. Enerlich, TNOiK, Toruń 2003.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 18 grudnia 1998 r. *w sprawie określenia szczegółowych zasad współpracy specjalistycznych uzbrojonych formacji ochronnych z Policją, jednostkami ochrony przeciwpożarowej, obrony cywilnej i strażami gminnymi (miejskimi)* (Dz.U. Nr 161, poz. 1108).

Rozporządzenie Rady Ministrów z 23 marca 2010 r. *w sprawie wymogów, jakie powinni spełniać kierownik do spraw bezpieczeństwa, służby porządkowe i służby informacyjne* (Dz.U. 2010 Nr 52 poz. 308).

Stawski W., *Odpowiedzialność podmiotu koncesjonowanego za transport wartości pieniężnych w świetle praktyki*. Zob.: http://neostrada.digitalart.pl

Stawski W., *Organizacja konwoju*, Wydawnictwo Policealnej Szkoły Detektywów i Pracowników Ochrony O'Chikara, Lublin 1999.

Ura E., *Prawne zagadnienia ochrony osób i mienia*, Fosze, Rzeszów 1998.

Ustawa z dnia 20 marca 2009 r. *o bezpieczeństwie imprez masowych* (Dz.U. 2009 nr 62 poz. 504 z późn. zm.).

Ustawa z dnia 22 sierpnia 1997 r. *o ochronie osób i mienia* (Dz.U. z 1997 r., Nr 114, poz. 740, z późn. zm.).

Ustawa z dnia 24 maja 2013 r. *o środkach przymusu bezpośredniego i broni palnej* (Dz.U. 2013 poz. 628 z późn. zm.).

Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz.U. 2007 Nr 89 poz. 590 z poźn. zm.).

[33] Por.: T. Barański, R. Szklarek, *Specjalistyczne uzbrojone*…dz. cyt., s. 148.

Serhiy Stasevych[1]
Mariia Ruda[2]
Olha Kuz[3]
Mykhailo Paslavskyi[4]
Taras Boyko[5]

Information Security In Internet Communications

Streszczenie

Żyjemy w czasach globalnej informatyzacji wszystkich procesów gospodarki światowej, w tym w sferach życia gospodarczego i społecznego Ukrainy. Sfera informacyjna ma bardzo silny wpływ na stan politycznego, gospodarczego, obronnego i innych elementów bezpieczeństwa narodowego Ukrainy. W dzisiejszym świecie toczy się ciągła walka o kontrolę nad przepływami informacji. Wygrywa ten, kto nie tylko kształtuje przepływy i umie regulować je we własnym interesie, ale także potrafi zapewnić integralność swojego zasobu informacyjnego, chronić go przed zewnętrznymi, czasem wrogimi wpływami. Podstawą współczesnego społeczeństwa jest technologia informacyjna i informacja, która stała się towarem i głównym produktem produkcji i tworzenia wartości. Współczesny człowiek zanurzony jest w świecie technologii informacyjnych, otoczony ogromną ilością informacji, często negatywnych. Coraz więcej danych osobowych obywateli pozostaje na stronach internetowych różnych instytucji, organizacji itp. Komunikacja informacyjna ludzi z prawdziwego życia coraz częściej przenosi się do sfery online (wideo, audio, multimedia).

Problem bezpieczeństwa informacji stał się dotkliwy wraz z utworzeniem jednolitej przestrzeni informacyjnej, w której gromadzi się, przetwarza, przekształca, przechowuje

[1] Assoc. Prof. Serhiy Stasevych, Lviv Polytechnic National University, Lviv, Ukraine.
[2] Dr Mariia Ruda, Lviv Polytechnic National University, Lviv, Ukraine.
[3] Dr Mariia Ruda, Lviv Polytechnic National University, Lviv, Ukraine
[4] Dr Mykhailo Paslavskyi, Ukrainian National Forestry University, Lviv, Ukraine
[5] Prof. Taras Boyko, Lviv Polytechnic National University, Lviv, Ukraine

i wymienia informacje. Wynika to z następujących czynników: wzrost liczby urządzeń komputerowych i komunikacyjnych; tworzenie i zwiększanie wykorzystania systemów informacji i zarządzania; potrzeba zautomatyzowanego przetwarzania dużych zbiorów danych; wzrost strat (reputacyjnych i finansowych) spowodowanych zniszczeniem, fałszowaniem, ujawnieniem lub nielegalnym powielaniem informacji; różnego rodzaju zagrożenia i kanały nieuprawnionego dostępu do informacji. We współczesnym społeczeństwie informacja staje się najważniejszą wartością, a branża odbioru, przetwarzania i rozpowszechniania informacji – wiodącą branżą, w którą z roku na rok inwestuje się coraz więcej kapitału. Według naukowców informacja staje się ważnym zasobem strategicznym, którego brak prowadzi do znacznych strat w gospodarce. Informatyzacja społeczeństwa jest jednym z decydujących czynników modernizacji gospodarki na zasadach rynkowych i kluczem do integracji Ukrainy ze społecznością światową.
Słowa kluczowe: Bezpieczeństwo informacji, bezpieczeństwo komunikacji internetowej, ochrona informacji, bezpieczeństwo systemów informatycznych, komunikacja internetowa.

Abstract

We live in a time of global informatization of all processes of the world economy, including in the spheres of economic and social life in Ukraine. The information sphere has a very strong influence on the state of political, economic, defense and other components of Ukraine's national security. In the modern world there is a continuous struggle for control over information flows. The winner is the one who not only forms the flows and knows how to regulate them in his own interests, but also is able to ensure the integrity of his information resource, to protect it from external, sometimes hostile, influence. The basis of modern society is information technology and information that has become a commodity and the main product of production and value creation. Modern man is immersed in the world of information technology, surrounded by a huge array of information and often negative. More and more personal data of citizens remain on the websites of various institutions, organizations, etc. Information communication of people from real life is increasingly moving into the field of online (video, audio, multimedia).

The problem of information security has become acute with the creation of a single information space in which the accumulation, processing, transformation, storage and exchange of information. The problem of information security has become acute with the creation of a single information space in which the accumulation, processing, transformation, storage and exchange of information. This is due to the following factors: an increase in the number of computer facilities and communications; creation and increasingly widespread use of information and management systems; the need for automated processing of large data sets; increase in losses (reputational and financial) from destruction, falsification, disclosure or illegal reproduction of information; a variety of types of threats and channels of unauthorized access to information. In modern society, information is becoming the most important value, and the industry of receiving, processing and broadcasting information - the leading industry, where every year more and more capital is invested. According to leading scientists, information is becoming an important strategic resource, the lack of which leads to significant losses in the economy. Informatization of society is one of the decisive factors in modernizing the economy on a market basis and the key to Ukraine's integration into the world community. Informatization of society is one of the decisive factors in modernizing the economy on a market basis and the key to Ukraine's integration into the world community.
Keywords: Information security, security of Internet communication, protection of information, security of information systems, Internet communications.

Introduction

The world is moving step by step towards the creation of an information society in which new production systems also require a qualitatively new system of human relations. The new model of society, which is related to the concept of information, also requires a significant rethinking of our ideas about the essence of the development of human civilization. To do this, we need to look at the history of mankind from a new angle, namely: not as a process of finding new and more efficient means of production, but as a process of finding new and more effective means of communication.

Communication is a very complex and multidimensional phenomenon that has a universal character. Here we will only outline the idea of communicative construction of society as the most essential structure that determines its sphere of production, stereotypes of thinking, social behavior. Suffice it to mention that our society for many years was fundamentally anti-communicative. It was built according to the principles of a rationally operating machine, where everyone was given the role of a cog, which was easy to replace with another, the main thing is that the machine as a whole worked. In a society built on the principles of communication, man is no longer a cog, but a major figure in the production and transformation of information. Society then is not a machine, but a flexible system of diverse and multidimensional communication structures. Obviously, the value of the human person in this society is growing significantly, and the higher it is, the richer a person is spiritually and intellectually.

At the same time, today, the means of communication is becoming more important than the message. That is, the content of information depends primarily on what channel it is transmitted – radio, television, newspapers, Internet.

Informatization of all processes in the state has not only a positive side, but also a negative one: the use of computer technology for illegal, anti-social, criminal purposes. Studies have shown that cybercrime in the world is growing, penetrating the computer information space, and creating new ways to create cybercrime.

It should be noted that currently there is no universal integrated system of information systems protection; but there are separate components of information security systems that each entity uses to ensure its security objectives; to ensure reliable protection it is necessary to use a range of organizational and managerial, organizational and technical and organizational and legal measures, tools, methods.

Even the world's largest companies fall victim to cybercriminals who steal corporate data using various schemes to hack corporate databases and devices. One of these schemes works due to non-compliance by campaign employees with the rules of safe work with corporate resources. Thus, in March 2021, the California Financial Control Service (USA) was subjected to a phishing attack, as a result of which the identification data of several thousand customers were in the hands of a hacker.

Human information security in this context is not only the protection of intellectual property rights, but also the right to free access to information, free dissemination of information, protection of personal data from unauthorized access.

The concept of information security means the state of protection of the information environment of society, which ensures its formation, use and development in the interests of citizens, organizations, the state and the protection of entities from negative information action. In turn, the information environment means the sphere of activity of state entities related to the creation, transformation, dissemination and consumption of information.

The information environment can be divided into the following components: a) the production of information technology and information services; b) information market – the formation of information resources, preparation of information products, provision of information services; c) consumption of information; and most importantly, without which the information environment cannot function d) information and telecommunication systems of information dissemination. All state entities that use information must have an information culture – the ability to effectively use information resources and means of information communication. The main factors shaping the information culture of modern society:

a) the education system, which determines the general level of intellectual development of people, their material and spiritual needs;
b) the information infrastructure of society, which determines the ability of people to receive, transmit and use the necessary information;
c) democratization of society, which determines the legal guarantees for access to sources of information of the internal and external market;
d) the development of the country's economy, on which depend the material opportunities for people to obtain the necessary education, as well as the acquisition and use of modern means of telecommunications.

In the information society, a person must: In the information society, a person must:

– have various technical means to search for information and information technologies (software for creation, processing, storage, transfer of information);
– be able to formulate their need for information and search for it in the whole set of information resources;
– be able to adequately select and evaluate the quality of information, process information.

Considering information security as a state of information security, then, security issues can be grouped by the following types:

– humanitarian, which occurs in the case of uncontrolled use and dissemination of personal data, invasion of privacy, libel, etc.;
– economic and legal, which arise in case of leakage, distortion and loss of commercial and financial information, theft of intellectual property, industrial espionage, etc.;
– political, arising from information wars, attacks on information systems of important defense, transport, industrial facilities of the state, etc.

Analysis of the literature

The culture of information security in [1] is defined as a way of organizing and developing an information society that provides a quality information environment (quality of information consumed, protection of the subject from negative information actions), creates an opportunity to fully meet the information needs of the subject, and the subject is aware of himself as a subject of information security, able to detect threats, has technologies to protect against them, adheres to the rules of information ethics in the process of transforming the information environment.

Separately, the author highlights the concept of 'culture of information self-defense'. It comprehensively combines the features of the material and ideal worldview of the individual, which form his information culture in terms of culture of information and professional competence, and in terms of culture of information security.

The culture of information self-defense is characterized by those features of the information culture of the individual, which determine the ability to handle information without harming themselves and other participants in information relations; the ability to withstand information threats and maintain mental health in the face of negative information. It is formed throughout a person's life in the process of continuous learning, education and self-education, which contributes to the high level of information culture and literacy of society.

The classification of information security threats can be carried out as follows: threats of information leakage; threats of violation of information integrity; threats of blocking information. The diversity of classifications in the current legislation is due not only to different approaches to the choice of classification features and purposes of classification, but also the lack of proper theoretical justification of the nature of information security threats [2, 3].

A. Loginov offers the same list of threats to information security in his own dissertation research. In particular, he defines threats as: disclosure of information resources; violation of the integrity of information resources; equipment failure [4].

In turn, S. Gutsu [5] and O. Litvinenko [6] agree that the main threats to information security can be presented as follows:

- threats of influence of low-quality information (unreliable, false, misinformation) on the person, society, the state;
- threats of unauthorized and illegal influence of outsiders on information and information resources (their production, system of formation and use);
- threats to the information rights and freedoms of the individual (the right to produce information, its dissemination, search, receipt, transmission and use; the right to intellectual property to information, including material).

Until 2016, the main attention was paid to the technical protection of information, the Doctrine of Information Security of Ukraine [7], adopted in 2017, shifted the emphasis to protection against information expansion by the aggressor state.

In the same context, we can provide a broader classification proposed by A. Pogrebnyak [8], who notes that threats can be both accidental and intentional.

Accidental threats include:

- errors of staff and users;
- loss of information due to improper storage;
- accidental destruction or replacement;
- failure of equipment, power supply, disk systems, network components;
- incorrect operation of the software, in particular due to infection with computer viruses, etc.

Intentional threats include:

- unauthorized access to information and network resources;
- disclosure and modification of data and programs, their copying;
- disclosure, modification or substitution of computer network traffic;
- development and distribution of computer viruses, introduction of logic bombs into software;
- theft of magnetic carriers and settlement documents;
- destruction of archival information or its intentional destruction;
- falsification of messages, refusal of the fact of receiving information or change of time of its reception;
- interception and acquaintance with the information which is transferred on communication channels.

Summarizing the above, we can conclude that the approach to understanding the essence of information security for different categories of entities may differ significantly, for example, the security of ordinary citizens and government officials, the security of different enterprises and companies. Therefore, it is quite logical and noteworthy to classify threats that have a narrower, or in other words special character, in particular, threats to information security of network resources. As a criterion, you can use the way to influence the information or ways to implement threats to information.

Research results

Measures to ensure the security of information systems can be divided into: regulatory (legislative), moral and ethical, organizational (administrative), physical and technical (hardware and software).

The normative-legal measures of protection include the laws in force in the state, decrees and regulations, which regulate the rules of information circulation, enshrine the

rights and responsibilities of participants in information relations in the process of its processing and use, and establish liability for violations of these rules, thereby preventing the misuse of information and is a deterrent to potential violators.

The moral and ethical measures of counteraction include norms of behavior, which are traditionally formed as information in the country or society increases. These norms are generally not binding, as legally approved regulations, but their non-compliance usually leads to a decline in the authority, prestige of a person, group of persons or organization. Moral and ethical norms are both unwritten (for example, generally accepted norms of honesty, patriotism, etc.) and written, ie framed in some statute of rules or regulations.

Organizational (administrative) protection measures are organizational measures that regulate the functioning of the data processing system, the use of its resources, staff activities, as well as the order of user interaction with the system so as to make it most difficult or impossible to implement security threats.

Physical protection measures are based on the use of various mechanical, electronic or electromechanical devices and structures specifically designed to create physical barriers to possible penetration and access of potential intruders to the components of the system that protect information, and also technical means of visual supervision, communication and the security alarm system.

Technical (hardware and software) security measures are based on the use of various electronic devices and special programs that are part of automated systems and perform (alone or in combination with other means) security functions (identification and authentication of users, delimitation of access to resources, event registration, cryptographic closure of information, etc.).

The basic principles of information security of our citizens are laid down in the articles of the Constitution of Ukraine [9]:

17. '…Protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the affair of the entire Ukrainian people…'

31. 'Everyone is guaranteed the secrecy of correspondence, telephone conversations, telegraph and other correspondence. Exceptions may be established only by a court in cases provided by law, in order to prevent crime or find out the truth during a criminal investigation, if otherwise impossible to obtain information.'

32. '…The collection, storage, use and dissemination of confidential information about a person without his or her consent is not permitted, except as provided by law, and only in the interests of national security, economic well-being and human rights…'

34. 'Everyone is guaranteed the right to freedom of thought and speech, to freely express their views and beliefs. Everyone has the right to freely collect, store, use and disseminate information orally, in writing or otherwise – of their choice…'

50. '…Everyone is guaranteed the right of free access to information on the state of the environment, the quality of food and household items, as well as the right to its dissemination. Such information may not be classified by anyone.'

As can be seen from the above articles of the Constitution, the state guarantees the citizens of Ukraine the protection of confidential information of a person, the right to collect, store, use and disseminate information in an arbitrary manner. The Law of Ukraine 'On Information' regulates the relations of citizens of Ukraine on the creation, collection, receipt, storage, use, dissemination, protection, defense of information [10].

Article 1 of the Law stipulates that 'information – any intelligence and / or data that can be stored on physical media or displayed electronically', and 'information protection – a set of legal, administrative, organizational, technical and other measures, ensuring the safety, integrity of information and proper access to it.' Article 2 of the Law establishes the basic principles of information relations: 'guaranteed right to information; openness, availability of information, freedom of information exchange; reliability and completeness of information; freedom of expression and belief; legality of receiving, using, disseminating, storing and protecting information; interference in her personal and family life.' Section II of the Law classifies information by content, in particular Article 11 deals with information about an individual:

"1. Information about an individual (personal data) – information or a set of information about an individual who is identified or can be specifically identified.

2. The collection, storage, use and dissemination of confidential information about a person without his or her consent is not permitted, except in cases specified by law and only in the interests of national security, economic well-being and protection of human rights. Confidential information about an individual includes, in particular, information about his or her nationality, education, marital status, religious beliefs, state of health, as well as address, date and place of birth.

Everyone shall have free access to information concerning him or her personally, except as provided by law."

Articles 22 and 23 of the Law introduce the concepts of mass information and its means, information products and information service:

Article 22. 'Mass information and its means

1. Mass information – information that is disseminated in order to bring it to an unlimited number of people.
2. Mass media – means intended for public distribution of printed or audiovisual information.

Article 23. Information products and information service

1. Information products – a materialized result of information activities, designed to meet the needs of the subjects of information relations. An information service is an activity of providing information products to consumers in order to meet their needs.

2. Information products and information services are objects of civil law relations governed by the civil legislation of Ukraine.'

As can be seen from the above articles in the Law 'On Information', citizens of Ukraine have the right to create, collect, receive, store, use, distribute information products and information services. The concept of confidential information is introduced.

Other laws of Ukraine prescribe rules for the protection of information in the process of its creation, processing and transmission, for example, the Law of Ukraine 'On protection of information in information and telecommunications systems' [11].

Article 1 of this Law states:

– protection of information in the system - activities aimed at preventing unauthorized actions regarding information in the system;…
– complex system of information protection – an interconnected set of organizational and engineering measures, means and methods of information protection;
– cryptographic protection of information – a type of information protection implemented by converting information using special (key) data in order to hide / restore the content of information, confirm its authenticity, integrity, authorship, etc.;
– technical protection of information - a type of information protection aimed at ensuring with the help of engineering measures and / or software and hardware means to prevent leakage, destruction and blocking of information, violation of the integrity and mode of access to information."

The State Standard of Ukraine DSTU 3396.0-96 'Information protection. Technical protection of information. Basic provisions" [12] provides possible ways to implement information threats:

3.1 The object of technical protection is information that is a state secret or other secret provided by the legislation of Ukraine, or confidential information that is state property or transferred to the state in possession, use, disposal (hereinafter – information with limited access, IwLA).

3.2 The object, purpose and tasks of technical protection of information are defined and established by the persons who own, use, dispose of IwLA within the rights and powers granted by the laws of Ukraine, bylaws and regulations of the system of technical protection of information.

3.3 Carriers of IwLA can be physical fields, signals, chemicals that are formed in the process of information activities, production and operation of products for various purposes (hereinafter – information activities).

3.4 The medium of distribution of IwLA carriers can be communication lines, signaling, control, power networks, terminal and intermediate equipment, engineering communications and constructions, enclosing building constructions, and also light-transmitting elements of buildings and constructions (openings), air, water and other environments, soil, vegetation, etc.

3.5 Leakage or violation of the integrity of IwLA (distortion, modification, destruction) may be the result of the implementation of information security threats (hereinafter - the threat) ...

4.1.3 Threats may be carried out by: – technical channels, including channels of spurious electromagnetic radiation and interference, acoustic, optical, radio, radio engineering, chemical and other channels;

– channels of special influence by formation of fields and signals for the purpose of destruction of system of protection or violation of integrity of the information;

– unauthorized access by connecting to equipment and communication lines, disguise as a registered user, overcoming protection measures for the use of information or imposing false information, the use of embedded devices or programs and the introduction of computer viruses.'

This State Standard stipulates that information carriers are physical fields, signals, chemicals that are formed in the process of information activities, production and operation of products. And the medium of distribution of information carriers can be communication lines, alarms, control, power networks, network equipment, utilities and buildings, as well as translucent elements of buildings and structures (windows), air, water and other environments. That is, those elements of the environment from which different types of receivers can illegally remove information.

Resolution of the Cabinet of Ministers of Ukraine 'Rules for ensuring the protection of information in information, telecommunications and information-telecommunications systems' [13] states that to ensure the protection of information in the system creates a comprehensive system of information protection, which is designed to protect information from:

– leakage by technical channels, which include channels of spurious electromagnetic radiation and guidance, acoustic-electric and other channels formed under the influence of physical processes during the operation of information processing facilities, other technical means and communications;
– unauthorized actions with information, including the use of computer viruses;
– special influence on the means of information processing, which is carried out by the formation of physical fields and signals and can lead to a violation of its integrity and unauthorized blocking.

The state standard of Ukraine 'Information protection. Technical protection of information. Terms and definitions' introduces terms related to information security [14]:

Thus, paragraph 5 'Threat to information' contains the following definitions:

– information leakage – uncontrolled dissemination of information that leads to its unauthorized receipt.
– violation of the integrity of information – distortion of information, its destruction.
– blocking of information – impossibility of the authorized access to the information.

The definition of the general purposes of information protection should be approached from the standpoint of protection of interests and legal rights of the subjects of information relations. It is always necessary to remember that it is necessary to protect the subjects of information relations, because in the end it is them, and not the information itself or its processing systems can be damaged. In other words, the protection of information and its processing systems is a secondary task. The main task is to protect the interests of the subjects of information relations. This placement of emphasis allows you to correctly determine the security requirements for specific information and its processing systems.

According to the possible interest of different subjects of information relations, there are four main ways to harm them through various influences on information and its processing systems:

- confidentiality violation (disclosure) of information;
- violation of the integrity of information (its complete or partial destruction, distortion, falsification, misinformation);
- violation (partial or complete) system operability. Failure or unauthorized modification of the components of the information processing system, their modification or substitution may lead to incorrect calculation results, system failures from the flow of information (non-recognition of one of the interacting parties of the transmission or reception of messages) and / or refusals to service end users ;
- unauthorized duplication of open information (non-confidential), such as programs, databases, various documents, literary works, in violation of the rights of information owners, copyright, etc. Information, having the properties of material objects, has such a feature as the inexhaustibility of the resource, which significantly complicates the control over its replication.

The main organizational measures that must be considered when creating a comprehensive information security system of a certain structure:

1. Only authorized users should have access to information and software in the information system.
2. Develop a procedure for administering passwords to different systems.
3. Develop authorization procedures for different users to different information systems.
4. Use organizational measures and software and hardware to restrict access to files with data only authorized users.
5. Access to computer resources, obtaining permission to access information and software, and obtaining a password requires the permission of the appropriate manager.
6. Unfold the monitor screens so that they are not visible from doors, windows and places in uncontrolled areas.

7. To involve information security testing specialists to assess information security systems.
8. Provide for physical security measures (locks, passes for staff, fencing, security, etc.).
9. Provide procedures for escorting outsiders by authorized employees.
10. Ensure that electromagnetic radiation from computers does not penetrate outside the premises.
11. Protect all storage media, provide access to work with them to authorized users.
12. Develop an action plan to ensure the smooth operation of staff in emergencies.
13. Register, collect, store, process and issue information about all events occurring in the system and related to its security.

Citizens of the state must be able to consume information, learn to think critically, to compare and analyze information obtained from various sources of communication. Because the perception of all the information by faith can cause a person cognitive dissonance.

One of the first researchers of influence electronic means of dissemination of information was the Canadian philosopher Marshall McLuhan.

Marshall McLuhan's book 'Understanding Media: The Extensions Of Man' [15] was one of the first studies in the field of media ecology. According to McLuhan, the media should become objects of study in themselves, regardless of their content (content). The basic idea is that the mass media (communication) influences society primarily not by its content, but by the characteristics that distinguish it from other media. The simplest media is electric light, which creates the environment through a simple presence. 'Electric light is pure information. It is, so to speak, a means of communication without message.'

Electric light does not contain any content, but nevertheless allowed people to take advantage of the night and made the economic activities of modern society around the clock. Similarly, television, radio, newspapers and other media have a huge and unpredictable impact on the development of society the very fact of its existence. However, these effects go unnoticed because researchers are primarily interested in the nature of the messages transmitted. The need to study the hidden media effects McLuhan formulated in the form of the famous saying 'The means of transmitting the message itself is the message' (The Medium is the Message) [15].

According to McLuhan, all media can be divided into two large groups. The main criterion for classification is the level of consumer involvement in the communication process. Information that is transmitted through different media requires different degrees of consumer involvement. Since the main result of information consumption is the extraction of content, distinguish between media that provide information in a convenient form that does not require additional effort to comprehend, and inconvenient, which requires additional effort from the consumer of information.

Television is certainly a convenient form of information consumption, when the viewer is provided with maximum comfort and convenience. But books (especially scientific) are certainly not comfortable carriers of information that require maximum attention from the reader and additional imagination. Thus, there are 'hot' media, which involve the maximum number of mechanisms of perception (audiovisual), and 'cold' media, which use one, maximum two ways of transmitting information and force the recipient to strain the imagination to 'guess' the meaning of information. As an example of the first type of media, we can cite the already mentioned television, and as the second – also the mentioned books.

To ensure a culture of information security of society, it is necessary to provide a way of learning and development of members, especially children and youth.

On January 19-20, 2021, the Ministry of Digital Transformation of Ukraine together with the Ministry of Internal Affairs with the support of the Advisory Mission of the European Union and the International Telecommunication Union held an international conference on the results of last year's 'Safe Online 2020: Modern Challenges' [16]. It was attended by leading international experts on Internet security, including the British partners Internet Watch Foundation, the Australian eSafety Commissioner, UN agencies, the UN Special Rapporteur and Ukrainian NGOs.

Lectures and panel discussions on the following topics were conducted:

- modern dangers of the Internet and ways to combat them;
- ways to build a more secure online space in Ukraine;
- the impact of pornography on the consciousness of children and adults;
- sexual violence in the digital environment;
- blocking of materials and problems with the legislation;
- Artificial Intelligence;
- tips for parents on the safety of children on the Internet;
- disinformation and fakes.

Here are some speeches from this conference.

- Mykhailo Fedorov, Deputy Prime Minister – Minister of Digital Transformation of Ukraine: 'Online security is one of the strategic priorities of the Ministry of Digital Transformation. We are implementing a comprehensive approach in this direction – such as creating and implementing concepts that will strengthen online security in the country. We with the Ministry of Internal Affairs hold a large-scale international conference, which covers all aspects of online security. This is a platform where they are looking for ways to make the digital environment safe for Ukrainians, taking into account the world experience.'
- Tetyana Kovalchuk, Deputy Minister of Internal Affairs of Ukraine: 'Today the state is uniting its efforts to protect human security online. The Ministry of Internal Affairs raises this issue to the level of state policy, introduces new standards of law

enforcement, putting people and their safety to the forefront of the security system and nomocracy'.

- Antti Hartikainen, Head of the European Union Advisory Mission (EUMC) in Ukraine: 'Cyberspace has no borders, as do cybercriminals. However, law enforcement is limited by the borders of its state, and this is a challenge. Unfortunately, cybercriminals and cybergroups are well aware of these limitations. That's why education and awareness raising are so important.'
- Dorin Bogdan-Martin, Director of the International Telecommunication Union: "The COVID-19 pandemic has shaken the world and the pace of society, while setting new standards of living in a new normal. 'This unprecedented transition is based on our children and young people. As a specialized UN agency on ICT, ITU is committed to supporting the work of the Government of Ukraine and all our members in ensuring safe, sustainable and inclusive cyberspace.'

On February 8, 2022, the world celebrates Safer Internet Day [17] under the slogan 'Together for the best Internet'. Safer Internet Day (SID) was launched by Insafe and INHOPE with the support of the European Commission to promote the safe and positive use of digital technologies, especially by children and young people. The Center for the Best Internet is represented by the National Committee for Safer Internet Day in Ukraine.

This day is held to involve everyone who has a role to play in creating a better Internet for all, including the youngest users. Moreover, it is an invitation for everyone to respectful online communication to provide the best digital experience. Safer Internet Day provides a unique opportunity to conduct online security events together with the whole world: in an educational institution, library, public organization, as well as in government agencies and business organizations. Every year more and more organizations join the Safer Internet Day in Ukraine, as well as all over the world. The Center for the Best Internet invites you to join the joint celebration of this day in Ukraine in your family, educational institution, city, organization, country, world.

The textbook 'Guide to socio-pedagogical support for the formation of safe behavior of adolescents on the Internet' [18] contains detailed exercises and information materials to cover the topic of safe behavior on the Internet in professional activities with children, youth and professional communities. The manual also contains theoretical material on safe behavior on the Internet, a description of classes and training exercises on the development of competencies of safe behavior on the Internet: 'Respect for human rights online'; 'Participation online'; 'Maintaining health when working with digital devices'; 'Appeal for help and protection'.

Exercises can be used separately or adapted to the needs of the target audience – children, youth, parents and / or their substitutes, educational and library communities, employees of youth, social, law enforcement. The manual 'Caution. Vigilance. Protection. Politeness. Courage' [19] contains lesson plans for primary school students and focuses on

the key principles of network etiquette and safety. Classes are offered in five topics: prudence on the Internet, vigilance on the Internet, protection on the Internet, friendliness on the Internet, courage on the Internet. The Handbook for Parents 'Clan Click-Click. Raising Children in the Digital Age' [20] provides in an accessible form the necessary information and advice that will be useful to parents to promote the positive use of digital technologies by children. The Center for Better Internet [21] was established to promote the safe use of digital technologies, development and support of the information and digital society, promotion of culture and security of Internet use. Priorities of the Center for the Best Internet 2019-2021: research of citizens' attitudes to safe behavior on the Internet; Involvement of children and youth in planning activities for safe behavior on the Internet and the opportunity to choose those topics that need to be considered in the context of safe Internet; inclusion - helping families with children with disabilities to protect the child from threats and use the Internet for its development and recreation; participation in the Internet management forum; coordination of Safer Internet Day in Ukraine.

In 2020, the Center for Better Internet will become a participant in the Safer Internet Center (SIC) + Program Better Internet for Kids (BIK) project. The Best Internet for Children portal provides information, guidance and resources on improving Internet issues from Insafe-INHOPE's shared network of safe Internet centers in Europe and other key parties.

Conclusions

As we see, the information security of a citizen, enterprise, company, government agency, public authorities is not so much in the technical protection of information systems, but as in the moral, ethical and organizational training of citizens and employees of all institutions.

In modern conditions Information security not only gives a citizen the right to free access to information, free dissemination of information, protection of personal data from unauthorized access, but also the state of protection of the information environment of society from negative information influences on its citizens.

The state should form an information culture through the education system in preschool and school educational institutions. It must be acknowledged that the Internet has become a significant factor in the socialization of not only adults but also children and adolescents, and that the Internet is an important and integral part of the life of a modern child, a space for most fundamental rights of the child. The current generation of young people is more receptive to multimedia information (video, audio, graphics, text) through the WWW (World Wide Web) and more aware of it than with the usual visual re-reading of textual information.

It is impossible and not necessary to completely limit access to cyberspace. Lots of developing useful information, literature, music and just communication of interests,

communication with relatives and friends – all this can be found on the Internet. It is enough to know the rules of safe behavior to ensure personal safety on the Internet for both adults and school-age children.

You need to learn the rules that will help you work safely on the Internet:

- remember that you communicate with a person on the Internet,
- put yourself in the place of a person, with whom you speak
- defend your point of view, but do not offend your interlocutors,
- when you use telecommunications networks, then you are dealing with a monitor screen. Words, and only words – this is all that your interlocutor sees when communicating in the messenger. When you communicate on the Internet, you can easily make a mistake in interpreting the words of your interlocutor. When you connect with someone, remember that your words are fixed,
- adhere to the communication ethics,
- respect the time and opportunities of others. There is a stereotype that today people have less and less time, and the creation of new devices can save time. When you send an e-mail or communicate on the Internet, you are actually claiming someone's time. And then you are responsible for ensuring that the recipient does not spend this time in vain.

References:

Chernykh O.O. Onlaik: navchalno-metodychnyi posibnyk., K.: VAITE, 2020. – 108 s. URL: https://www.osce.org/files/f/documents/0/f/483533.pdf.

Doktryna informatsiinoi bezpeky Ukrainy, zatv. Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku № 47/2017 URL: http://www.president.gov.ua/documents/472017-21374.

Hutsu S.F. Pravovi osnovy informatsiinoi diialnosti: Navch. posibnyk Kh.: Nats. Aerokosm. Un-t «Khark. aviats. in. -t», 2009.

Klan Klits-Klats. Vykhovannia ditei v tsyfrovu eru. URL: https://edpro.ua/blog/informacijna-bezpeka.

Konstytutsiia Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy, 1996, № 30.

Lohinov A. V. Administratyvno-pravove zabezpechennia informatsiinoi bezpeky orhaniv vykonavchoi vlady: dys. kan. yur. nauk za spets-tiu 12.00.07 / Nats. akad. vnutr. sprav Ukrainy. K., 2005.

Lytvynenko O. Problema informatsiinoi bezpeky v konteksti mihratsiinykh protsesiv. URL: http://www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf.

McLuhan, Herbert Marshall. Understanding Media: The Extensions Of Man. 1st Ed.: McGraw Hill, 1964; Reissued by MIT Press, 1994.

Obachnist. Pylnist. Zakhyst. Vvichlyvist. Smilyvist. Posibnyk iz tsyfrovoho hromadianstva y bezpeky. URL: https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf.

Panchenko O.A., Panchenko L.V. Informatsiina bezpeka ta informatsiina kultura v suchasnomu informatsiinomu suspilstvi //Pravova informatyka. 2015. № 2(46).

Pohrebniak A.V. Tekhnolohii kompiuternoi bezpeky: Monohr. Rivne: MEHU, 2011.

Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh : Postanova Kabinetu Ministriv Ukrainy vid 29.03.2006 r. № 373. Ofitsiinyi visnyk Ukrainy. 2006. № 13

Sait "Krashchyi Internet dlia ditei". URL: https://www.betterinternetforkids.eu/en-GB/home.

Sait Den bezpechnoho Internetu. URL: https://www.saferinternetday.org/.

Sait Ministerstva ta Komitetu tsyfrovoi transformatsii Ukrainy. URL: https://thedigital.gov.ua/news/mizhnarodna-konferentsiya-pro-bezpechniy-onlayn-vid-mintsifri-ta-mvs.

Sait Tsentru krashchoho Internetu. URL: https://betterinternetcentre.org/.

Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia: DSTU 3396.0-96. Vydannia ofitsiine. Kyiv, Derzhstandart Ukrainy, 1996.
Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia: DSTU 3396.2-97. Vydannia ofitsiine. Kyiv, Derzhstandart Ukrainy, 1997.
Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh" Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1994, № 31.
Zakon Ukrainy “Pro informatsiiu” // Vidomosti Verkhovnoi Rady, 1992, № 48.
Zolotar O.O. Informatsiina bezpeka liudyny: teoriia i praktyka: monohrafiia. – Kyiv: TOV «Vydavnychyi dim «ArtEk», 2018.
Zolotar O.O., Trubin I.O. Klasyfikatsiia zahroz informatsiinii bezpetsi. Informatsiia i pravo. 2013. № 3(9).

Grzegorz Zając

Mariusz Stachowicz[1]

Prawne i instytucjonalne aspekty bezpieczeństwa w cyberprzestrzeni. Ujęcie międzynarodowe i krajowe

Streszczenie

Bezpieczeństwo w cyberprzestrzeni stanowi jedno z poważniejszych zagadnień współczesnych państw i organizacji międzynarodowych. Podejmuje się wiele wspólnych działań na rzecz walki z zagrożeniami w cyberprzestrzeni. Trwają wysiłki w kierunku wypracowania jednolitych standardów postepowania w przypadku popełniania przestępstw cybernetycznych. Istnieją już międzynarodowe regulacje prawne dotyczące zwalczania cyberterroryzmu oraz wiele międzynarodowych strategii walki z tym zjawiskiem. Celem opracowania jest ukazanie prawnych aspektów cyberbezpieczeństwa oraz omówienie instytucji odpowiedzialnych w tym obszarze. Dokonano ujęcia międzynarodowego poprzez analizę aktów prawnych oraz dokumentów politycznych i strategii międzynarodowych oraz europejskich dotyczących zwiększenia bezpieczeństwa w cyberprzestrzeni. W artykule ukazano również kampanie mające na celu uświadamiać społeczeństwo w zakresie zagrożeń w cyberprzestrzeni. Ukazano też różnorodność definicji cyberterroryzmu oraz dokonano analizy tego zjawiska pod kątem międzynarodowych regulacji i strategii.

Słowa kluczowe: cyberbezpieczeństwo, cyberterroryzm, cyberprzestrzeń, bezpieczeństwo w Internecie

Abstract

Security in cyberspace is one of the most serious issues of contemporary states and international organizations. Many joint actions are taken to combat threats in cyberspace. Efforts are underway to develop uniform standards of conduct in the event of committing cyber crimes. There are already international legal regulations on combating cyberterrorism and many international strategies to combat this dangerous phenomenon. The aim of the study is to show the legal aspects of cybersecurity and discuss the institutions responsible in this area. An international approach was made through the analysis of legal acts and policy documents and international and European strategies regarding the increase of security in cyberspace. The article also presents campaigns aimed at raising public awareness of threats in cyberspace. It also shows the diversity of

[1] Mgr Mariusz Stachowicz, starszy sierżant, Komenda Powiatowa Policji w Wieliczce.

definitions of cyberterrorism and analyzes this phenomenon in terms of international regulations and strategies.
Keywords: cybersecurity, cyberterrorism, cyberspace, safety in internet.

Wstęp

W dobie XXI wieku ochrona cyberprzestrzeni stała się jednym z głównych zagadnień instytucji państwa zajmujących się bezpieczeństwem wewnętrznym i zewnętrznym. Stabilność funkcjonowania oraz niezakłócony rozwój globalnego społeczeństwa informacyjnego możliwy jest wówczas, gdy cyberprzestrzeni nic nie zagraża. Bezpieczeństwo teleinformatyczne stanowi współcześnie ważny element polityki państwa we wszystkich dziedzinach. Coraz większa informatyzacja oraz korzystanie z elektronicznych narzędzi w gospodarce czy życiu społecznym wymaga stosowania najwyższych standardów zabezpieczeń. Państwo w tym celu powinno podjąć wszelkie dostępne działania, w tym rozwiązania prawne, organizacyjne i instytucjonalne, w celu minimalizacji wystąpienia zagrożenia w przestrzeni cybernetycznej.

Współcześnie na zagrożenia występujące w cyberprzestrzeni narażony jest tak naprawdę każdy człowiek, każda instytucja, zarówno te pozarządowe, jak i w szczególności instytucje państwa. Atak w przestrzeni internetowej można dokonać z dowolnego miejsca na świecie, a jego konsekwencje mogą być niezwykle szkodliwe i bardzo poważne dla całego bezpieczeństwa państwa. Podnoszenie świadomości w tym zakresie jest kluczowe. Nieustannie rośnie liczba incydentów komputerowych. Kategoria nowych zagrożeń również wzrasta. W pracy postanowiono omówić istniejące rozwiązania prawne i instytucjonalne oraz scharakteryzować instrumenty służące do zwalczania tego groźnego zjawiska.

Cel pracy i metodologia

Cyberterroryzm jest zjawiskiem międzynarodowym, nie ograniczającym się tylko do jednego państwa, lecz dotykającym wszystkie podmioty prawa międzynarodowego, a szerzej również wszystkich uczestników stosunków międzynarodowych i społeczeństwa. Celem opracowania było ukazanie prawnych regulacji zjawiska cyberterroryzmu w Polsce, wraz z ukazaniem międzynarodowych uregulowań dotyczących zwalczania zagrożenia cyberterroryzmu. Dokonano także charakterystyki instytucji państwa odpowiedzialnych za zwalczanie zjawiska terroryzmu w cyberprzestrzeni oraz ukazano najważniejsze działania mające na celu eliminację w jak największym stopniu tego zagrożenia. Hipotezą jaką autorzy postawili zakładała, że prawne środki i właściwa struktura instytucjonalna skutecznie mogą przeciwstawiać się temu zagrożeniu, gdyż cyberterroryzm stanowi coraz poważniejsze zagrożenie zarówno dla instytucji państwa jak i społeczeństwa w wielu płaszczyznach, w tym ekonomicznej, społecznej, prawnej, politycznej.

Analizę tematu oparto zasadniczo na metodzie analizy i krytyki piśmiennictwa oraz metodzie dogmatyczno-prawnej. Wykorzystano w tym celu analizę dostępnych materiałów źródłowych w postaci umów międzynarodowych, czy krajowych aktów prawnych regulujących prawne aspekty zwalczania cyberterroryzmu, a także dokonano analizy i wyjaśnienia teoretycznego ujęcia z bogatej literatury przedmiotu. Wykorzystana literatura była pomocna w rozwiązaniu problemu badawczego, jakim jest ukazanie i zwalczanie zagrożenia cyberterroryzmu w Polsce.

Charakterystyka pojęcia bezpieczeństwa i cyberbezpieczeństwa

Państwo uznawane jest za najbardziej rozwiniętą formę rozwoju społecznego. Przez wzgląd na ów fakt termin bezpieczeństwo stał się nieodłącznym elementem funkcji, jakie państwo realizuje. Zgodnie z tradycyjną rolą państwa bezpieczeństwo pełni dwie, kluczowe funkcje. Chodzi o funkcję wewnętrzną oraz zewnętrzną. Funkcja wewnętrzna odnosi się do dbania o bezpieczeństwo w obrębie całej, państwowej jurysdykcji. Jest to związane z zaspokajaniem potrzeb o podłożu psychicznym, co dotyczy poczucia bezpieczeństwa. Zgodnie z klasyczną funkcją administracji państwowej, czyli funkcją porządkowo-reglamentacyjną: „[…] bezpieczeństwo nie jest wszystkim lecz wszystko bez bezpieczeństwa jest niczym". Zgodnie z takim podejściem jednym z nadrzędnych zadań państwa jest ochrona obywateli przed zagrożeniami wewnętrznymi i zewnętrznymi[2].

Geneza pojęcia bezpieczeństwo silnie powiązana jest również z kształtowaniem się na przestrzeni lat instytucji, jaką jest policja. Odnosząc się przykładowo do pruskiej ustawy o administracji policyjnej z roku 1931 trzeba wskazać, że stanowiła ona, iż władze policyjne miały obowiązek realizowania takich przedsięwzięć, które będą w stanie zapobiegać zagrożeniom powszechnym i jednostkowym naruszającym bezpieczeństwo czy też porządek publiczny[3].

Jeżeli chodzi zaś o wiek XX to pojawiła się wówczas widoczna cenzura w zakresie postrzegania terminu bezpieczeństwo. Miało to bezpośredni związek z tworzącymi się wówczas systemami totalitarnymi, tj. systemem faszystowskim oraz komunistycznym. Działalność państwa przyjęła charakter ideologiczny. Zajęto się wtedy ochroną pozycji hegemonistycznej wobec rządzącej w państwie partii politycznej. W tamtym okresie to partia rządząca stanowiła swoistą podporę systemu polityczno-ustrojowego. Przez wzgląd na ów fakt doszło do dynamicznego rozbudowania systemu takich instytucji, których

[2] A. Chabasińska, Z. Czachów, *Bezpieczeństwo Narodowe Polski. Zagrożenia i determinanty zmian*, wyd. Difin, Warszawa 2016, s. 28.

[3] A. Misiuk, *Administracja spraw wewnętrznych w Polsce (od połowy XVIII wieku do współczesności). Zarys dziejów*, Olsztyn 2005, s. 12.

kluczowym zadaniem było ochranianie bezpieczeństwa państwa. Pojawił się chociażby kontrwywiad polityczny[4].

Misiuk zaznacza, iż termin bezpieczeństwo państwa jest znaczeniowo zbliżone do terminu bezpieczeństwo publiczne. Jednakowoż przejawia jednocześnie zdecydowanie węższy zakres przedmiotowy. Dzieje się tak ze względu na to, że dotyczy konieczności zapewnienia właściwego i zarazem wysoce bezpiecznego funkcjonowania:

- głównych państwowych instytucji,
- urządzeń państwowych,
- porządku o charakterze konstytucyjnym5.

W takim ujęciu, jak powyższe bezpieczeństwo odnosiło się do zagrożeń zarówno zewnętrznych, jak i wewnętrznych. Misiuk wskazał, że źródłem tego rodzaju zagrożeń mogą być inne kraje, zjawiska międzynarodowe (np. terroryzm) oraz wydarzenia o podłożu typowo społecznym mogące zagrażać stabilności ekonomicznej państwa[6].

Bezpieczeństwo wpisane jest w kontekst potrzeb indywidualnych każdego człowieka. Ponadto związane jest zasadniczo ze stosunkami wewnętrznymi państw i relacjami na płaszczyźnie międzynarodowej. Współcześnie kwestią kluczową jest zachowanie odpowiedniego poziomu bezpieczeństwa, co związane jest z utrzymaniem na bardzo wysokim poziomie:

- stabilizacji,
- pokoju,
- porządku publicznego[7].

Rozważania na temat postrzegania terminu bezpieczeństwo zamieścił w swojej publikacji R. Zięba. Jego zdaniem bezpieczeństwo przejawia charakter podmiotowy, dlatego że jest naczelną potrzebą człowieka i grup społecznych. Zagrożenie bezpieczeństwa zawsze budzi niepokój. Autor traktuje bezpieczeństwo, jako brak zagrożeń. Ujęcie podmiotowe bezpieczeństwa wykorzystywane jest najczęściej w nauce o stosunkach międzynarodowych[8].

Tym samym bezpieczeństwo i zarazem jego stan ściśle powiązane są z zagrożeniami i samą potrzebą tego, aby bezpieczeństwo przejawiało wysoki poziom[9]. Zdaniem R. Zięby bezpieczeństwo zaliczane jest do kategorii pojęć wykazujących się swoim dychotomicznym charakterem. Bezpieczeństwo można definiować, jako całkowity brak zagrożeń. Jednak kluczowe jest wówczas to, aby podejmować nieustanne działania, prowadzić badania, które przyczynią się do ochrony przed zagrożeniami. Sama ochrona przed zagrożeniami mieści się w katalogu wartości wewnętrznych. Takie ujęcie

[4] A. Misiuk, *Rzecz o bezpieczeństwie – geneza, istota, rozwój*, UW, Warszawa 2012, s. 98.
[5] A. Misiuk, *Administracja…*, *op. cit*., s. 12.
[6] *Ibidem*, s. 18.
[7] S. Pikulski, *Podstawowe zagadnienia bezpieczeństwa publicznego*, Szczytno 2013, s. 54.
[8] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego*, SCHOLAR, Warszawa 2013, s. 20.
[9] W. Lis, *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, KUL, Lublin 2016, s. 49.

bezpieczeństwa to ujęcie wąskie. Drugie z ujęć, czyli ujęcie przeciwstawne określane jest jako szerokie. Związane jest ono bezpośrednio z kształtowaniem takich warunków, które przyczynią się do osiągnięcia wysokiego stopnia prawdopodobieństwa dalszego przetrwania[10].

Zgodnie z kolejną definicją stan braku bezpieczeństwa pojawia się wówczas, gdy towarzyszy temu rzeczywiste zagrożenie, a jego postrzeganie jest prawidłowe. Mowa w tym kontekście o dużym zagrożeniu. Jeżeli chodzi zaś o bezpieczeństwo Rzeczypospolitej Polskiej to trzeba wskazać, że składa się na nie szereg, powiązanych ze sobą celów, mianowicie:

- ochrona suwerenności, jak i niezawisłości RP,
- utrzymanie nienaruszalności granic państwa,
- utrzymanie jego integralności terytorialnej,
- zapewnienia wysokiego poziomu bezpieczeństwa obywatelom kraju, tj.:
  - prawa człowieka,
  - podstawowe wolności,
  - porządek o charakterze demokratycznym,
- stworzenie takich warunków, które pozwolą na w pełni niezakłócony rozwój kraju o podłożu nie tylko cywilizacyjnym, ale i gospodarczym, a także wzrost dobrobytu wśród obywateli Polski,
- ochrona narodowego dziedzictwa,
- ochrona narodowej tożsamości,
- wypełnienie poszczególnych zobowiązań o charakterze sojuszniczym,
- obrona interesów państwa,
- promowanie interesów państwa11.

Warto dodać, że zgodnie ze współczesnymi definicjami bezpieczeństwo postrzegane jest jako stan, w którym panuje spokój oraz pewność, co do braku zagrożeń. Związane jest to z poczuciem zabezpieczenia, co wiąże się właśnie z brakiem zagrożeń, jak i ochroną przed niebezpieczeństwami[12].

Charakterystyka bezpieczeństwa teleinformatycznego

Podejmując próbę scharakteryzowania tego, czym jest tak właściwie bezpieczeństwo teleinformatyczne należy najpierw skupić się na jego definicji. Z literatury przedmiotu wynika, że jest to zbiór takich zagadnień, które mają bezpośredni związek z problematyką telekomunikacji oraz informatyki. Bezpieczeństwo teleinformatyczne powiązane jest zaś ściśle z szacowaniem ryzyka występującego w obrębie korzystania z:

[10] R. Zięba, *Instytucjonalizacja …*, *op.cit.,* s. 27.
[11] R. Szpyra, *Bezpieczeństwo militarne państwa*, wyd. Akademii Obrony Narodowej, Warszawa 2012, s. 26.
[12] *Ibidem*, s. 35.

- komputerów,
- sieci komputerowych,
- przesyłania różnego rodzaju informacji w formie zdalnej, co związane jest bezpośrednio z:
  – poufnością danych,
  – integralnością,
  – dostępnością danych[13].

Oprócz szacowania ryzyka dzięki bezpieczeństwu teleinformatycznemu jest ono również odpowiednio kontrolowane. Kluczowe jest współcześnie to, aby systemy teleinformatyczne budowane były w sposób w sposób w pełni bezpieczny. To samo tyczy się aplikacji mobilnych. Ten fakt spoczywa na projektantach sieciowych oraz programistach. Warto podkreślić, że bezpieczeństwo teleinformatyczne to przedmiot studiów teoretycznych z następujących dziedzin nauki:

- telekomunikacja,
- informatyka,
- ekonomia[14].

Dzięki powiązaniu ze sobą tych metod ostatecznie stało się możliwe opracowanie efektywnych metod, które służą ocenie bezpieczeństwa i kontrolowaniu powstałych zagrożeń. Niestety pomimo podejmowania licznych działań system teleinformatyczny nadał pełen jest luk i nieścisłości, które powodują zagrożenia dla użytkowników sieci teleinformatycznych.

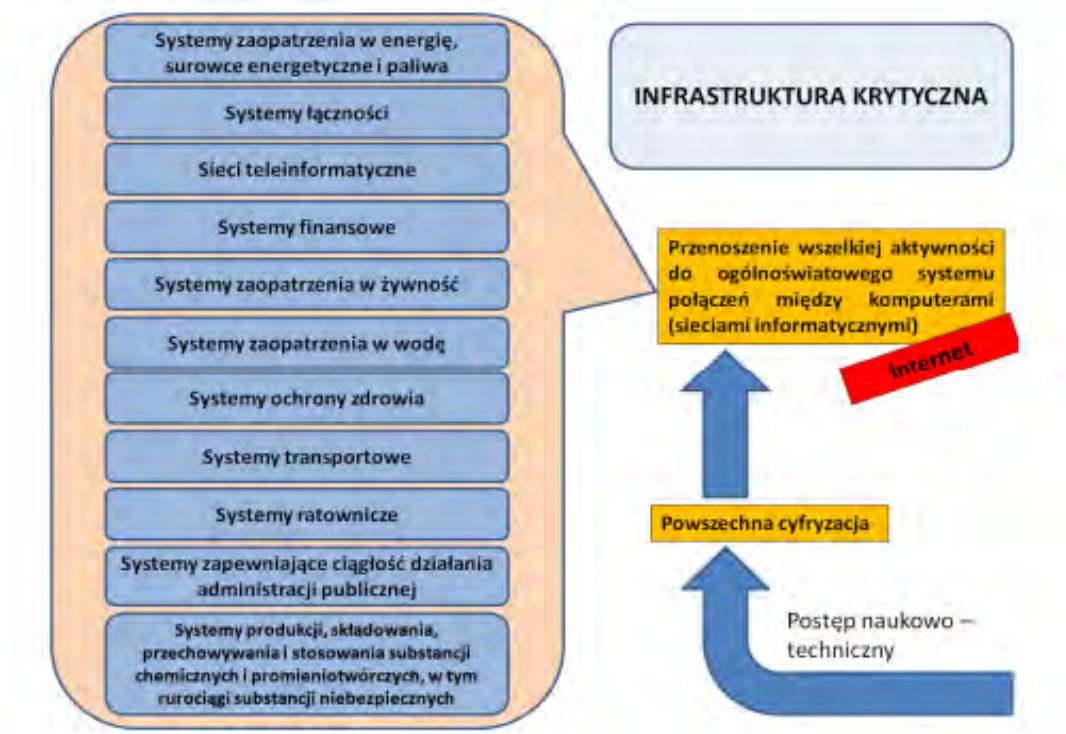
Podejmując próbę zdefiniowania bezpieczeństwa teleinformatycznego należy wskazać, że określane jest ono również terminem wywodzącym się z języka angielskiego: *cybersecurity.* Definiuje się je jako zbiór zagadnień z dziedziny telekomunikacji oraz informatyki. Stanowi ono dziś jeden z kluczowych aspektów każdego rodzaju działalności, w której pojawiają się komputery oraz gromadzone i przetwarzane są poufne dane. Należy podkreślić, że stosowanie tego typu zabezpieczeń regulowane jest w Polsce na mocy europejskich regulacji w postaci tzw. RODO[15]. Przepisy z zakresu prawa obligują tak naprawdę dany podmiot do tego, aby chronił dane, który pozyskał od swoich klientów oraz kontrahentów[16]. Celem tego rozporządzenia jest zharmonizowanie przepisów w całej Unii Europejskiej w zakresie przetwarzania danych osobowych w taki sposób, by były one bezpieczne i właściwie chronione.

W sytuacji, gdy takie dane zostaną skradzione na przedsiębiorstwo mogą zostać nałożone bardzo wysokie kary finansowe. Niezbędne jest więc zadbanie o bezpieczeństwo

[13] B. Biernacik, L. Kalman, *Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polskiej – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, ASzWoj, Warszawa 2016, s. 65.
[14] *Ibidem*, s. 67.
[15] 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*, Dz.U. UE, L119, 4.05.2016.
[16] K. Malak, *Bezpieczeństwo polityczne i wojskowe*, Difin, Warszawa 2019, s. 45.

teleinformatyczne na najwyższym poziomie. Ograniczy to negatywne skutki sytuacji, w której dane zostaną skradzione.

Charakteryzując bezpieczeństwo teleinformatyczne trzeba wspomnieć o tym, że ma ono na celu zapewnienie ochrony wszystkim danym, jak i informacjom, które są najpierw gromadzone, a kolejno przetwarzane przez systemy informatyczne oraz komunikacyjne. Za sprawą rozwoju technicznego, a zarazem globalnego wykorzystywania informatycznych systemów o charakterze wspomagającym niezbędne jest odpowiednie zarządzanie tymi systemami.



Rys. Sieci teleinformatyczne w systemach infrastruktury krytycznej

Źródło: B. Biernacik, L. Kalman, *Systemy i sieci teleinformatyczne SZ RP – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, ASzWoj, Warszawa 2016, s. 280.

Oczywiście w dobie XXI wieku zarządzanie to jest w pełni zautomatyzowane przy wykorzystaniu urządzeń zdalnych. Utrzymywanie stałego dostępu do sieci teleinformatycznych jest w kontekście zachowania odpowiedniego poziomu bezpieczeństwa kluczowe. Bowiem poprzez sieci teleinformatyczne dochodzi do kierowania poszczególnymi systemami[17]. Aby państwo było w tym zakresie bezpieczne

[17] M. Madej, M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 87.

niezbędne jest sterowanie procesami technologicznymi np. w zakładach zajmujących się produkcją broni za sprawą zautomatyzowanych systemów. To samo tyczy się ochrony danych określanych mianem wrażliwych. Same sieci teleinformatyczne odgrywają jedną z nadrzędnych ról w systemach infrastruktury krytycznej, do czego nawiązano za sprawą rysunku.Odpowiednie zarządzanie infrastrukturą krytyczną ma zapobiegać wszelkim zakłóceniom w jej funkcjonowaniu. Dotyczy to również sieci teleinformatycznych i zapewnienia im wysokiego poziomu bezpieczeństwa.

Zagrożenia dla bezpieczeństwa teleinformatycznego

Współcześnie przez wzgląd na cyfryzację biznesu wręcz konieczne stało się stosowanie różnego rodzaju zabezpieczeń, które będą w stanie zwiększyć bezpieczeństwo teleinformatyczne danego podmiotu. Dzięki nim ograniczone zostanie również ryzyko wystąpienia zagrożeń. Źródeł zagrożeń pojawiających się w zakresie bezpieczeństwa teleinformatycznego jest naprawdę wiele. Jednakże nie tylko brak należytych zabezpieczeń stanowi źródło zagrożeń dla bezpieczeństwa teleinformatycznego, ale również nieświadomość, czy ignorancja/bagatelizowanie ze strony użytkowników Internetu w podejściu do bezpieczeństwa w sieci.

Od lat luki w zabezpieczeniach sieci teleinformatycznych są wykorzystywane przez hakerów, którzy dzięki swojej wiedzy oraz zdolnościom są w stanie sabotować zabezpieczenia sieci teleinformatycznych. Kolejno zdobywają oni dostęp do konkretnych zasobów. To właśnie od określenia haker wywodzi się pierwszy rodzaj e-przestępstw określany mianem hakingu. Ze zjawiskiem hakingu mocno powiązana jest cyberprzestępczość.

W Polsce zjawisko to zostało zdefiniowane w Strategii Cyberbezpieczeństwa RP na lata 2019-2024[18]. Strategia ta wynika z ustawy o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r[19]. Istota przyjęcia obecnie obowiązującej Strategii jest podobna do poprzednich, jednak zakłada ona w większym stopniu wzmacnianie istniejącego systemu cyberbezpieczeństwa. Głównym celem Strategii jest określenie celów oraz środków politycznych i regulacyjnych, które zwiększą poziom odporności systemów informacyjnych operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na cyberzagrożenia. Założeniem jest również zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń. Przyjęte rozwiązania prawne i organizacyjne powinny wpływać na lepsza wykrywalność i zwalczanie cyberprzestępstw o charakterze

[18] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, Monitor Polski 2019, poz. 1037. Przed przyjęciem tej Strategii obowiązywał Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016, oraz Strategia Cyberbezpieczeństwa RP na lata 2017-2022.
[19] Dz.U. 2022, poz. 1863.

hybrydowym i szpiegowskim. W bieżącej Strategii określono pięć szczegółowych celów polityki rządu RP:

1) Rozwój krajowego systemu cyberbezpieczeństwa.
2) Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.
3) Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni.
4) Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa.
5) Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa

Dzięki odpowiedniemu podejściu do bezpieczeństwa w cyberprzestrzeni przez powyższe podmioty dochodzi jednocześnie do zwiększenia poziomu bezpieczeństwa narodowego.

Definicja cyberterroryzmu

Podejmując próbę zdefiniowania cyberterroryzmu należy wskazać, że jest to jeden z terminów najczęściej występujących w obrębie bezpieczeństwa teleinformatycznego. Brak jest jednej międzynarodowej definicji cyberterroryzmu. Wynika to z faktu, iż jest ona niejednoznaczna i niejednorodna. Jak wskazuje Bielski, różnorodność ataków terrorystycznych, czy odmienne podejście naukowców i ośrodków analitycznych w zakresie różnych czynników badawczych, nie sprzyja wypracowaniu wspólnego stanowiska zarówno w ramach organizacji międzynarodowej, ani też w ramach jednego państwa[20]. Jednakże poszczególne instytucje wewnętrzne państwa, czy naukowcy lub inne instytucje podejmują próby zdefiniowania tego zjawiska i opisania go zgodnie z zainteresowaniami badawczymi lub przedmiotem działań. Przykładowo D. Denning traktuje cyberterroryzm, jako: „[…] konwergencję terroryzmu oraz cyberprzestrzeni". Cyberatak, aby uznany został za przejaw terroryzmu musi skutkować przemocą wobec mienia bądź osób lub generować powszechny strach[21]. Zdaniem A. Lewisa mianem cyberterroryzmu należy określić wykorzystanie sieci komputerowej, jako narzędzia służącego ku temu, aby całkowicie sparaliżować bądź poważnie ograniczyć możliwości efektywnego wykorzystania struktur narodowych. Może to dotyczyć na przykład:

- energetyki,
- transportu,
- instytucji rządowych[22].

[20] K. Bielski, *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Acta Politica Nr 34, nr 889/2015, s. 95.
[21] D., Denning, *Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism*, Committee on Armed Services, U.S. House of Representatives, Georgetown University, Washington 2000, s. 317.
[22] J. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington 2002, s. 100.

Według wspomnianego wyżej autora cyberterroryzm może być też utożsamiany, jako zjawisko mające na celu wymuszenie na rządzie bądź populacji konkretnych działań. Jest to ściśle związane z zastraszaniem[23].

Zgodnie z definicją zaproponowaną przez M. Terlikowskiego cyberterroryzmem jest działalność o podłożu terrorystycznym w obrębie, której odpowiednie programy, urządzenia elektroniczne i właśnie systemy teleinformatyczne stanowią rodzaj narzędzia (można mówić w tym kontekście o swoistej broni), jaką posługują się terroryści[24].

Cyberterroryzm zawsze wykorzystuje komputery, a szerzej technologie o charakterze ICT, aby doprowadzić do działań terrorystycznych odbywających się w cyberprzestrzeni. W jednej z definicji ujęto, że cyberterroryzm stanowi zasadniczo atak, który motywowany jest politycznie. Może to być również groźba ataku na:

- komputery,
- sieci,
- systemy informacyjne[25].

Tego typu ataki mają za zadanie zniszczyć konkretną infrastrukturę bądź zastraszyć rząd oraz ludzi. Cyberataki mogą mieć również związek z wymuszeniem konkretnych celów o podłożu politycznym bądź społecznym. Internet wykorzystywany jest w tym kontekście przez organizacje terrorystyczne, do tego, by szerzyć propagandę, dezinformację, a także żeby się komunikować[26].

Warto odnieść się do jeszcze jednej definicji cyberterroryzmu. Zgodnie z tą definicją zwykło się tak nazywać atak, który dokładnie przemyślany jest pod względem politycznym oraz militarnym na systemy teleinformatyczne. Cyberterroryzm nie zawsze przyjmuje postać ataku może wystąpić również, jako groźba. Atakowi podlegają zaś gromadzone skrzętnie dane po to, aby sparaliżować lub całkowicie zniszczyć infrastrukturę krytyczną państwa. Niejednokrotnie cyberterroryzm przyjmuje formę wymuszenia na rządzie bądź społeczeństwie działań politycznych oraz militarnych. Cyberatak może być pojedynczy bądź złożony. Poza tym cyberterroryzmem jest wykorzystanie sieci teleinformatycznej do tego, aby prowadzić:

- działania propagandowe,
- rekrutację,
- komunikację,
- mobilizację,
- zbieranie konkretnych informacji, danych odnośnie celów ataku,
- planowanie,

[23] *Ibidem*.
[24] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe Haking, haktywizm i cyber-terroryzm*, PWN, Warszawa 2017, s. 81.
[25] *Ibidem.*
[26] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej", 2012/1, s. 179.

- koordynowanie akcji,
- dezinformację,
- walkę o podłożu typowo psychologicznym[27].

Cyberterroryzm stanowi specyficzną formę zagrożeń, jakie występują w XXI wieku. Zasadniczo obejmuje on wszelkie te działania, które realizowane są w stosunku do systemów teleinformatycznych. Cyberterroryzm stosuje się, aby doszło do osiągnięcia określonych celów terrorystycznych. Zagrożenia cyberterroryzmem mogą być zarówno regionalne jak i lokalne. Zagrożenia te nie dotyczą wyłącznie państwa, jako podmiotu[28]. Istnieją bowiem cyberprzestępstwa, które można nazywać cyberterroryzmem, a które realizowane są na mniejszą skalę. W tym przypadku ich szkodliwość również jest mniejsza. Są to zasadniczo formy przestępstw i różnego rodzaju działań pod względem prawnym zabronione, jednak dokonuje się ich właśnie w cyberprzestrzeni wykorzystując do tego komputery oraz Internet[29].

W pierwszej grupie cyberprzestępstw występują oszustwa oraz fałszerstwa. W drugiej grupie znajdują się posiadanie treści, które są nielegalne. Dotyczy to bezpośrednio:

- pozyskiwania takich treści,
- ich wytwarzania,
- rozpowszechniania,
- posiadania[30].

Do kolejnej, tj. trzeciej grupy zagrożeń zaliczane są ataki na systemy teleinformatyczne, a do ostatniej należy kopiowanie i późniejsze rozpowszechnianie w celach typowo zarobkowych utworów, które chronione są prawem autorskim[31].

Inny podział zagrożeń w tym zakresie został zaproponowany przez Komisję Europejską. W tym przypadku zagrożenia w cyberprzestrzeni dzielą się następująco:

- przestępstwa przeciw poufności danych, ich integralności i dostępności związane z nielegalnym dostępem do określonych systemów. Dzielą się wówczas na:
  - hacking,
  - podsłuchiwanie,
  - podawanie fałszywej, nieprawdziwej tożsamości,
  - sabotaż,
  - szpiegostwo komputerowe,
  - wymuszenia o charakterze komputerowym,
- manipulowanie fakturami bądź kontami firmowymi, tworzenie nieprawdziwych aukcji internetowych, nielegalne używanie kart kredytowych, tworzenie komputero-

[27] E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, PWN, Warszawa 2013, s. 38.
[28] *Ibidem*, s. 87.
[29] *Ibidem*, s. 90.
[30] P. Kardas, *Oszustwo komputerowe w kodeksie karnym*, „Przegląd Sadowy" 2011/11, s. 60.
[31] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Difin, Warszawa 2013, s. 34-38.

wych podróbek, molestowanie dzieci wykorzystując do tego Sieć internetową, przeprowadzanie ataków na ludzkie życie, manipulowanie systemami, np. systemem szpitalnym, jak i kontrolowanie ruchu powietrznego,

- przestępstwa, które odnoszą się w sposób bezpośredni do dziecięcej pornografii, przekazywanie instrukcji ku temu, jak prowadzić działania przestępcze, lobbing i molestowanie, oferowanie popełnienia przestępstwa, rozpowszechnianie informacji, które są nieprawdziwe, hazard prowadzony za pośrednictwem Sieci internetowej,
- przestępstwa, które związane są w sposób bezpośredni z naruszaniem praw autorskich oraz praw pokrewnych, dotyczy to m.in.:
  - nieautoryzowanego kopiowania programów komputerowych,
  - nielegalnego rozpowszechniania programów komputerowych,
  - nielegalnego używania baz danych32.

Tego typu zagrożenia, do których nawiązano powyżej mogą wystąpić w przestrzeni lokalnej i regionalnej. Atakom mogą ulec zarówno samorządy terytorialne, lokalni i regionalni przedsiębiorcy, jak również mieszkańcy. Cyberprzestępczość jest obecnie poważnym problemem, którego skala jest bardzo wysoka.

Prawo międzynarodowe w zakresie zwalczania cyberprzestępczości

W prawie międzynarodowym brak jest definicji cyberterroryzmu, jak i samego terroryzmu. Natomiast powszechnie uznaje się zbliżone zjawiska jako mające charakter cyberterroryzmu. W kontekście międzynarodowych regulacji należy wymienić europejskie rozwiązania prawne, choćby Konwencję o zwalczaniu cyberprzestępczości uchwaloną przez Radę Europy w Budapeszcie z dnia 23 listopada 2001 r. (ETS No. 185)[33]. W konwencji określono środki jakie należy podjąć w prawie krajowym w celu większej ochrony społeczeństwa przed nielegalnymi aktami w cyberprzestrzeni. Zobowiązano państwa do penalizowania przestępstw:

a) naruszających poufność danych w systemach informatycznych,
b) komputerowych polegających na fałszowaniu danych lub oszustwie komputerowym,
c) w zakresie pornografii dziecięcej,
d) związanych z naruszeniem praw autorskich i pokrewnych.

Państwa zostały także zobowiązane do objęcia odpowiedzialnością karną osób, które usiłują, pomagają lub podżegają do popełnienia któregokolwiek z wyżej wymienionych przestępstw.

[32] R. Kośla, *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, Ossolineum, Wrocław 2017, s. 102.
[33] Dz.U. 2015, poz. 728. Konwencja weszła w życie 18 marca 2004 r., natomiast Polska ratyfikowała konwencję w dniu 29.01.2015 r. i weszła w życie w stosunku do Polski 27.05.2015 r.

Warto jeszcze wspomnieć o działaniach Unii Europejskiej w zakresie zwalczania cyberterroryzmu. Tutaj należy wskazać na dokument nie będący prawnie wiążącą regulacją, lecz będący politycznym drogowskazem dla państw członkowskich. Obecnie realizowana jest europejska strategia cyfrowa na lata 2021-2030 „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[34]**.** W ramach tej strategii określono na najbliższe lata program walki z cyberprzestępczością. Do głównych celów unijnego programu należą:

a) zmiana dyrektywy w sprawie bezpieczeństwa sieci i informacji,
b) wdrożenie środków regulacyjnych dotyczących internetu,
c) zwiększenie finansowania programu „Cyfrowa Europa", „Horyzont Europa" do nawet 4,5 mld EUR w ramach inwestycji publicznych i prywatnych w latach 2021-2027,
d) opracowanie i wdrożenie unijnej sieci ośrodków monitorowania bezpieczeństwa wspieranych przez sztuczną inteligencję oraz ultrabezpieczną infrastrukturę łączności wykorzystującą technologie kwantowe,
e) rozwijanie współpracy i wymiany między podmiotami odpowiedzialnymi za cyberbezpieczeństwo i organami ścigania (w tym Europol, ENISA),
f) budowa wspólnej jednostki ds. cyberprzestrzeni,
g) wdrażanie programu dotyczącego cyberprzestępczości w ramach strategii w zakresie unii bezpieczeństwa,
h) wzmocnienie pozycji UE w zakresie cyberprewencji w celu zapobiegania szkodliwym działaniom w cyberprzestrzeni, zniechęcania do nich, powstrzymywania przed nimi i reagowania na nie,
i) dokonanie aktualizacji polityki w zakresie cyberobrony,
wzmocnienie cyberbezpieczeństwa krytycznej infrastruktury kosmicznej w ramach programu kosmicznego.

Podmioty odpowiedzialne za zwalczanie cyberprzestępczości

W Polsce funkcjonują podmioty, które ponoszą szczególną odpowiedzialność za zwalczanie bezpieczeństwa w cyberprzestrzeni. Oczywiście w tym zakresie bardzo ważna jest odpowiednia współpraca pomiędzy tymi podmiotami. Do podmiotów, które mają za zadanie chronić bezpieczeństwo cyberprzestrzeni zalicza się:

- Ministerstwo Spraw Wewnętrznych,
- Ministerstwo Administracji i Cyfryzacji,
- Ministerstwo Obrony Narodowej,
- Agencję Bezpieczeństwa Wewnętrznego,
- Służbę Kontrwywiadu Wojskowego,

[34] Komisja Europejska, Wspólny Komunikat do Parlamentu Europejskiego i Rady, Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN (2020) 18, wersja ostateczna, 16.12.2020.

- Podmioty należące bezpośrednio do sektora prywatnego[35].

Wszystkie podmioty odpowiedzialne za cyberbezpieczeństwo powinny dążyć do realizacji wspólnych celów w zakresie wzrostu bezpieczeństwa w cyberprzestrzeni. Wspomniane cele dotyczą przede wszystkim:

- odpowiedniego zabezpieczenia krytycznej infrastruktury teleinformatycznej przed zagrożeniami, które pojawiają się w cyberprzestrzeni,
- stworzenie dla całego państwa wspólnej polityki bezpieczeństwa w cyberprzestrzeni, które obejmowało będzie sektor prywatny oraz publiczny,
- dążenie do stworzenia możliwie najlepszego systemu służącego koordynacji umożliwiającego efektywną współpracę podmiotów sektora publicznego i prywatnego w zakresie bezpieczeństwa cyberprzestrzeni,
- dążenie do tego, aby możliwie najszybciej reagować na skutki incydentów komputerowych, dzięki czemu ograniczone zostaną ich koszty,
- podejmowanie działań, które przyczynią się do wzrostu świadomości społecznej w kontekście bezpieczeństwa w cyberprzestrzeni[36].

Jeżeli chodzi o strukturę krajowego systemu cyberbezpieczeństwa to wymaga ona wielopoziomowych działań opartych na rzetelnej współpracy wymienionych wyżej podmiotów. Kluczowe jest funkcjonowanie należytych norm z zakresu prawa, które wpłyną pozytywnie na skuteczne działanie państwa oraz instytucji odpowiedzialnych za bezpieczeństwo w cyberprzestrzeni. Warto jednocześnie dodać, że samo wprowadzenie pojęcia, jakim jest „cyberprzestrzeń" stanowiło inicjatywę prezydenta. Pojęcie to zaczęło obowiązywać w polskim systemie prawnym. Jednak, aby poszczególne działania na rzecz cyberbezpieczeństwa Polski przynosiły oczekiwane rezultaty to konieczne jest dalsze regulowanie zasad takiej ochrony i ustalanie obszarów odpowiedzialności za tę ochronę. Tyczy się to zarówno cyberprzestrzeni, jak i krytycznej infrastruktury teleinformatycznej. Spójna polityka bezpieczeństwa jest w tym zakresie kluczowa, ponieważ poszczególne komponenty infrastruktury teleinformatycznej stanowią własność różnych jednostek samorządu terytorialnego (administracji publicznej). Spójna polityka bezpieczeństwa w tym zakresie powinna stanowić, więc priorytet. Co ważne, znaczna część elementów infrastruktury technicznej należy do podmiotów prywatnych. Dlatego też niezbędne jest ustalenie metod i zakresu współpracy pomiędzy administracją publiczną, a sektorem prywatnym[37]. Tylko wtedy działania na rzecz przeciwdziałania zagrożeniom w cyberprzestrzeni będą miały sens. Oczywiście konieczne jest przy tym podejmowanie współpracy z innymi krajami i organizacjami międzynarodowymi. Wówczas wymiar współpracy będzie naprawdę rozległy i tym samym bardziej miarodajny.

[35] T. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, PWN, Warszawa 2018, s. 272.
[36] J. Gajewski, W. Paprocki, J. Pieriegud, *Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych*, Gdańska Akademia Bankowa, Gdańsk 2018, s. 38-40.
[37] *Ibidem*, s. 45.

Odnosząc się do podmiotów, które mają wpływ na stan polskiej cyberprzestrzeni i jej bezpieczeństwa należy wskazać na Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV[38]. Jednostką odpowiedzialną za prowadzenie owego zespołu jest Szef Agencji Bezpieczeństwa Wewnętrznego. Zespół ma za zadanie reagować aktywnie na wszelkie incydenty komputerowe. Ma przede wszystkim skutecznie rozpoznawać zagrożenia, wykrywać je i oczywiście efektywnie przeciwdziałać ich powstawaniu[39].

W Polsce funkcjonuje także NASK, czyli Naukowa i Akademicka Sieć Komputerowa, która odpowiedzialna jest za realizację działań o charakterze badawczym i rozwojowym w kwestii opracowania nowoczesnych rozwiązań, które wpłyną na poprawę bezpieczeństwa teleinformatycznego, tak by stało się ono bardziej: niezawodne oraz efektywne[40]. Różne struktury zapewniają większy poziom bezpieczeństwa w cyberprzestrzeni. Jednakże, musi istnieć koordynacja działań poszczególnych jednostek z uwagi na złożoność zjawiska.

Instrumenty wpływające na wzrost bezpieczeństwa w cyberprzestrzeni

Bezpieczeństwo w cyberprzestrzeni to istotna problematyka we współczesnym świecie. Coraz więcej pojawia się incydentów, które obniżają jej poziom. Aby bezpieczeństwo w cyberprzestrzeni przejawiało wysoki poziom należy przede wszystkim uświadomić w tym zakresie społeczeństwo. Edukacja obywateli oraz poziom podnoszenia ich wiedzy w tym zakresie to jedno z zadań, jakie powinna spełniać administracja samorządowa. Realizowanie specjalnych kampanii w najmniejszych jednostkach samorządu terytorialnego, czyli gminach to pierwszy krok, który jest w stanie pomóc. Organizowanie spotkań z mieszkańcami jest w stanie wiele zmienić. Nadal wiele osób nie zdaje sobie sprawy, jak szkodliwe może być kliknięcie w zainfekowany link wysłany w wiadomości SMS. Niejednokrotnie ludzie tracą w ten sposób całe swoje oszczędności. Wiedza z zakresu bezpieczeństwa w cyberprzestrzeni musi być promowana nieustannie.

Ważne jest także prowadzenie dalszych badań oraz tworzenie prac naukowo-rozwojowych związanych z problematyką cyberbezpieczeństwa. Innowacyjne podejście do tego problemu jest bardzo ważne. Eksperci powinni poszukiwać sposobów, które będą w stanie zapobiegać rozprzestrzenianiu niebezpiecznych linków i szkodliwego oprogramowania. Tyczy się to również kwestii reagowania w takich sytuacjach. Sieć i systemy teleinformatyczne muszą być całkowicie bezpieczne, aby państwo i jego

[38] CSIRT GOV został utworzony na podstawie art. 2 pkt 1 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018, poz. 1580.
[39] C. Banasiński, *Cyberbezpieczeństwo. Zarys wykładu*., Wolters Kluwer, Warszawa 2018, s. 67-68.
[40] NASK jest instytutem badawczo-rozwojowym zajmującym się działaniami na rzecz bezpieczeństwa internetu założonym w 1991 r. na Uniwersytecie Warszawskim, a posiadający obecnie od 2017 r. status Państwowego Instytutu Badawczego.

obywatele mogli normalnie funkcjonować. Jako przykład jednostki, która się tym zajmuje należy podać NASK, do którego nawiązano w poprzednim podrozdziale. Jednym z działań, które powinny być organizowane cyklicznie są kampanie społeczne. Przykładowo w ostatnim kwartale roku 2019 pojawiła się kampania o nazwie CyberLiga Początek. Została ona zainicjowana właśnie przez NASK. CyberLiga to grupa superbohaterów, których zadaniem było zadbanie o bezpieczeństwo internautów w Sieci internetowej. Wspomnianych bohaterów nazwano: Kapitan Antyvir oraz Lady Antyspam. Superbohaterowie zmagają się na przykład z PhisingManem oraz RansonWoman. Była to kampania o charakterze edukacyjnym. Jej bohaterowie specjalnie posługiwali się językiem młodzieżowym, aby dotrzeć do takiego właśnie grona odbiorców. Głównym Zadaniem kampanii było przybliżenie internautom zagrożeń, jakie występują w Internecie. Powstała ona, jako część obchodów Europejskiego Miesiąca Cyberbezpieczeństwa[41].

Kampania miała na celu edukowanie internautów odnośnie najpowszechniejszych zagrożeń, z jakimi można spotkać się w Sieci internetowej. NASK posiadając świadomość tego, jak przeciwdziałać zagrożeniom stworzył kampanię o silnym potencjale. Miała ona uświadamiać ludzi, tak by przestali być w sieci naiwni, a kierowali się zdrowym rozsądkiem. Warto w tym miejscu zaznaczyć, że wspomniany wyżej Europejski Miesiąc Cyberbezpieczeństwa, który w języku angielskim określany jest mianem: *European Cyber Security Month, ECSM* to kampania w wymiarze ogólnoeuropejskim. Kampania ta organizowana jest przez ENISA na prośbę Komisji Europejskiej[42]. Dlatego też w październiku każdego roku wszystkie kraje członkowskie Unii Europejskiej muszą organizować wydarzenia, których nadrzędnym celem jest podniesienie świadomości odnośnie bezpieczeństwa w Internecie, jak i w zakresie nowoczesnych technologii. Warto podkreślić, że kampania w Polsce od lat jest koordynowana właśnie przez NASK.

Inna kampania społeczna związana ściśle z cyberbezpieczeństwem nosi nazwę STOP.THINK.CONNECT, czyli stój, pomyśl, połącz. Kampania ta stanowi polską wersję międzynarodowej kampanii. Jej głównym celem jest zwiększenie świadomości społecznej oraz znaczące zwiększenie bezpieczeństwa w obrębie cyberprzestrzeni. Jest to inicjatywa, która funkcjonuje już od kilkunastu lat, gdyż powstała w roku 2010. Z roku na rok jest ona doskonalona i dostosowywana do nowych zagrożeń. Inicjatywa ta zrzesza m.in.:

- przedsiębiorców prywatnych,
- różnego rodzaju organizacje non-profit,
- instytucje rządowe[43].

Za tę inicjatywę w Polsce odpowiedzialny jest zespół CERT Polska. Zespół ów należy do struktur Państwowego Instytutu Badawczego, do którego się wcześniej

[41] https://www.iab.org.pl/aktualnosci/iab-polska-partnerem-kampanii-cyberbezpieczenstwa-cyberliga/, [dostęp 23.07.2022].
[42] K. Liderman, *Bezpieczeństwo informatyczne. Nowe wyzwania*, PWN, Warszawa 2020, s. 112.
[43] *Ibidem*, s. 115.

odniesiono, czyli NASK. Do znaczenia haseł wykorzystywanych w kampanii odniesiono się w tabeli.

Tabela. Hasła kampanii STOP.THINK.CONNECT

Dane hasło	Omówienie hasła
STÓJ	Zanim internauta skorzysta z Internetu powinien dowiedzieć się czy jest tam w pełni bezpieczny. Powinien skupić się dodatkowo na tym, aby unikać zagrożeń, czyli na przykład nie wchodzić w podejrzane linki.
POMYŚL	To hasło powiązane jest z tym, by internauci upewniali się czy droga do świata Internetu na pewno jest w pełni bezpieczna. Zawsze powinni sprawdzać czy na przykład nie pojawiają się komunikaty o charakterze ostrzegawczym. Korzystanie z Internetu powinno być bowiem rozważne i w pełni przemyślane. Konieczne jest w tym kontekście zadbanie również o najbliższe otoczenie.
POŁĄCZ	Hasło nawołuje do tego, aby ankietowani cieszyli się możliwościami bezpiecznego korzystania z Internetu.

Źródło: https://stojpomyslpolacz.pl/stp/o-kampanii/16,STOJ-POMYSL-POLACZ-jest-polska-wersja-miedzynarodowej-kampanii-STOP-THINK-CONNEC.html, [dostęp 30.07.2022].

Kampania ta jest bardzo łatwa w odbiorze. Specjalnie skonstruowano ją w taki sposób, aby mogła trafić do każdego. Problem zagrożeń w sieci jest problemem niezwykle poważnym, który trudno byłoby jednoznacznie wyeliminować. W związku z tym tego rodzaju kampanie są współcześnie konieczne. Powinno być ich, jak najwięcej, gdyż skala problemu jest naprawdę rozległa.

Do kategorii kluczowych celów kampanii zalicza się następujące cele:

- podniesienie poziomu społecznej świadomości w kwestii cyberbezpieczeństwa za sprawą informowania internautów o możliwych zagrożeniach oraz przedstawienie sposobów na to, jak z takimi problemami można sobie łatwo poradzić,
- promowanie takich zachowań, które wpłyną na poprawę bezpieczeństwa internautów, a zarazem ich rodzin i otoczenia, w jakim na co dzień funkcjonują,
- kreowanie odpowiednich postaw, jakie internauci powinni przybierać w Sieci internetowej. Kampania ma na celu promowanie tego typu postaw wśród wszystkich użytkowników Internetu,
- zaangażowanie w działania na rzecz cyberbezpieczeństwa zarówno podmiotów z sektora publicznego, jak i prywatnego,
- budowanie środowiska zaangażowanego, które przyczyni się do promowania należytych praktyk oraz edukacji związanej z bezpieczeństwem w obrębie Sieci internetowej[44].

Należy jednocześnie stwierdzić, że na zwiększenie poziomu cyberbezpieczeństwa wpływ ma również funkcjonowanie stowarzyszeń. Jednym ze stowarzyszeń, do których warto jest się odnieść jest Stowarzyszenie Cyberbezpieczni. Misją stowarzyszenia jest rozprzestrzenianie wiedzy odnośnie cyberbezpieczeństwa. Działania te realizowane są

[44] https://stojpomyslpolacz.pl/stp/o-kampanii/16,STOJ-POMYSL-POLACZ-jest-polska-wersja-miedzynarodowej-kampanii-STOP-THINK-CONNEC.html, [dostęp 30.07.2022].

w taki sposób, by skutecznie oddziaływać na bezpieczeństwo wszystkich użytkowników Sieci internetowej. W ramach partnerstwa stowarzyszenie prowadzi współpracę z jednym z wiodących stowarzyszeń funkcjonujących na terenie Europy o nazwie DsiN, które zlokalizowane jest w Berlinie[45]. Jest to bardzo ważne, gdyż stowarzyszenia mogą wymieniać się doświadczeniami i spostrzeżeniami, tworząc wspólnie silne ramy bezpieczeństwa, które są później przekazywane odbiorcom.

Bardzo ważne jest tworzenie coraz to nowych systemów bezpieczeństwa, takich jak Arakis Enterprise. Jest to innowacyjny system służący do wczesnego ostrzegania. Wyposażony jest w algorytmy automatycznego wykrywania wzorców zagrożeń. Ostrzega o cyberzagrożeniach IT oraz OT. Architektura przytoczonego systemu oparta jest bezpośrednio na rozproszonych sensorach REF. Sensory te rozproszone są w różnych segmentach sieci IT i OT, a także modułu centralnej analizy ARAKIS Management Center. Dzięki modułowi dochodzi do korelacji i późniejszej klasyfikacji poszczególnych danych oraz incydentów, które udało się wykryć[46].

System ARAKIS pozwala na wnikliwą analizę zagrożeń. Jest to system skuteczny. Dlatego też konieczne jest by był on stale ulepszany. Bowiem reagowanie na zagrożenia będzie jeszcze skuteczniejsze. Inny, istotny system dla ochrony bezpieczeństwa finansowego w cyberprzestrzeni nosi nazwę Botsense. Istnienie tego systemu jest współcześnie nadzwyczaj istotne, gdyż pozwala on w czasie rzeczywistym na wykrycie próby przejęcia konta. Ponadto jest on w stanie autoryzować wszelkie nieidentyfikowane transakcje płatnicze. Posiada zatem liczne zalety. Ważne jest aby program był udoskonalany, by mógł funkcjonować jeszcze lepiej, gdyż obecnie przejęcia kont bankowych to jedno z najpoważniejszych cyberzagrożeń[47].

Zarówno zasoby informacyjne, jak i poszczególne komponenty infrastruktury teleinformatycznej Polski podlegają tak naprawdę tym samym trendom, które stosowane są w innych krajach. Bezpieczeństwo w polskiej cyberprzestrzeni nie odbiega od poziomu globalnego. Ważne jest jednak to, aby było ono nieustannie wzmacniane. Konieczne jest to chociażby przez wzgląd na postępującą informatyzację. Niezbędne jest w tym zakresie tworzenie rozwiązań o charakterze:

- profilaktycznym,
- technicznym,
- organizacyjnym,
- prawnym[48].

[45] https://cyberbezpieczni.org.pl/, [dostęp 02.08.2022].
[46] M. Molendowska, R. Miernik, *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia*, Wydawnictwo Adam Marszałek, Warszawa 2021, s. 95.
[47] *Ibidem*, s. 98.
[48] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP z 2020 roku*, Warszawa 2021.

Dzięki temu możliwa będzie kompleksowa ochrona obywateli bez względu na region, jaki zamieszkują. Aby cyberprzestrzeń była bezpieczna muszą być podejmowane działania, w których udział biorą:

- władze,
- społeczeństwo,
- sektor prywatny,
- organizacje o charakterze pozarządowym.

Tylko współpraca w tym zakresie może przynieść oczekiwane rezultaty. Jej doskonalenie jest priorytetem. Różnorodne organizacje mają możliwość komunikowania się ze społeczeństwem zarówno poprzez organizowanie kampanii i akcji społecznych, jak i poprzez kampanie w Internecie. Możliwości w dobie XXI wieku jest naprawdę wiele. Jednak liczne działania i inicjatywny wymagają przede wszystkim wsparcia w wymiarze technicznym. Niezbędne jest więc:

- rozbudowywanie systemów służących do wczesnego ostrzegania przed atakami,
- zastosowanie dodatkowych rozwiązań o podłożu prewencyjnym,
- wysoki poziom ochrony najważniejszych systemów teleinformatycznym,
- organizowanie specjalnych ćwiczeń, które pozwolą ocenić odporność infrastruktury na możliwe ataki cybernetyczne,
- dążenie do tego, aby skonsolidowano dostęp do usług publicznych,
- rozbudowa Rządowego Zespołu Reagowania na Incydenty Komputerowe,
- opracowanie odpowiedniego planu służącego wykorzystaniu systemu powszechnej komunikacji w sytuacjach kryzysowych, co pozwoli skutecznie przeciwdziałać skutkom ewentualnych incydentów,
- tworzenie rozwiązań o charakterze zapasowym, czyli takich za pośrednictwem, których możliwe będzie skuteczne przejęcie zadań infrastruktury krytycznej, jeżeli podstawowe systemy będą z jakichś względów niedostępne[49].

Innym skutecznym rozwiązaniem, które może wpłynąć efektywnie na wzrost bezpieczeństwa cyberprzestrzeni jest angażowanie możliwie najszerszego grona użytkowników sieci globalnej. Bowiem dzięki świadomości zagrażających niebezpieczeństw będą oni w stanie skutecznie chronić cyberprzestrzeń. Poza tym konieczne jest ciągłe szkolenie specjalistów i ekspertów, którzy na co dzień w swojej pracy zajmują się właśnie cyberbezpieczeństwem. Chodzi przede wszystkim o specjalistów bezpieczeństwa teleinformatycznego, jak i kadrę urzędniczą, która musi znać procedury ochronne. To samo tyczy się racjonalizowania programów związanych z kształceniem studentów. Warto jest zadbać w tym zakresie o różnorodne działania konsultacyjne i doradcze[50]. Pomocna może być współpraca z przedsiębiorstwami trudniącymi się na co dzień problematyką bezpieczeństwa teleinformatycznego.

[49] *Ibidem*.
[50] C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo*, Wolters Kluwer Polska, Warszawa 2020, s. 108.

Wszystkie działania, do których się odniesiono są niezwykle istotne. Ważne jest aby odpowiednie podmioty przykładały do nich dużą wagę. Problematyki cyberzagrożeń nie można w najmniejszym nawet stopniu bagatelizować. Jednak do kategorii czołowych przedsięwzięć mających realny wpływ na podniesienie poziomu bezpieczeństwa w cyberprzestrzeni są kampanie społeczne przejawiające charakter edukacyjno-prewencyjny. Takich kampanii powinno być coraz więcej, tak by możliwe było dotarcie do, jak największego grona użytkowników Sieci internetowej. Podsumowując powyższe wskazania należy zaznaczyć, że poszczególne badania i prace rozwojowe powinny determinować powstawanie innowacyjnych metod oraz technik do analizowania cyberzagrożeń i skutecznego im przeciwdziałania.

Zakończenie

Cyberprzestrzeń stanowi współcześnie nowe środowisko bezpieczeństwa. Dlatego też konieczne jest wdrażanie nieustannych przeobrażeń, które wpłyną pozytywnie na podniesienie poziomu bezpieczeństwa w tym zakresie. Jednym z najpoważniejszych zagrożeń, do jakich dochodzi w cyberprzestrzeni jest cyberterroryzm. Stanowi on zagrożenie dla państwa, jak i zamieszkujących go obywateli.

Dzięki dokonanej analizie problemu badawczego przy pomocy właściwie dobranych metod badawczych możliwe stało się zweryfikowanie hipotezy badawczej, która zakładała, że opracowanie odpowiednich środków oraz przyjęcie właściwej struktury instytucjonalnej i organizacyjnej skutecznie mogą przeciwstawiać się temu zagrożeniu. W związku z faktem, że cyberterroryzm stanowi coraz poważniejsze zagrożenie zarówno dla instytucji państwa jak i społeczeństwa w wielu płaszczyznach, ukazano wybrane ważniejsze instrumenty prawne oraz organizacyjne zapewniające do ograniczania zagrożenia w cyberprzestrzeni. w tym ekonomicznej, społecznej, prawnej, politycznej. Hipotezę udało się potwierdzić, a cele pracy zrealizować.

Dzięki analizie materiałów źródłowych, aktów prawa międzynarodowego oraz krajowych regulacji, w połączeniu z wykorzystaniem teoretycznych rozważań nad obranym zagadnieniem udało się znacząco poszerzyć wiedzę odbiorców na temat cyberterroryzmu i zagrożeń, jakie są z nim związane.

Podniesienie poziomu cyberbezpieczeństwa wymaga podjęcia licznych działań. Jednak kluczowe jest to, aby świadomość społeczna związana z zagrożeniami w cyberprzestrzeni znacząco wzrosła. Dzięki posiadaniu wysokiej świadomości w tym zakresie możliwe jest uchronienie siebie i najbliższego otoczenia.

Bibliografia

Aleksandrowicz T., *Świat w sieci. Państwa, społeczeństwa ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, PWN, Warszawa 2018.

Apanowicz J., *Metodologia ogólna,* Wydawnictwo Bernardium, Gdynia 2002.

Banasiński C., *Cyberbezpieczeństwo. Zarys wykładu.,* Wolters Kluwer, Warszawa 2018.
Banasiński C., Rojszczak M., *Cyberbezpieczeństwo,* Wolters Kluwer Polska, Warszawa 2020.
Bielski K., *Cyberterroryzm – nowe zagrożenie bezpieczeństwa państwa w XXI wieku*, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Acta Politica Nr 34, nr 889/2015
Biernacik B., Kalman L., *Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polskiej – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, ASzWoj, Warszawa 2016.
Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Difin, Warszawa 2013.
Chabasińska A., Czachów Z.., *Bezpieczeństwo Narodowe Polski. Zagrożenia i determinanty zmian*, wyd. Difin, Warszawa 2016.
Denning D., *Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services,* U.S. House of Representatives, Georgetown University, Washington 2000.
Dutkiewicz W., *Podstawy metodologii badań do pracy magisterskiej i licencjackiej z pedagogiki*, wydawnictwo Stachurski, Kielce 2000.
Fehler W., *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne*, Wyd. Arte, Warszawa 2015.
Frączek M., *Wybrane aspekty bezpieczeństwa cybernetycznego SZRP*, AON, Warszawa 2014.
Gajewski J., Paprocki W., Pieriegud J., *Cyfryzacja gospodarki i społeczeństwa – szanse i wyzwania dla sektorów infrastrukturalnych,* Gdańska Akademia Bankowa, Gdańsk 2018.
https://machnacz.eu/83-infrastruktura-krytyczna/121-cyberterroryzm-a-przestepczosc-zorganizowana [dostęp 15.08.2022].
https://prokonsumencki.pl/obowiazki-informacyjne-sprzedawcy/rodo-w-sklepie-internetowym-wszystko-co-musisz-wiedziec-tylko-przydatne-informacje/ [dostęp 02.08.2022].
https://www.arakis.pl/#nask, [dostęp 12.06.2022].
https://www.iab.org.pl/aktualnosci/iab-polska-partnerem-kampanii-cyberbezpieczenstwa-cyberliga/, [dostęp 23.07.2022].
Jakubczak R., Marczak J., Gąsiorek K., Jakubczak J., *Podstawy bezpieczeństwa narodowego Polski w erze globalizacji*. Wyd. Akademia Obrony Narodowej, Warszawa 2008.
Jakubowska P., Krajowy system cyberbezpieczeństwa funkcjonuje, ale wymaga ulepszeń, https://www.prawo.pl/ biznes/krajowy-system-cyberbezpieczenstwa.pl., [dostęp 15.07.2022].
Kardas P., *Oszustwo komputerowe w kodeksie karnym*, „Przegląd Sadowy" 2011/11.
Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System.,* PWN, Warszawa 2015.
Komisja Europejska, Wspólny Komunikat do Parlamentu Europejskiego i Rady, Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN (2020) 18, wersja ostateczna, 16.12.2020
Konwencja Rady Europy o zwalczaniu cyberprzestępczości, uchwalona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. 2015, poz. 728
Kośla R., *Cyberterroryzm – definicja zjawiska i zagrożenie dla Polski*, Ossolineum, Wrocław 2017.
Łakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii,* UW, Warszawa 2013.
Lewis J., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, Washington 2002.
Lichocki E., *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, PWN, Warszawa 2013.
Liderman K., *Bezpieczeństwo informatyczne. Nowe wyzwania,* PWN, Warszawa 2020.
Lis W., *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej,* KUL, Lublin 2016.
Lis W., *Współczesne zagrożenia bezpieczeństwa państwa*, KUL, Lublin 2018.
Łobocki M., *Wprowadzenie do metodologii badań pedagogicznych*, Impuls, Kraków 2007.
Madej M., Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.
Malak K., *Bezpieczeństwo polityczne i wojskowe,* Difin, Warszawa 2019.
Malec M., *Percepcja bezpieczeństwa: definicje, wymiary, paradygmaty*, Wyd. Ministerstwo Obrony Narodowej, Warszawa 2012.
Misiuk A.*, Administracja spraw wewnętrznych w Polsce (od połowy XVIII wieku do współczesności). Zarys dziejów*, Olsztyn 2005.
Misiuk A., *Administracja spraw wewnętrznych w Polsce. Zarys dziejów,* Olsztyn 2005.
Misiuk A., *Rzecz o bezpieczeństwie – geneza, istota, rozwój,* UW, Warszawa 2012.

Molendowska M., Miernik R., *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia,* Wydawnictwo Adam Marszałek, Warszawa 2021.
myslenice.pl, [dostęp 23.07.2022].
nowastrategia.org.pl, [dostęp 12.05.2022].
Palka S., *Metodologia, badania, praktyka pedagogiczna,* Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2013.
Pieprzny S., *Ochrona bezpieczeństwa i porządku publicznego w prawie administracyjnym*, Wyd. Uniwersytetu Rzeszowskiego, Rzeszów 2009.
Pikulski S., *Podstawowe zagadnienia bezpieczeństwa publicznego,* Szczytno 2013.
Pilch T., Bauman T., *Zasady badań pedagogicznych. Strategie jakościowe i ilościowe,* PWN, Warszawa 2007.
Raport o stanie bezpieczeństwa cyberprzestrzeni RP z 2020 roku, Warszawa 2021.
Sienkiewicz P., *Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym,* AGH, Kraków 2012.
Skorny Z., *Metody badań i diagnostyka psychologiczna,* Ossolineum, Wrocław 2010.
Skrabacz A., Gąsiorek K., *Obrona narodowa w tworzeniu bezpieczeństwa Polski w XXI wieku,* PWN, Warszawa 2017.
Strategia Cyberbezpieczeństwa RP na lata 2019-2024, 2019 r.
Szpyra W., *Bezpieczeństwo militarne państwa,* wyd. Akademii Obrony Narodowej, Warszawa 2012.
Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe Akademii Marynarki Wojennej", 2012/1.
Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe Haking, haktywizm i cyberterroryzm,* PWN, Warszawa 2017.
Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Monitor Polski 2019, poz.1037
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz.1580
Wiśniewski B., Zalewski S., *Bezpieczeństwo wewnętrzne RP w ujęciu systemowym i zadań administracji publicznej,* Bielsko-Biała 2016.
Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego*, SCHOLAR, Warszawa 2013.
Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego*. Wyd. Naukowe SCHOLAR, Warszawa 2004.
Zięba R., *Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych. Sprawy międzynarodowe,* Difin, Warszawa 1999.
Zięba R., Zając J., *Budowa zintegrowanego systemu bezpieczeństwa Polski. Ekspertyza,* Ministerstwo Rozwoju Regionalnego. Warszawa 2010.

Grzegorz Wilk-Jakubowski[1]

Tomasz Konopka[2]

Radosław Harabin[3]

Znaczenie komunikacji w sytuacjach kryzysowych na przykładzie największej w Polsce katastrofy budowlanej hali wystawienniczej Międzynarodowych Targów Katowice z 28 stycznia 2006 r.

Wstęp

Głównym celem niniejszego artykułu jest analiza procesu komunikacji kryzysowej na przykładzie największej w Polsce katastrofy budowlanej, która wydarzyła się 28 stycznia 2006 r. w Chorzowie. W pracy zastosowano kilka metod badawczych. Ich użyteczność została poddana ocenie przez pryzmat przydatności do realizacji wyżej określonego celu. W pierwszej części pracy dominują trzy metody badawcze: historyczna metoda genetyczna, metoda deskryptywna oraz instytucjonalno-prawna, natomiast w drugiej – wykorzystano również metodę decyzyjną oraz komparatystyczną.

W pierwszej części artykułu przedstawiony zostanie problem badawczy organizacji czynności służb ratunkowych oraz logistycznych po wystąpieniu katastrofy budowlanej

[1] Dr hab. Grzegorz Wilk-Jakubowski, prof. ucz., Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach, ORCID ID: 0000-0002-3906-4103

[2] Dr Tomasz Konopka, dziekan, adiunkt, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach

[3] Dr hab. Radosław Harabin, prof. ucz., Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach, ORCID ID: 0000-002-5180-5840

hali wystawienniczej Międzynarodowych Targów Katowice. W drugiej części artykułu przedstawione zostaną działania komunikacyjne przedstawicieli organów władzy publicznej (w szczególności sztabu kryzysowego), z uwzględnieniem zaangażowania polityków (pełniących najwyższe funkcje w państwie). W zakończeniu zaprezentowane zostaną wnioski z przeprowadzonych badań.

Problematyka organizacji działań służb ratunkowych oraz logistycznych po wystąpieniu kryzysu była wielokrotnie podejmowana w literaturze przedmiotu. Przykład mogą stanowić monografie autorstwa Eugeniusza Nowaka[4]. Wartościowa jest również analiza systemu ratowniczego, w tym organizacji i działalności służb ratowniczo-gaśniczych w portach lotniczych Grzegorza Zająca[5]. Równie często badacze podejmowali się przeprowadzania analiz problematyki teoretycznej analizy procesu komunikacji w sytuacjach kryzysowych (publikacje monograficzne w tym zakresie wydali m.in.: Jadwiga Stawnicka, czy Dorota Domalewska[6]). W literaturze naukowej nie był natomiast w ogóle podejmowany problem praktycznego wymiaru komunikacji kryzysowej. Żaden z badaczy nie podjął się też analizy znaczenia procesów komunikacji kryzysowej na przykładzie największej w Polsce katastrofy budowlanej, która wydarzyła się 28 stycznia 2006 r. w Chorzowie. Celem niniejszego artykułu jest zatem wypełnienie luki w literaturze przedmiotu. Niniejszy artykuł stanowi także odpowiedź na postulat organizatorów Konferencji „Awarie Budowlane", aby nie poddawać analizie jedynie przyczyn i przebiegu akcji ratowniczej podjętej na skutek zaistnienia katastrofy budowanej w Chorzowie, lecz skoncentrować uwagę badawczą na niepodjętych jeszcze wątkach, które przyczynić się mogą w przyszłości do podniesienia skuteczności reagowanie kryzysowego[7]. Powyższy cel zostanie osiągnięty poprzez wskazanie we wnioskach propozycji działań doskonalących obieg informacji w przypadku zaistnienia sytuacji kryzysowych.

Działania z zakresu zarządzania kryzysowego podczas katastrofy budowlanej hali wystawienniczej Międzynarodowych Targów Katowice

Największa w Polsce katastrofa budowlana miała miejsce w hali wystawienniczej nr 1 Międzynarodowych Targów Katowice[8]. W chwili zdarzenia – tj. 28 stycznia 2006 r. o godzinie 17[15], kiedy to pod naporem grubej warstwy lodu i śniegu zapadła się środkowa

[4] E. Nowak, *Zarządzanie logistyczne w sytuacjach kryzysowych*, Akademia Obrony Narodowej, Warszawa 2008. E. Nowak, *Logistyka w sytuacjach kryzysowych*, Akademia Obrony Narodowej, Warszawa 2009.

[5] G. Zając, *Instytucjonalne i organizacyjne aspekty bezpieczeństwa w portach lotniczych Rzeczypospolitej Polskiej*, [w:] Przegląd Europejski, vol. 2022, no. 2, ISSN: 1641-2478, s.79-94.

[6] J. Stawnicka, *Komunikacja w sytuacjach kryzysowych*, Oficyna Wydawnicza WW, Katowice 2010. Zob. D. Domalewska, *Wielowymiarowość komunikacji w kontekście bezpieczeństwa. Komunikacja w sytuacjach kryzysowych i komunikacja strategiczna*, Akademia Sztuki Wojennej, Warszawa 2020.

[7] Z. Mendera, *Analiza przyczyn katastrofy hali wystawowej w Katowicach*, „Awarie budowlane" 2007, nr 1, s. 94.

[8] Z. Mendera, *Analiza przyczyn katastrofy hali wystawowej w Katowicach*, [w:] XXIII Konferencja Naukowo-Techniczna Szczecin-Międzyzdroje. *Awarie budowlane – zapobieganie – diagnostyka – naprawy – rekonstrukcje*, Wydawnictwo Uczelniane Politechniki Szczecińskiej, Szczecin 2007, s. 93.

część dachu hali, w obiekcie przebywało 500-700 osób (wystawców i zwiedzających uczestniczących w wystawie gołębi pocztowych oraz innych zwierząt, a także personelu oraz służb technicznych i porządkowych). Zniszczenia objęły obszar o powierzchni ponad 10 000 m^2. Ze względu na fakt, że miejsce katastrofy budowlanej było położone na granicy dwóch miast (Katowic oraz Chorzowa) – zgłoszenia telefoniczne o zdarzeniu napłynęły niemal równocześnie do dwóch miejskich stanowisk kierowania Państwowej Straży Pożarnej oraz Pogotowia Ratunkowego[9]. Dyspozytorzy tych stanowisk zadysponowali na miejsce katastrofy podległe sobie jednostki (w sumie 9 zastępów ratowniczo-gaśniczych), co przyczyniło się do szybszego zwiększenia koncentracji sił ratunkowych. Ponadto na miejsce zdarzenia grupę operacyjną zadysponował również oficer dyżurny Wojewódzkiego Stanowiska Koordynacji Ratownictwa, który o godz. 17[21] otrzymał informację o zawaleniu się dachu hali wystawowej z miejskich stanowisk kierowania PSP z Katowic oraz Chorzowa (postawił on w stan gotowości 3 plutony gaśnicze, pluton ratownictwa drogowego, 3 dźwigi oraz ciężki samochód ratownictwa technicznego, a także powiadomił o zdarzeniu kierownictwo komendy wojewódzkiej PSP, Centrum Koordynacji Ratownictwa Medycznego, Wojewódzkie Centrum Zarządzania Kryzysowego i Wojewódzki Sztab Policji wnioskując o postawienie w stan gotowości podległych im służb)[10].

W pierwszej fazie po wystąpieniu kryzysu działania ratownicze podejmowali jedynie uczestnicy wystawy oraz osoby postronne (ich celem była ewakuacja rannych znajdujących się w strefie zagrożenia)[11]. Pierwsze zastępy ratowniczo-gaśnicze oraz zespoły ratownictwa medycznego pojawiły się na miejscu zdarzenia o godz. 17[30]. Kierowanie działaniami ratowniczymi objął dowódca zmiany – kpt. Ryszard Wolski. Celem podjętych przez niego działań było zabezpieczenie miejsca katastrofy przed powrotem do hali ludzi, którzy wcześniej zdążyli się z niej ewakuować (osoby te usiłowały powrócić na miejsce zdarzenia w celu wydostania spod gruzów innych poszkodowanych). Ponadto przy pomocy sprzętu zgromadzonego na miejscu katastrofy (podnośniki, lewary, poduszki pneumatyczne, piły i urządzenia hydrauliczne do cięcia metalu) rozpoczęto przeprowadzanie akcji ratowniczej mającej na celu ewakuację rannych spod zawalonej części hali oraz udzielenie im pomocy medycznej (w tym celu sprawdzono, czy służby techniczne Międzynarodowych Targów Katowice wyłączyły zasilanie elektryczne w zawalonej hali, a także oświetlono teren akcji). W związku z niedoborem sił i środków zgromadzonych na miejscu katastrofy – Ryszard Wolski poprosił o zadysponowanie

[9] G. Wilk-Jakubowski, *Logistic Management in Crisis Situation*, „VADYBA. Journal of Management" 2014, nr 1(24), s. 73.
[10] W. Błaszczyński, *Funkcjonowanie krajowego systemu ratowniczo-gaśniczego na przykładzie katastrofy budowlanej w Chorzowie*, [w:] *Zarządzanie kryzysowe w Polsce*, red. M. Jabłonowski, L. Smolak, Akademia Humanistyczna imienia Aleksandra Gieysztora, Pułtusk 2007, s. 229-259.
[11] G. Wilk-Jakubowski, *Logistic Management in Crisis Situation*…, s. 74.

dodatkowych zespołów ratownictwa medycznego i technicznego oraz sprzętu (w szczególności dźwigów)[12].

Po dotarciu na miejsce katastrofy grupy operacyjnej Wojewódzkiego Stanowiska Koordynacji Ratownictwa (godz. 17^{35}) – kierowanie działaniami ratowniczymi przejął oficer operacyjny – mł. bryg. Janusz Ciesielski. Podzielił on teren akcji na dwa odcinki bojowe: północy i południowy – w każdym z nich siły ratunkowe miały za zadanie uwolnić przygniecionych przez konstrukcję dachu ludzi i udzielić im pomocy medycznej. Ponadto poprosił o skierowanie na obszar katastrofy dodatkowych sił i środków. W odpowiedzi na jego prośbę na miejsce akcji zadysponowane zostały zastępy ratowniczo-gaśnicze, zastępy ratownictwa technicznego, pluton ratownictwa drogowego oraz dwa plutony gaśnicze. Pomimo znaczącej wielkości potencjału skoncentrowanego na miejscu katastrofy – zgromadzone siły i środki nadal nie umożliwiały efektywnego prowadzenia działań ratowniczych –egzemplifikację może stanowić występowanie przerw w transporcie rannych do szpitali. Poprawę sytuacji w tym zakresie przyniosło dopiero zorganizowanie punktu segregacji rannych (jedynie osoby z najcięższymi obrażeniami były odwożone ambulansami do szpitali; lekko rannym pomoc medyczna była udzielana na miejscu) [13].

Kierownictwo nad działaniami ratunkowymi – bezpośrednio po przybyciu na teren katastrofy (tj. o godz. 17^{50}) – przejął Śląski Komendant Wojewódzki Państwowej Straży Pożarnej – nadbryg. Janusz Skulich. Na jego wniosek Krajowe Centrum Koordynacji Ratownictwa i Ochrony Ludności zadysponowało na teren katastrofy grupy poszukiwawczo-ratownicze z psami (w pierwszej kolejności z Nowego Sącza i Kęt), 80 kadetów ze szkół Państwowej Straży Pożarnej z Częstochowy i Krakowa, zastępy ratownictwa technicznego i dźwigi z terenu województwa małopolskiego i opolskiego oraz grupę psychologów ze Szkoły Głównej Służby Pożarniczej, zaś Centrum Zarządzania Kryzysowego Wojewody – z uwagi na niską temperaturę (–17 st. C) – skierowało na miejsce akcji 2 autobusy i koce, a także zajęło się organizacją ciepłych napojów i posiłków dla służb ratowniczych i pomocniczych[14]. Ponadto na teren katastrofy przybyli funkcjonariusze Policji oraz Straży Miejskiej, którzy otrzymali od kierującego działaniami ratowniczymi zadanie zabezpieczenia terenu przed osobami postronnymi, a także transportowania poszkodowanych do miejsca segregacji, a następnie do zespołów ratownictwa medycznego[15]. Janusz Skulich sformułował również sztab akcji (był on systematycznie uzupełniany o specjalistów przybyłych na miejsce katastrofy), który

[12] Komenda Wojewódzka Państwowej Straży Pożarnej, Analiza zdarzenia dot.: miejsce zagrożenia związane z zawaleniem się dachu hali wystawowej Międzynarodowych Targów Katowickich w Chorzowie przy ulicy Bytkowskiej 1b w dniach 28.01.2006-20.02.2006 r., Katowice 2006.

[13] Informacje na temat wolnych miejsc w szpitalach w poszczególnych miastach były na bieżąco przekazywane zespołom ratownictwa medycznego przez Centrum Koordynacji Ratownictwa Medycznego.

[14] G. Wilk-Jakubowski, *Logistic Management in Crisis Situation…*, s. 74.

[15] Po godz. 20^{15} zadania te wykonywali także żołnierze Żandarmerii Wojskowej z Gliwic i Katowic. Dodatkowo po 21^{25} zajęli się oni organizacją transportu zwierząt uratowanych podczas akcji do jednego z rozłożonych namiotów.

wyznaczył osoby upoważnione do zorganizowania punktów pomocy medycznej, punktu przyjęć sił oraz zabezpieczenia logistycznego (prowadzenie akcji ratunkowej było bowiem uzależnione od pozyskania tarcz do pił spalinowych, paliwa, namiotów pneumatycznych oraz kocy termicznych). Ponadto po pojawieniu się na miejscu zdarzenia pierwszych samochodów kwatermistrzowskich – kierujący działaniami ratowniczymi zlecił rozłożenie namiotów pneumatycznych (umieszczano w nich m.in. zwłoki poszkodowanych, czy też zwierzęta uratowane podczas akcji).

Podkreślić należy, że głównym zadaniem sił ratunkowych na miejscu katastrofy nadal pozostawało w tym czasie: uwalnianie osób spod elementów zawalonej konstrukcji hali (realizację tego zadania wspierała od godz. 21^{10} Małopolska Grupa Poszukiwawczo-Ratownicza z psami, która wskazywała miejsca, w których mogli się znajdować żywi ludzie), przenoszenie poszkodowanych do miejsca segregacji rannych, udzielanie im pierwszej pomocy, a także przekazywanie najciężej rannych zespołom ratownictwa medycznego w celu przetransportowania ich do szpitali. Z kolei aktywność Policji oraz Straży Miejskiej nadal była ukierunkowana na zabezpieczenie terenu akcji ratowniczej przed osobami postronnymi oraz pomoc przy transportowaniu rannych do miejsca segregacji, a następnie do zespołów ratownictwa medycznego (dodatkowo w późniejszym czasie Policja podjęła się organizacji depozytu przedmiotów należących do osób poszkodowanych w katastrofie)[16].

Ostatnia żywa osoba została wyciągnięta spod dachu zawalonej hali o godz. 22^{15}. W tym czasie w akcji ratowniczej uczestniczyło m.in. ok. 300 strażaków Państwowej Straży Pożarnej, 280 funkcjonariuszy Policji, 80 żołnierzy Żandarmerii Wojskowej, 40 strażników miejskich oraz prawie 200 ratowników medycznych i lekarzy (w tym 17 z psami poszukiwawczymi). Ich działalność była skoncentrowana wokół poszukiwania osób żywych, uwalniania ludzi martwych uwięzionych pod zawaloną konstrukcją dachu i przewożenia ich do miejsc składowania zwłok, a następnie do kostnic. Kierujący działaniami ratunkowymi – pomimo jednoznacznej opinii ekspertów – wstrzymywał się do 29 stycznia do godziny 14^{00} z uznaniem, że na obszarze zawaliska znajdują się już wyłącznie osoby martwe. Z tego też powodu na terenie katastrofy nie był używany ciężki sprzęt (np. dźwigi, wyciągarki, czy koparki). Dopiero po tym, gdy kolejne akcje przeszukania miejsca katastrofy przeprowadzone przy wykorzystaniu geofonów oraz psów poszukiwawczych nie doprowadziły do odnalezienia śladów życia, podjął on decyzję o rozpoczęciu procesu stopniowego wycofywania sił. Działania służb od tego momentu koncentrowały się na zabezpieczeniu obiektu przed osobami postronnymi (funkcjonariusze Policji, pracownicy Prokuratury oraz niezależni eksperci prowadzili także czynności mające na celu zebranie i zabezpieczenie śladów mogących ustalić przyczynę zawalenia się hali targowej), zaś aktywność Wojewódzkiego Zespołu Reagowania Kryzysowego

[16] W. Błaszczyński, *Funkcjonowanie krajowego systemu ratowniczo-gaśniczego na przykładzie katastrofy budowlanej w Chorzowie…*, s. 229-259.

skupiała się wokół organizacji wsparcia psychologicznego dla poszkodowanych, ich rodzin i uczestników działań ratowniczych, a także wyboru specjalistycznej firmy do rozebrania hali wystawowej oraz ustaleniu procedury realizacji tego zadania[17].

Początek ostatniej fazy zarządzania kryzysowego (tj. usuwania skutków sytuacji kryzysowej) nastąpił 2 lutego 2006 r. w momencie wprowadzenia na miejsce katastrofy firmy dysponującej ciężkim sprzętem przeznaczonym do realizacji prac rozbiórkowych (tj. Przedsiębiorstwa Budownictwa Ogólnego i Usług Technicznych „Śląsk" sp. z o.o. z Katowic). W tym czasie Janusz Skulich podjął decyzję o przekazaniu kierowania działaniami Komendantowi Miejskiemu PSP w Chorzowie – st. bryg. Edwardowi Gąsowskiemu. W trakcie podjętych w tej fazie prac spod zawalonej konstrukcji hali wydobyto ostatnie 2 ofiary śmiertelne (w sumie spod gruzów wyciągnięto 64 osoby martwe). Na miejscu katastrofy nadal pozostawały zastępy ratownictwa technicznego Państwowej Straży Pożarnej oraz zespół ratownictwa medycznego realizujące zabezpieczenie prac rozbiórkowych. Po ich zakończeniu (tj. po wyciągnięciu wszystkich elementów zawalonej konstrukcji dachu i odkryciu posadzki hali targowej) 20 lutego podjęto decyzję o zakończeniu akcji. Uratowano 140 osób (1 z uratowanych osób zmarła w szpitalu)[18].

Podkreślić należy, że o wysokiej skuteczności działań ratowniczych świadczyć może nie tylko stosunek liczby osób uratowanych w wyniku przeprowadzonej akcji do liczby osób, które poniosły śmierć w wyniku katastrofy, lecz także wyniki analizy obrażeń odniesionych przez poszkodowanych – niemal wszystkie osoby (64 z 65 ofiar śmiertelnych) straciły życie w chwili katastrofy[19].

Komunikacja kryzysowa podczas katastrofy budowlanej w Chorzowie

Zgłoszenia telefoniczne o zdarzeniu napłynęły niemal równocześnie do dwóch miejskich stanowisk kierowania Państwowej Straży Pożarnej oraz Pogotowia Ratunkowego. Jako pierwsze – o godz. 17[18] – informację o zawaleniu się dachu hali wystawowej na terenie Międzynarodowych Targów Katowice otrzymało Miejskie Stanowisko Kierowania PSP w Chorzowie. Dwie minuty później zgłoszenie wpłynęło również do Miejskiego Stanowiska Kierowania PSP w Katowicach. Efektem tych działań było zadysponowanie na miejsce katastrofy 9 zastępów ratowniczo-gaśniczych, a także przekazanie informacji o zdarzeniu do Wojewódzkiego Stanowiska Koordynacji Ratownictwa (WSKR)[20]. Oficer

[17] *Ibidem*.
[18] G. Wilk-Jakubowski, *Logistic Management in Crisis Situation*…, s. 75.
[19] G. Wilk-Jakubowski, *Zarządzanie logistyczne w sytuacjach kryzysowych na przykładzie organizacji zabezpieczenia logistycznego po katastrofie budowlanej w Chorzowie*, [w:] red. W. Saletra, A. Zagórska, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2016, s. 257.
[20] Komenda Wojewódzka Państwowej Straży Pożarnej, *Analiza zdarzenia dot.: miejsce zagrożenia związane z zawaleniem się dachu hali wystawowej Międzynarodowych Targów Katowickich*…, s. 6.

Dyżurny WSKR z kolei powiadomił o katastrofie kierownictwo komendy wojewódzkiej PSP (w tym rzecznika prasowego), a także Wojewódzkie Centrum Zarządzania Kryzysowego, którego działalność koncentrowała się na zapewnieniu obiegu informacji podczas sytuacji kryzysowych. Z podmiotu tego do Wojewódzkiego Stanowiska Koordynacji Ratownictwa o godzinie 19^{50} przekazana została informacja o uruchomieniu linii telefonicznych, pod którymi można było uzyskać informacje na temat osób poszkodowanych w katastrofie[21]. Od początku prowadzenia akcji ratowniczej środki masowego przekazu były informowane o jej przebiegu przez Rzecznika Prasowego Wojewody Śląskiego oraz Rzecznika Prasowego Śląskiego Komendanta Wojewódzkiego PSP w Katowicach, a w późniejszym czasie także przez Rzecznika Prasowego Komendanta Wojewódzkiego Policji w Katowicach, Rzeczników Prasowych prokuratury okręgowej i apelacyjnej oraz przedstawicieli innych służb uczestniczących w działaniach ratowniczych. Najpierw rzecznicy przekazywali sobie informacje drogą telefoniczną, by następnie – po przybyciu na miejsce katastrofy – kontaktować się między sobą osobiście. Początkowo ich aktywność ograniczała się w głównej mierze do informowania dziennikarzy przybyłych na miejsce katastrofy o przebiegu oraz organizacji akcji ratowniczej. W tym celu wyznaczono – zabezpieczane przez funkcjonariuszy Policji – miejsce, w którym reporterom na bieżąco przekazywane były informacje.

Efektem działalności rzeczników był pozytywny ton doniesień medialnych na temat przebiegu oraz organizacji akcji ratowniczej (uwaga środków masowego przekazu początkowo koncentrowała się niemal wyłącznie na akcentowaniu jej sprawności, pozytywnej oceny wyposażenia, a także optymalnej liczebności zgromadzonych na miejscu katastrofy służb)[22].

W późniejszym czasie, w celu usprawnienia przekazu informacji, wyznaczono rzecznika prasowego akcji. Pełnienie tej funkcji powierzono Rzecznikowi Prasowemu Wojewody Śląskiego – Krzysztofowi Mejerowi. Zadania wypełniane przez pozostałych rzeczników prasowych zostały ograniczone do informowania mediów o działaniach własnych jednostek. Zaplanowano także, że wymiana informacji pomiędzy rzecznikami prasowymi odbywać się będzie w nieokreślonych przedziałach czasowych. Przygotowaniem materiałów dla nich zajmowali się pracownicy biur i zespołów prasowych każdej z wymienionych instytucji (tj. Wojewody Śląskiego, Śląskiego Komendanta Wojewódzkiego PSP w Katowicach, Komendanta Wojewódzkiego Policji w Katowicach, prokuratury okręgowej i apelacyjnej oraz przedstawicieli pozostałych służb

[21] *Ibidem*, s. 14.

[22] Przykład może stanowić relacja Marka Czyża z „Wiadomości" wyemitowanych 28.01.2006 r. o godzinie 19^{30}: „Strażacy mają tu wszystko, czym powinni dysponować. Tyle sprzętu ratowniczego nigdy w życiu na oczy nie widziałem (…) jest (…) wszystko, co potrzebne, żeby akcja przebiegała sprawnie". M. Czyż, „Wiadomości", TVP 1, relacja z 28.01.2006, godz. 19^{30}. W relacji tej negatywnie oceniono jedynie brak wyposażenia funkcjonariuszy Policji w latarki. Wątek ten był podejmowany także w późniejszych przekazach medialnych, w których występowały osoby poszkodowane, które przed kamerami twierdziły, że zakupiły i przekazały latarki przybyłym na miejsce funkcjonariuszom Policji. Por. M. Dominiak, *Komunikacja w kryzysie. Emocje, czy chłodna kalkulacja?,* „Piar.pl" 2006, nr 2(8), s. 22-23.

uczestniczących w działaniach ratowniczych). Z uwagi na fakt, że na miejscu katastrofy przebywała duża liczba dziennikarzy – występowała konieczność ciągłego wypowiadania się na temat różnych aspektów prowadzonej akcji ratunkowej przez osoby, które nie posiadały pełnej wiedzy na temat jej przebiegu. Dodatkowy problem stanowiło wykorzystywanie do kontaktów między rzecznikami prasowymi telefonów komórkowych (numery te były powszechnie znane dziennikarzom, a zatem przez cały czas pozostawały zajęte)[23]. Ponadto, ze względu na dużą liczbę uczestników akcji ratunkowej – nie było możliwe określenie osób odpowiedzialnych za kontakty z przedstawicielami środków masowego przekazu we wszystkich grupach ratowniczych[24]. W powyższych okolicznościach wypowiedzi przedstawicieli tych grup zawierały niepełne lub niepotwierdzone informacje o przebiegu prowadzonej akcji ratunkowej. Konieczne było więc dementowanie niektórych wyrażonych przez nich opinii, a także stwierdzeń lub tłumaczenie powodów podjęcia przez kierującego działaniami ratowniczymi określonych decyzji (na przykład odnośnie niedopuszczenia do działań spontanicznie przybywających na teren akcji grup ratowniczych, rezygnacji z wykorzystania grupy poszukiwawczo-ratowniczej z Niemiec, czy też zarzutów o zbyt wczesnym przerwaniu akcji ratowniczej)[25].

Po przybyciu na miejsce katastrofy najważniejszych osób w państwie (m.in. Prezesa Rady Ministrów – Kazimierza Marcinkiewicza, Ministra Zdrowia – Zbigniewa Religi, a następnego dnia także Prezydenta RP – Lecha Kaczyńskiego, podjęto decyzję o zorganizowaniu konferencji prasowych. Nie mogły się one odbyć na terenie Międzynarodowych Targów Katowice z powodu odłączenia energii elektrycznej – dlatego też Rzecznik Prasowy Wojewody Śląskiego wyznaczył Śląski Urząd Wojewódzki w Katowicach jako miejsce ich organizacji. Pierwsza z konferencji odbyła się w dniu 29 stycznia 2006 r. o godzinie 2^{00}. Wzięli w niej udział m.in. premier Kazimierz Marcinkiewicz, członkowie rządu, Wojewoda Śląski – Tomasz Pietrzykowski oraz przedstawiciele służb ratowniczych. Tego samego dnia zorganizowane zostały jeszcze cztery konferencje prasowe, w których uczestniczyli m.in. Wojewoda Śląski – Tomasz Pietrzykowski, Komendant Główny PSP – Kazimierz Krzowski oraz Śląski Komendant Wojewódzki PSP – Janusz Skulich. Podczas wyżej wymienionych konferencji na bieżąco przekazywano informacje na temat aktualnej sytuacji na miejscu katastrofy, tj. przebiegu akcji ratowniczej, skali zaangażowanych sił i środków, zamierzeniach służb ratowniczych, działaniach podejmowanych przez Radę Ministrów i administrację rządową w województwie, a także ilości osób, które zostały ranne oraz straciły życie w wyniku

[23] Komenda Wojewódzka Państwowej Straży Pożarnej, *Analiza zdarzenia dot.: miejsce zagrożenia związane z zawaleniem się dachu hali wystawowej Międzynarodowych Targów Katowickich…*, s. 40.

[24] Już w po dwóch godzinach od wystąpienia analizowanej sytuacji kryzysowej na miejscu znajdowało się ponad 1 300 osób zaangażowanych w prowadzenie akcji ratunkowej. M. Czyż, „Wiadomości", TVP 1, relacja z 28.01.2006, godz. 19^{30}.

[25] Włączenie się do działań z zakresu komunikacji kryzysowej biegle posługującego się językiem niemieckim Kapelana Strażaków Województwa Śląskiego – Henryka Kuczoby – przyczyniło się do bieżącego przekazywania niemieckiej stacji telewizyjnej informacji na temat sytuacji na miejscu katastrofy. Zob. Komenda Wojewódzka Państwowej Straży Pożarnej, *Analiza zdarzenia dot.: miejsce zagrożenia związane z zawaleniem się dachu hali wystawowej Międzynarodowych Targów Katowickich…*, s. 40-42.

zawalenia się dachu hali[26]. W związku z podjęciem decyzji o rezygnacji z organizacji konferencji prasowych w kolejnych dniach – ostatnie tego rodzaju wydarzenie odbyło się 29 stycznia o godzinie 16^{00}. Zadanie przekazywania bieżących informacji środkom masowego przekazu zostało nałożone na poszczególnych rzeczników prasowych, osoby kierujące działaniami ratowniczymi, a także rzeczników prasowych podmiotów upoważnionych do ustalenia przyczyn zawalenia się dachu. Koordynację przekazu informacji w tym zakresie powierzono Rzecznikowi Prasowemu Wojewody Śląskiego.

Koordynator Wojewódzkiego Stanowiska Koordynacji Ratownictwa po otrzymaniu listy rannych osób, które ucierpiały w katastrofie, zlecił niezwłocznie utworzenie punktu informacyjnego w Komendzie Wojewódzkiej PSP w Katowicach dla osób poszukujących wiadomości na temat stanu zdrowia swoich krewnych, którzy uczestniczyli w wystawie. Informacja o wydzielonym numerze telefonu, pod którym przekazywano wiadomości o stanie rannych, a także miejscu ich hospitalizacji, została udostępniona środkom masowego przekazu 29 stycznia o godz. 4^{30}. Dane te były w późniejszym czasie systematycznie aktualizowane przez Centrum Koordynacji Ratownictwa Medycznego oraz Wojewódzkiego Centrum Zarządzania Kryzysowego. Podmioty te zaangażowane były również w prowadzenie działalności komunikacyjnej w szerszym wymiarze. Pierwszy z nich – Centrum Koordynacji Ratownictwa Medycznego – zajmował się przekazywaniem wiadomości o stanie oraz liczbie poszkodowanych osób rzecznikowi prasowemu Wojewody Śląskiego, a także mediom, informował także za ich pośrednictwem o możliwości oddawania krwi dla ofiar katastrofy[27]. Z kolei drugi z wymienionych podmiotów – Wojewódzkie Centrum Zarządzania Kryzysowego – udostępniał informacje na temat przebiegu akcji ratowniczej, ilości sił i środków zaangażowanych w prowadzone działania, a także gromadził oraz dostarczał sztabowi akcji wiadomości na temat deklarowanej przez wolontariuszy pomocy oraz użyczonego specjalistycznego sprzętu, paliwa, czy przekazanych środków finansowych. O ile informacje na temat osób, które zostały ranne – jak już wskazano wyżej – były przekazywane przez koordynatora Wojewódzkiego Stanowiska Koordynacji Ratownictwa, o tyle wiadomości na temat poszkodowanych, którzy zmarli na skutek katastrofy, udzielała Prokuratura w Chorzowie[28].

W późniejszym czasie system koordynacji obiegu informacji na temat podejmowanych działań został oparty na pracy ośmioosobowego zespołu. Celem pierwszego z podzespołów (czteroosobowego) było utrzymywanie stałej łączności z kierującym działaniami ratowniczymi (w tym także wykonywanie jego poleceń) oraz przekazywanie informacji na temat podjętych działań do Urzędu Wojewódzkiego oraz Krajowego Centrum Koordynacji Ratownictwa i Ochrony Ludności. Zadaniem drugiego

[26] *Ibidem*, s. 18-21.
[27] *Ibidem*, s. 35, 40.
[28] *Ibidem*, s. 19.

podzespołu (dwuosobowego) było koordynowanie obiegu informacji na temat dyspozycyjności sprzętu możliwego do wykorzystania podczas prowadzonej akcji. Zespół ten zajmował się także realizacją nadzoru nad funkcjonowaniem informatycznego sytemu wspomagania decyzji. Ponadto jedna osoba została wydelegowana do Centrum Zarządzania Kryzysowego Wojewody Śląskiego w celu zapewnienia przepływu informacji pomiędzy Urzędem Wojewódzkim a Komendą Wojewódzką Państwowej Straży Pożarnej. Ostatnia z osób otrzymała zadanie utrzymywania stałego kontaktu z środkami masowego przekazu oraz instytucjami i osobami prywatnymi oferującymi swoją pomoc. W późniejszym czasie udzielała ona również informacji o osobach poszkodowanych[29].

Problem katastrofy na terenie Międzynarodowych Targów Katowickich znajdował się przez wiele tygodni w centrum zainteresowania mediów krajowych i zagranicznych. W samej tylko prasie opublikowanych zostało ponad 300 artykułów na ten temat[30]. Mimo konieczności działania pod presją czasu, koordynacja obiegu informacji między służbami zaangażowanymi w prowadzenie akcji ratowniczej przebiegała prawidłowo. Sprzyjało temu powołanie w 2002 r. Wojewódzkiego Centrum Koordynacji Ratownictwa Medycznego, które to zajmowało się koordynacją działań służb medycznych ze strażą pożarną, policją, ratownikami górskimi i Wojewodą Śląskim. Odnotować trzeba, że działania informacyjne sztabu kryzysowego były podejmowane *ad hoc*, gdyż nie istniały wówczas przepisy prawne regulujące sposób ich funkcjonowania[31]. Wątek ten podjęty został chociażby w artykule w Newsweeku: „System działa, chociaż wciąż nie ma przepisów regulujących jego funkcjonowanie (…) Na Śląsku zwyciężył zapał i rozsądek ludzi, przyzwyczajonych do sytuacji kryzysowych"[32]. Pokłosiem sprawnie działającego systemu koordynacji informacji między służbami był fakt, że w zgodnej opinii ekspertów udzielających wywiadów w mediach, żadna z osób poszkodowanych nie zmarła w wyniku wychłodzenia[33]. Pozytywnie ocenić należy także działania z zakresu komunikacji ze środkami masowego przekazu. Szybko otrzymywały one wiarygodne informacje z miejsca katastrofy. Podstawowe źródło wiadomości dla mediów stanowili rzecznicy prasowi, a także osoby wyznaczone do koordynacji obiegu informacji przez sztab kryzysowy. Z tego też względu w zdecydowanej większości relacji podsumowujących przeprowadzoną akcję ratunkową dominowały oceny pozytywne. Podkreślano, że media były na bieżąco szczegółowo informowane o tym, jakie jednostki brały udział w akcji ratunkowej, jakie działania podejmowały, a także jaki był stan ofiar i osób poszkodowanych, a medialne spekulacje odnośnie ewentualnych nieprawidłowości były w przekonywający sposób prostowane. Dla przykładu zarzuty dotyczące przedwczesnego zakończenia działań

[29] *Ibidem*, s. 37.
[30] *Ibidem*, s. 48.
[31] Ustawa o zarządzaniu kryzysowym została uchwalona dopiero rok później. Zob. Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym*, Dz.U. 2007, nr 89, poz. 590 z późn. zm.
[32] *W Chorzowie na końcu świata, „*Newsweek" z dn. 12.02.2006 r. Cyt. za: M. Dominiak, *Komunikacja w kryzysie…*, s. 22.
[33] *Ibidem*.

ratunkowych były odpierane nie tylko przez Janusza Skulicha – Śląskiego Wojewódzkiego Komendanta PSP, lecz także Ministra Zdrowia – Zbigniewa Religę[34].

Pozytywnie ocenić należy także udział polityków w proces komunikacji kryzysowej. W przeciągu kilku pierwszych godzin po zaistnieniu analizowanej sytuacji kryzysowej wypowiedzi do mediów udzielił zarówno Prezes Rady Ministrów – Kazimierz Marcinkiewicz, Ministra Zdrowia – Zbigniew Religa, Minister Transportu i Budownictwa – Jerzy Polaczek, jak i Prezydent RP – Lech Kaczyński. W publicznych wystąpieniach najwyższych osób w państwie zawarte były zarówno słowa współczucia dla najbliższych ofiar, wyważona ocena bieżącej sytuacji, planowana pomoc dla poszkodowanych, jak i obietnica wyjaśnienia przyczyn katastrofy. W celu udzielenia wsparcia rodzinom osób, które zginęły w wyniku katastrofy, Prezydent RP przekazał milion złotych zaoszczędzonych z wydatków bieżących Kancelarii Prezydenta. Analogiczne wsparcie zadeklarował Marszałek Sejmu – Marek Jurek oraz Prezes Rady Ministrów – Kazimierz Marcinkiewicz. Ostatni z wymienionych polityków poinformował także o przyznaniu rodzinom osób, które zginęły w wyniku katastrofy rent specjalnych oraz o ich pochowaniu na koszt państwa. Przedstawiciele władzy odwołali także wizyty zagraniczne (np. Marszałek Sejmu zrezygnował z wylotu do Rzymu, a Prezydent z zaplanowanej podróży do Pragi)[35].

Wnioski

Z przeprowadzonych analiz wynika, że koordynacja obiegu informacji między służbami zaangażowanymi w prowadzenie akcji ratowniczej przebiegała prawidłowo. Pozytywnie ocenić należy także działania z zakresu komunikacji podjęte przez rzeczników prasowych i inne osoby wyznaczone do koordynacji obiegu informacji przez sztab kryzysowy oraz przedstawicieli świata polityki. Przyczyniły się one do tego, że w zdecydowanej większości relacji medialnych dotyczących przeprowadzonych działań ratowniczych dominowały oceny pozytywne.

Na podstawie przeprowadzonych analiz wskazać można także propozycje działań doskonalących: (1) wyeliminować należy przekazywanie przez wiele osób z różnych

[34] Janusz Skulich wyjaśniał: „Zanim (…) podjąłem tę decyzję, rozmawiałem z lekarzami oraz specjalistami ratownictwa medycznego. Ich zdaniem przy temperaturze minus 15 stopni niemal niemożliwe jest, aby ktokolwiek przeżył. Poza tym zawalisko prześwietlono specjalnymi kamerami i geofonami". Zob. „Wiadomości", TVP 1, relacja z 30.01.2006, godz. 19^{30}. W podobnym tonie wypowiedział się Zbigniew Religa: „Hipotermia w takiej temperaturze jest oczywista. (…) Jestem pod ogromnym wrażeniem organizacji całego przedsięwzięcia, organizacji pomocy w tym niebywałym dramacie". Por. M. Marklowska, *Czas ratowania,* „Służba zdrowia" 2006, nr 9-13, s. 3 i n. Za największy błęd podczas działań komunikacyjnych uznać należy brak zastosowania zasady *double chceck* podczas przekazywania wiadomości o liczbie ofiar śmiertelnych (w niedzielę 30 stycznia początkowo ogłoszono, że w wyniku katastrofy życie straciło 67 osób, by w późniejszym czasie jeszcze tego samego dnia poinformować o 62 osobach zmarłych i 5 zaginionych). P. Guła, J. Prońko, B. Wiśniewski, *Zarządzanie informacją w sytuacjach kryzysowych,* Wyższa Szkoła Administracji w Bielsku-Białej, Bielsko-Biała 2009, s. 31-32.

[35] M. Dominiak, *Komunikacja w kryzysie…*, s. 32. Zob. też: „Wiadomości", TVP 1, relacja z 29.01.2006, godz. 19^{30}.

ośrodków informacyjnych wykluczających się informacji odnośnie organizacji i prowadzenia akcji ratowniczej – zadanie to powinien przejąć zespół ds. kontaktów z mediami, do którego zadań należeć powinno przygotowywanie stosownych komunikatów, (2) optować warto na rzecz opracowania procedury uruchamiania linii telefonicznej, pod którą można byłoby uzyskiwać informacje na temat osób poszkodowanych w danej sytuacji kryzysowej, celem jak najszybszego przekazania wiadomości członkom ich rodzin (rozwiązanie to zastąpić powinno dotychczasowe sposoby postępowania w sytuacjach kryzysowych zakładające funkcjonowanie kilku osobnych linii upoważnionych do przekazywania informacji wyłącznie o osobach rannych, czy też ofiarach śmiertelnych), bezwzględnie przestrzegać należy wreszcie zasady *double check* podczas komunikacji kryzysowej – przyczyni się to do ograniczenia niepotrzebnych emocji, które i tak zazwyczaj towarzyszą sytuacjom kryzysowym.

Bibliografia

Błaszczyński W., *Funkcjonowanie krajowego systemu ratowniczo-gaśniczego na przykładzie katastrofy budowlanej w Chorzowie*, [w:] *Zarządzanie kryzysowe w Polsce*, red. M. Jabłonowski, L. Smolak, Akademia Humanistyczna imienia Aleksandra Gieysztora, Pułtusk 2007.

Domalewska D., *Wielowymiarowość komunikacji w kontekście bezpieczeństwa. Komunikacja w sytuacjach kryzysowych i komunikacja strategiczna*, Akademia Sztuki Wojennej, Warszawa 2020.

Dominiak M., *Komunikacja w kryzysie. Emocje czy chłodna kalkulacja?*, „Piar.pl" 2006, vol. 8, nr 2.

Guła P., Prońko J., Wiśniewski B., *Zarządzanie informacją w sytuacjach kryzysowych,* Wyższa Szkoła Administracji w Bielsku-Białej, Bielsko-Biała 2009.

Komenda Wojewódzka Państwowej Straży Pożarnej, *Analiza zdarzenia dot.: miejsce zagrożenia związane z zawaleniem się dachu hali wystawowej Międzynarodowych Targów Katowickich w Chorzowie przy ulicy Bytkowskiej 1b w dniach 28.01.2006-20.02.2006 r.,* Katowice 2006.

Marklowska M., *Czas ratowania,* „Służba zdrowia" 2006, nr 9-13.

Mendera Z., *Analiza przyczyn katastrofy hali wystawowej w Katowicach*, „Awarie budowlane" 2007, nr 1.

Nowak E., *Logistyka w sytuacjach kryzysowych*, Akademia Obrony Narodowej, Warszawa 2009.

Nowak E., *Zarządzanie logistyczne w sytuacjach kryzysowych*, Akademia Obrony Narodowej, Warszawa 2008.

Stawnicka J., *Komunikacja w sytuacjach kryzysowych*, Oficyna Wydawnicza WW, Katowice 2010.

Ustawa *o zarządzaniu kryzysowym* z dnia 26 kwietnia 2007 r., Dz.U. 2007, poz. 89, nr 590 z późn. zm.

Wilk-Jakubowski G., *Logistic Management in Crisis Situation,* „VADYBA. Journal of Management" 2014, nr 1(24).

Wilk-Jakubowski G., *Zarządzanie logistyczne w sytuacjach kryzysowych na przykładzie organizacji zabezpieczenia logistycznego po katastrofie budowlanej w Chorzowie*, [w:] red. W. Saletra, A. Zagórska, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2016.

„Wiadomości", TVP 1, relacja z 28.01.2006, godz. 19[30].

„Wiadomości", TVP 1, relacja z 29.01.2006, godz. 19[30].

„Wiadomości", TVP 1, relacja z 30.01.2006, godz. 19[30].

*W Chorzowie na końcu świata, „*Newsweek" z dn. 12.02.2006 r.

Zbigniew Filip[1]

„Walka" ośrodków pomocy społecznej z pandemią koronawirusa SARS-COV-2 (COVID-19) na przykładzie Miejskiego Ośrodka Pomocy Społecznej w Nowym Sączu

Streszczenie

Pandemia koronawirusa SARS-CoV-2 (COVID-19) to bardzo trudny czas, przede wszystkim ze względu na problemy zdrowotne, a także społeczne, psychologiczne i ekonomiczne. Naruszyła ona porządek społeczny i gospodarczy i sparaliżowała wiele dziedzin życia. Wszystkie państwa dążąc do zminimalizowania skutków kryzysu dla obywateli podjęły walkę o zdrowie publiczne przy pomocy różnorodnych działań, które miały powstrzymać rozprzestrzenianie się wirusa. Ogromna skala problemu, trudny, pandemiczny przebieg choroby i złożona patogeneza[2] zakażenia oraz brak skutecznej profilaktyki i skutecznych leków, a także negowanie przez niektóre środowiska tego występującego problemu stanowią ogromne wyzwanie nie tylko dla pracowników służby zdrowia, czy rządów, ale także dla całych światowych społeczeństw. Temat pandemii koronawirusa SARS-CoV-2 jest coraz szerzej poruszany w literaturze przedmiotu, choćby w kontekście wpływu pandemii koronawirusa na działalność organizacji pozarządowych[3]. Brak jest jednak opracowań, które w przejrzysty sposób przedstawiałby ten temat

[1] Mgr Zbigniew Filip, wykładowca, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach; urzędnik Wydziału Zarządzenia Kryzysowego Urzędu Miasta Nowego Sącza.

[2] Patogeneza to elementy i środki, które powodują powstawanie i rozwój chorób. Patogeneza jest dziedziną patologii, która bada powstawanie i rozwój stanów chorobowych, jak również pochodzenie chorób i przyczyny, które doprowadziły do rozwoju choroby - https://znaczenia.com.pl/znaczenie-patogeneza-co-to-jest-pojecie-i-definicja-znaczenia/ [dostęp 28.06.2022].

[3] Zob. szerzej w: G. Zając, *Wpływ pandemii koronawirusa na działalność organizacji pozarządowych a bezpieczeństwo lokalnych społeczności,* [w:] G. Górski, A. Potoczek (red.), *Bezpieczeństwo lokalne – wybrane problemy teorii i praktyki*, Toruń 2022, s. 229-252

z podziałem na jednostki bezpośrednio realizujące zadania związane z wystąpieniem pandemii. Autor w poniższym artykule postara się przedstawić jakie zadania realizowane były przez ośrodki pomocy społecznej w walce z koronawirusem SARS-CoV-2.
Słowa kluczowe: ośrodki pomocy społecznej, pandemia, koronawirus SARS-CoV-2, COVID-19.

Abstract

The SARS-CoV-2(COVID-19) coronavirus pandemic has been a very difficult time, primarily because of health problems, as well as social, psychological and economic problems. It has disrupted the social and economic order and paralyzed many areas of life. All countries, in an effort to minimize the impact of the crisis on citizens, have taken up the fight for public health with a variety of measures to stop the spread of the virus. The enormous scale of the problem, the difficult, pandemic course of the disease and the complex pathogenesis of the infection, as well as the lack of effective prophylaxis and effective drugs, as well as the denial by some quarters of the problem, pose a formidable challenge not only to health professionals or governments, but also to entire global societies. The topic of the SARS-CoV-2 coronavirus pandemic is increasingly discussed in the literature, but there are no studies that would clearly present this topic with a breakdown into units directly implementing tasks related to the occurrence of the pandemic. The author in the following article will try to present what tasks were carried out by social welfare centers in the fight against SARS-CoV-2 coronavirus.
Keywords: social care centers, pandemic, SARS-CoV-2 coronavirus, COVID-19.

Wstęp

Rok 2020 postawił przed całym światem wyzwanie porównywane przez wielu do epidemii grypy hiszpanki sprzed niemal równo stu lat – pandemię koronawirusa SARS-CoV-2. To nowe zjawisko (zagrożenie) zmieniło życie społeczeństwom na całym świecie poprzez wprowadzanie nowych zakazów i ograniczeń społecznych, gospodarczych i innych[4]. Nowy wirus, o objawach podobnych do sezonowej grypy, wzbudzał międzynarodowe obawy z powodu swojej wysokiej zakaźności oraz trudności identyfikacji, a tym samym brakiem skutecznego monitorowania przypadków zakażenia. Eksperci na całym świecie szybko ruszyli do badań i poszukiwań skutecznego leku, a władze kolejnych krajów zaczęły wprowadzać obostrzenia mające na celu zmniejszenie ilości ofiar śmiertelnych i ograniczenie rozprzestrzeniania się wirusa. Mimo że wielu epidemiologów krytykuje medialną panikę otaczającą koronawirus SARS-CoV-2 (COVID-19) oraz sensowność niektórych rozwiązań, istnienie epidemii nie może być poddawane w wątpliwość.

W tym trudnym okresie jednostki samorządu terytorialnego w tym podległe ośrodki pomocy społecznej stanęły na wysokości zadania, przygotowując środki ochrony osobistej, finansując zakup testów oraz organizując programy pomocy społecznej dla mieszkańców przebywających na administrowanym terenie. Dzięki współpracy ze służbą zdrowia, Strażą Pożarną, Policją oraz Strażą Miejską/Gminną, ośrodki pomocy społecznej mogły dotrzeć ze swoją pomocą do wielu osób, ale propagacja informacji o programach pomocy mogłaby

[4] *Ibidem*, s. 232.

być lepiej zorganizowana co skutkowało by lepszym dostępem do osób potrzebujących. Nieocenioną pomocą była także organizacja punktów izolacji dla powracających z emigracji, polowych punktów testów oraz hotelu dla pracowników służb medycznych. Dzięki odpowiedniej koordynacji prac, obywatele otrzymali szeroki wachlarz pomocy i miejmy nadzieję, że są z niego zadowoleni.

Działania podejmowane przez Miejski Ośrodek Pomocy Społecznej w Nowym Sączu (MOPS) na przełomie 2019 i 2020 r.

MOPS w Nowym Sączu analizując powstałe zagrożenie, Zarządzeniem Dyrektora w marcu 2020 r. powołał Zespół odpowiedzialny za bieżącą analizę i realizację zadań w związku z wystąpieniem choroby zakaźnej COVID-19, którego przeznaczeniem było m.in.:

1. opracowanie planu działania związanego z koniecznością zidentyfikowania oraz zabezpieczenia pomocy osobom i rodzinom objętym kwarantanną, które wymagają wsparcia pomocą społeczną, w tym m.in. w formie posiłku lub produktów żywnościowych, zakupu leków oraz wsparcia w postaci interwencji kryzysowej oraz specjalistycznego poradnictwa psychologicznego,
2. opracowanie planu dotyczącego sposobu zakupu oraz dostarczania produktów żywnościowych, leków lub innych niezbędnych środków – osobom objętym kwarantanną,
3. opracowanie innych planów działań niezbędnych w celu realizacji zadań związanych z wystąpieniem choroby zakaźnej,
4. współdziałanie z jednostkami miasta oraz wszelkimi instytucjami, organizacjami i stowarzyszeniami w zakresie realizowanych zadań,
5. całodobowa współpraca z Wydziałem Zarządzania Kryzysowego Urzędu Miasta Nowego Sącza.

W siedzibie Ośrodka przygotowano w miejscach ogólnodostępnych płyny do dezynfekcji rąk, pracowników wyposażono w maseczki ochronne, przyłbice, zainstalowano pleksy ochronne na stanowiskach do obsługi bezpośredniej petenta.

Kolejno wprowadzono „Procedury bezpieczeństwa i ochrony zdrowia osób pracujących w Miejskim Ośrodku Pomocy Społecznej w Nowym Sączu w trakcie trwania stanu epidemii COVID-19/zagrożenia epidemicznego COVID-19", w których zostały wskazane rozwiązania zapobiegające rozprzestrzenianiu się szkodliwych czynników biologicznych, środki zastosowane w celu ograniczenia prawdopodobieństwa zarażenia koronawirusem SARS-CoV-2, zasady higieny w miejscu pracy, postępowanie w przypadku podejrzenia zachorowania na COVID-19, komunikowanie się w sprawach związanych z działaniami wdrażanymi w celu ograniczenia prawdopodobieństwa zarażenia koronawirusem SARS-CoV-2 w pracy, jak również procedury dotyczące organizacji zajęć

w Dziale Centrum Sądeckiego Seniora oraz funkcjonowanie Działu Dzienny Dom Seniora w trakcie trwania epidemii COVID-19/zagrożenia epidemicznego COVID-19.

Opracowany i wdrożony został również „Regulamin pracy zdalnej", tym samym umożliwiono pracownikom wykonywanie pracy w tej formie, który podlegał aktualizacji w miarę potrzeb i możliwości Ośrodka. Pracownicy socjalni zgodnie z zaleceniami Wojewody Małopolskiego z dnia 12 marca 2020 r. zostali zobowiązani do bieżącego monitorowania w swoich rejonach sytuacji osób starszych, w szczególności chorych i samotnych pod kątem zabezpieczenia ich potrzeb, zapewniali pomoc osobom tego wymagającym, w ramach ustawy o pomocy społecznej w formie posiłków, produktów żywnościowych, zakupu leków. Dokonano również uregulowania funkcjonowania Działu – Ośrodek Interwencji Kryzysowej w związku z rozprzestrzenianiem się koronawirusa SARS-CoV-2. Ośrodek Interwencji Kryzysowej w Nowym Sączu udzielał wsparcia oraz specjalistycznej pomocy osobom znajdującym się w sytuacji kryzysowej wywołanej przez pandemie. Była to pomoc udzielana przez psychologów, pedagogów oraz prawnika. W ośrodku można było również uzyskać pomoc w postaci schronienia. Funkcjonujący w ośrodku hostel jest formą schronienia przeznaczoną dla osób znajdujących się w sytuacji kryzysowej, mający na celu zapewnienie im bezpieczeństwa. Pomoc świadczono w formie całodobowego poradnictwa pod ogólnodostępnymi numerami telefonów oraz indywidualnego kontaktu ze specjalistą/psychologiem w siedzibie Ośrodka Interwencji Kryzysowej w Nowym Sącz z zachowaniem środków bezpieczeństwa. Wyżej wymieniane formy pomocy skierowane były dla osób doświadczających trudności wynikających z:

1. sytuacji związanej z pandemią COVID-19;
2. doznawania przemocy domowej;
3. trudności życiowych takich jak: utrata pracy, strata bliskiej osoby;
4. konfliktów małżeńskich oraz rodzinnych;
5. trudności emocjonalnych;
6. trudności wychowawczych;
7. samookaleczeń, myśli oraz tendencji samobójczych.

Dostosowano zgodnie z wymogami pandemicznymi Dział – Izba Wytrzeźwień, w którym ograniczono liczbę osób przebywających w jednym pomieszczeniu, zmniejszając tym samym zagrożenie zarażeniem się osób wymagających wsparcia przez w/w Dział. Ograniczenia były na bieżąco aktualizowane, zgodnie ze zmieniającymi się wytycznymi w tym zakresie.

W październiku 2020 r. wprowadzono ograniczenia w wykonywaniu zadań przez MOPS w Nowym Sączu oraz rodzaj i formę tych ograniczeń. Zgodnie z Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, wprowadzono ograniczenia w postaci wnoszenia wszelkiej korespondencji za pośrednictwem profilu zaufanego ePUAP, poczty elektronicznej, podpisanej podpisem elektronicznym, poprzez nadanie

w placówce pocztowej, osobiście – poprzez złożenie korespondencji do skrzynki zlokalizowanej w budynku MOPS. Dopuszczono możliwość osobistego załatwienia spraw w siedzibie Ośrodka po wcześniejszym ustaleniu terminu, ograniczając tym samym ilość osób przebywających na jego terenie, oczekujących w ciągach komunikacyjnych. Udostępniono bezpośrednie numery telefoniczne, aby każda osoba zainteresowana określoną formą pomocy mogła bez przeszkód nawiązać bezpośrednie połączenie z określonym Działem/Zespołem.

Przez rok 2020 oraz w roku 2021, zgodnie z zapisami Rozporządzeń Rady Ministrów w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, dokonywano zawieszenia zajęć w Działach tut. Ośrodka – Dziennym Domu Seniora oraz Centrum Sądeckiego Seniora, odwołując tym samym czasowo zajęcia.

Miasto Nowy Sącz/Miejski Ośrodek Pomocy Społecznej w Nowym Sączu zawarł z Województwem Małopolskim/Regionalnym Ośrodkiem Polityki Społecznej w Krakowie umowę o udzielenie pomocy finansowej w ramach projektu „Kooperacje 3D – model wielosektorowej współpracy na rzecz wsparcia osób i rodzin", finansowanego ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, w ramach którego pracownicy Ośrodka zostali wyposażeni w środki ochrony osobistej, środki i sprzęt służący do dezynfekcji oraz dodatkowy sprzęt i wyposażenie w okresie: wrzesień 2020 r. – listopad 2020 r.[5]

Dzięki pozyskanym środkom dokonano poprawy bezpieczeństwa pracowników MOPS w Nowym Sączu, a w konsekwencji osób korzystających z ich usług. Wysokość wnioskowanej pomocy finansowej w ramach projektu „Kooperacje 3D – model wielosektorowej współpracy na rzecz wsparcia osób i rodzin" dla Miasta Nowego Sącza wyniosła – 60 tys. zł.

Wprowadzony na obszarze Rzeczpospolitej Polskiej stan epidemii zasadniczo wpłynął na funkcjonowanie grupy osób najbardziej zagrożonej ryzykiem zachorowalności na COVID-19, w szczególności osób w podeszłym wieku. Zalecenia dotyczące ograniczeń w zakresie przemieszczania się spowodowały wzrastające poczucie osamotnienia seniorów, powodujące pogorszenie stanu zdrowia oraz samopoczucia tej grupy osób. Wzrastająca liczba zachorowań na COVID-19 oraz liczba osób objętych kwarantanną uniemożliwiała także rodzinom oraz osobom dotychczas wspierającym osoby starsze udzielanie pomocy na dotychczasowym poziomie.

Mając powyższe na uwadze Miejski Ośrodek Pomocy Społecznej w Nowym Sączu przystąpił do bezpośredniej realizacji programu „Wspieraj Seniora" na rok 2020. Miasto Nowy Sącz wraz z MOPS w Nowym Sączu skorzystało z dofinansowania w kwocie 218.455,43 zł ze środków budżetu państwa z udziałem wkładu własnego w kwocie

[5] https://mops.nowysacz.pl/zawarto-umowe-na-pomoc-finansowa-dla-mops-w-ramach-projektu-kooperacje-3d-model-wielosektorowej-wspolpracy-na-rzecz-wsparcia-osob-i-rodzin/,[dostęp 28.06.2022].

55.000,00 zł na zorganizowanie i realizację usługi wsparcia[6]. W związku z realizacją programu Ośrodek opracował, kolejno wdrożył Zarządzeniem Dyrektora *„Procedurę postępowania w związku z realizacją Programu „Wspieraj Seniora" na rok 2020".* Środki zostały przeznaczone na przyznanie nagród dla 75 pracowników Ośrodka w Nowym Sączu zaangażowanych w realizację programu „Wspieraj Seniora".

Powołano spośród pracowników – Koordynatorów, Zespół koordynujący zamówienia oraz Zespół dyżurujący. Koordynatorzy odpowiadali za prawidłowe rozdzielenie zadań w ramach usług wsparcia oraz za rozdzielenie zadań w harmonogramie dyżurów oraz ustalenie dostępności pracowników w danym dniu roboczym. Zespół koordynujący zamówienia oraz Zespół dyżurujący został podzielony na pracowników technicznych obsługujących aplikację CAS, pracowników koordynujących zamówienia oraz pracowników realizujących zadanie w terenie (podział pracowników zależał od bieżących potrzeb zainteresowanych osób). Zespół koordynujący zamówienia realizował zadania według harmonogramu dyżurów, a Zespół dyżurujący według dostępności w danym dniu roboczym. Z uwagi na dużą rotację pracowników spowodowaną usprawiedliwioną nieobecnością m.in. chorobą lub zasiłkami opiekuńczymi z tyt. opieki nad dziećmi w realizację zadania zaangażowani zostali pracownicy Działów tut. Ośrodka, niezależnie od stanowiska na którym byli zatrudnieni. Pracownicy codziennie wykazywali gotowość do podjęcia dodatkowego zadania w ramach programu „Wspieraj Seniora". Seniorzy mogli zgłaszać się na ogólnopolską infolinię oraz bezpośrednio do Ośrodka osobiście, telefonicznie na wyznaczony numer telefonu komórkowego, który zawsze był obsługiwany przez wyznaczonego pracownika MOPS (w tym, w godzinach nocnych i w weekendy).

Usługi wsparcia dla seniorów polegały w szczególności na dostarczeniu zakupów obejmujących artykuły podstawowej potrzeby, w tym artykuły spożywcze, środki higieny osobistej, leki. Koszty zakupów pokrywał senior. Poza w/w MOPS w Nowym Sączu dopuszczał inne usługi wsparcia tj. np. poradnictwo specjalistyczne, sprawy urzędowe, wyprowadzanie psa lub inne wynikające z potrzeb seniorów (jeśli zakres tych usług nie wymagał upoważnienia od seniora lub udostępnienia danych wrażliwych). Usługi wsparcia były realizowane od 20 października 2020 r. do 31 grudnia 2020 r. Ośrodek odpowiadał za działania, mające na celu ochronę osób dla których będą realizowane usługi wsparcia. Zakres usług na rzecz osób dla których było realizowane wsparcie był ograniczony tzw. dystansem sanitarnym.

W związku z realizacją zadania nie zostały poniesione inne wydatki związane z zakupem np. artykułów biurowych, środków higieny osobistej, ubezpieczeń, promocji programu, kosztów dojazdu. Promocja programu była prowadzona bezkosztowo poprzez informacje przekazywane wśród wszystkich osób zgłaszających się, poprzez pracowników socjalnych terenowych oraz poprzez przekazanie informacji o realizowanym programie do

[6] https://www.gov.pl/attachment/7ac31239-462c-429a-92d4-513b9310c510, [dostęp 28.06.2022].

poszczególnych Wydziałów Urzędu Miasta Nowego Sącza oraz współpracujących Instytucji z terenu Miasta Nowego Sącza.

Program był pomocny we wzmocnieniu Miasta Nowego Sącza w realizacji usług wsparcia dla osób potrzebujących/seniorów w szczególności w uwrażliwieniu mieszkańców na potrzeby w/w, którzy znając numery telefonów często nawet anonimowo zgłaszali potrzebę zapewnienia usługi wsparcia dla osób potrzebujących/seniorów. Program przyczynił się również do docenienia zaangażowania poszczególnych pracowników Ośrodka, którzy w związku ze stanem epidemii COVID-19 pomimo obaw o własne zdrowie angażowali się w pomoc na rzecz osób potrzebujących/seniorów.

W związku z epidemią COVID-19, Miejski Ośrodek Pomocy Społecznej przystąpił do programu Państwowego Funduszu Rehabilitacji Osób Niepełnosprawnych pn. „Pomoc osobom niepełnosprawnym poszkodowanym w wyniku żywiołu lub sytuacji kryzysowych wywołanych chorobami zakaźnymi" – Moduł III, podpisując w dniu 3 czerwca 2020 roku umowę na realizację programu[7].

Program skierowany był do osób niepełnosprawnych, które na skutek wystąpienia sytuacji kryzysowych spowodowanych chorobami zakaźnymi (COVID-19) utraciły możliwość korzystania z opieki świadczonej w placówce rehabilitacyjnej. Pomoc była w formie dofinansowania kosztów związanych z zapewnieniem opieki w warunkach domowych, skierowana do osób niepełnosprawnych, które były:

1. uczestnikami warsztatów terapii zajęciowej;
2. uczestnikami środowiskowych domów samopomocy, funkcjonujących na podstawie przepisów ustawy z dnia 12 marca 2004 r. o pomocy społecznej.
3. podopiecznymi dziennych domów pomocy społecznej, funkcjonujących na podstawie przepisów ustawy z dnia 12 marca 2004 r. o pomocy społecznej.
4. podopiecznymi placówek rehabilitacyjnych, których działalność finansowana jest ze środków PFRON na podstawie art. 36 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych.
5. uczestnikami programów zatwierdzonych przez Radę Nadzorczą PFRON i w ramach tych programów korzystają ze wsparcia udzielanego przez placówki rehabilitacyjne.
6. pełnoletnimi (od 18 do 25 roku życia) uczestnikami zajęć rewalidacyjno-wychowawczych organizowanych zgodnie z przepisami rozporządzenia Ministra Edukacji Narodowej z dnia 23 kwietnia 2013 r. w sprawie warunków i sposobu organizowania zajęć rewalidacyjno-wychowawczych dla dzieci i młodzieży z upośledzeniem umysłowym w stopniu głębokim[8].
7. pełnoletnimi (od 18 do 24 roku życia) wychowankami specjalnych ośrodków szkolno-wychowawczych oraz specjalnych ośrodków wychowawczych, bądź

[7] https://pcpropole.pl/pomoc-osobom-niepelnosprawnym-poszkodowanym-w-wyniku-zywiolu-lub-sytuacji-kryzysowych-wywolanych-chorobami-zakaznymi/, [dostęp 28.06.2022].

[8] https://www.mops.katowice.pl/node/3063, [dostęp 28.06.2022].

uczniami szkół specjalnych przysposabiających do pracy funkcjonujących na podstawie ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe.

8. pełnoletnimi (od 18 do 25 roku życia) wychowankami ośrodków rehabilitacyjno-edukacyjno-wychowawczych oraz ośrodków rewalidacyjno-wychowawczych funkcjonujących na podstawie ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe.

Łącznie wsparciem objęto 182 osoby niepełnosprawne na kwotę 348.500,00 zł.

W roku 2021 Miasto Nowy Sącz/Miejski Ośrodek Pomocy Społecznej w Nowym Sączu przystąpił ponownie do Programu „Wspieraj Seniora" na rok 2021, ze środków pochodzących z Funduszu Przeciwdziałania COVID–19 na podstawie art. 65 ust. 5 pkt. 1 Ustawy z dnia 31 marca 2020 roku o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID–19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw
w zakresie realizacji zadania własnego, określonego w art. 17 ust. 2 pkt. 4 Ustawy z dnia 12 marca 2004 roku o pomocy społecznej[9] tj. podejmowania innych zadań z zakresu pomocy społecznej wynikających z rozeznanych potrzeb gminy, do których w czasie obowiązywania epidemii zaliczyć należy działania na rzecz ochrony Seniorów przed zakażeniem COVID–19.

Miasto Nowy Sącz poprzez Miejski Ośrodek Pomocy Społecznej w Nowym Sączu realizowało w/w program w I kwartale 2021 roku.

Usługi wsparcia w związku z realizacją programu „Wspieraj Seniora" adresowane były do:

1. seniorów, którzy pozostaną w domu w związku z zagrożeniem zakażenia COVID-19,
2. osób poniżej 70 roku życia, którzy pozostaną w domu w związku z zagrożeniem zakażenia COVID-19, w przypadku braku możliwości realizacji we własnym zakresie niezbędnych potrzeb, wynikających ze stanu zdrowia oraz sytuacji rodzinnej i społecznej tych osób.

W roku 2020 pracownicy MOPS w Nowym Sączu mieli możliwość skorzystania z testów immunologicznych, zwanych inaczej testami przesiewowymi na obecność COVID-19, które zostały przekazane przez Urząd Miasta Nowego Sącza/Wydział Zarządzania Kryzysowego.

Ponadto w ramach nadzoru nad jednostkami pomocy społecznej i pieczy zastępczej realizowano następujące zadania:

1. Systematyczne przekazywanie wytycznych, instrukcji, poleceń dotyczących, decyzji wydanych w ramach zwalczania i przeciwdziałania epidemii (wojewody małopolskiego, Głównego Inspektora Sanitarnego, Ministrów, Powiatowej Stacji Sanitarno-Epidemilogicznej).

[9] https://mops.nowysacz.pl/programy-rzadowe-i/program-wspieraj-seniora-na-rok-2021/, [dostęp 28.06.2022].

2. Przekazywanie informacji dot. planowanych projektów dofinansowujących jednostki w trakcie trwającej epidemii.
3. Współpraca z jednostkami organizacyjnymi pomocy społecznej i pieczy (w zakresie wprowadzonych przez jednostki zabezpieczeń, procedur uwzględniających specyfikę działalności jednostek jak i możliwości związane z posiadaną infrastrukturą. Działania jednostek skupiały się między innymi na:
   a) wdrożeniu rekomendacji, zaleceń i instrukcji Wojewody Małopolskiego oraz Głównego Inspektora Sanitarnego, dotyczących postępowania w ramach zwalczania i przeciwdziałania epidemii,
   b) systematycznym monitorowaniu stanu zdrowia mieszkańców domów pomocy społecznej poprzez obserwację i pomiary niezbędnych parametrów życiowych dla 340 mieszkańców domów pomocy społecznej,
   c) systematycznym monitorowaniu stanu zdrowia wychowanków placówek opiekuńczo-wychowawczych i dzieci przebywających w rodzinnej pieczy zastępczej,
   d) wykonywaniu testów przesiewowych dla mieszkańców i pracowników DPS w ilości ok. 800,
   e) zakupie dla jednostek pomocy społecznej w Nowym Sączu środków ochrony indywidualnej z własnych funduszy, jak również z grantów i programów krajowych oraz Unii Europejskiej. Wśród nich należy wyróżnić: Małopolska Tarcza Finansowa-Pakiet Społeczny, Bezpieczny Dom, Bezpieczny Dom – wsparcie dla kadry małopolskich domów pomocy społecznej, Zapewnienie Bezpieczeństwa i opieki mieszkańcom Domów Pomocy Społecznej oraz bezpieczeństwa pracownikom tych jednostek.
   f) zakupie sprzętu i wyposażenia niezbędnego do walki z epidemią COVID-19 w ramach w/w programów (kabiny dezynfekcyjne, środki ochrony indywidualnej itp.). Wsparcie finansowe pracowników jednostek pomocy społecznej - w sumie około 1.200.000,00 zł,
   g) opracowaniu i wdrożeniu procedur dotyczących przyjmowania osób do jednostek pomocy społecznej w czasie pandemii, postępowania z osobami podejrzanymi o zarażenie wirusem SARS-CoV-2, postępowania w czasie izolacji i kwarantanny z osobami podejrzanymi i chorymi na COVID-19,
   h) przeprowadzeniu szkoleń dla pracowników w zakresie postępowania i stosowania środków ochrony indywidualnej dla siebie i podopiecznych w czasie trwania pandemii,
   i) stosowaniu alternatywnych form zajęć z podopiecznymi w zakresie udziału w terapii i rehabilitacji z wykorzystaniem elektronicznych i radiowych mediów oraz środków masowego przekazu,

j) utworzeniu miejsc kwarantanny dla pracowników jednostek, którzy nie chcieli jej odbywać w warunkach domowych,
k) zgłaszaniu i organizowaniu szczepień dla mieszkańców DPS i pracowników domów pomocy społecznej w ilości ok. 340 szczepień, pracowników placówek opiekuńczo-wychowawczych,
l) utworzono miejsca kwarantanny dla pracowników jednostek, którzy nie chcieli jej odbywać w warunkach domowych. Zgłoszono i częściowo wykonano szczepienia dla osób mieszkających i pracujących w Domach Pomocy Społecznej (DPS) w ilości ok. 340 szczepień.

4. Monitoring sytuacji związanej z epidemią, przekazywanie sprawozdawczości, raportów, wsparcie organizacyjne jednostek podczas stwierdzonych zakażeń, pomoc w zakresie zabezpieczenia kadry w trakcie stwierdzonych zakażeń w DPS (delegowanie pracowników ze Środowiskowego Domu Samopomocy).
5. MOPS zajmował się tworzeniem bazy wolontariuszy chętnych do pracy w DPS.
6. W ramach współpracy z Wdziałem Zarządzania Kryzysowego UM Nowego Sącza, raz w tygodniu MOPS uczestniczył w posiedzeniach sztabu kryzysowego. W trakcie posiedzeń przekazywano aktualne informacje dot. sytuacji epidemiologicznej w jednostkach i ewentualnych problemów, czy koniecznych zmian wsparcia w zakresie zabezpieczenia w środki ochrony indywidualnej, w tym testy (dzięki zakupionym przez Prezydenta testom dokonano badania osób podejrzanych o zarażenie lub mających kontakt z osobą zarażoną COVID-19).
7. Dystrybucja środków ochrony indywidualnej z rezerw przekazanych przez Wojewodę.
8. Współpraca z Snepid-em.
9. Realizacja projektu „Wsparcie dzieci umieszczonych w pieczy zastępczej w okresie epidemii COVID-19", zwanego dalej „Projektem", w ramach Programu Operacyjnego Wiedza Edukacja Rozwój na lata 2014-2020 – Działanie 2.8 Rozwój usług społecznych świadczonych w środowisku lokalnym, PI 9iv: Ułatwianie dostępu do przystępnych cenowo, trwałych oraz wysokiej jakości usług, w tym opieki zdrowotnej i usług socjalnych świadczonych w interesie ogólnym[10].

W ramach realizacji projektu na kwotę ogółem: 237.409,79 zł dokonano zakupu:

1) środków ochrony indywidualnej: maseczek, rękawiczek, środków dezynfekcyjnych (9.128,29 zł),
2) 62 zestawów komputerowych i oprogramowania (201.707,70 zł),
3) 10 urządzeń wielofunkcyjnych (4.993,80 zł),

[10] https://www.power.gov.pl/strony/o-programie/dokumenty/program-wiedza-edukacja-rozwoj-2014-2020/ [dostęp 28.06.2022].

4) sprzętu i wyposażenia niezbędnego do uruchomienia pięciu miejsc kwarantanny w placówce opiekuńczo-wychowawczej typu socjalizacyjnego z miejscami interwencyj-nymi w Trzycierzu (21.580,00 zł).

Od dnia 26 listopada 2020 r. zostały wprowadzone zmiany w wytycznych dotyczących realizacji Programu Operacyjnego Pomoc Żywnościowa (PO PŻ) – Podprogram 2020 w zakresie podwyższenia kryterium dochodowego. Oznacza to, że z pomocy żywnościowej mogły skorzystać osoby, które znajdują się w trudnej sytuacji życiowej i osiągają dochody nieprzekraczające 220% kryterium dochodowego z ustawy o pomocy społecznej, tj. 1.542,20 zł w przypadku osoby samotnie gospodarującej oraz 1.161,60 zł w przypadku osoby w rodzinie. Głównym celem programu było udzielenie wsparcia osobom potrzebującym poprzez cykliczne przekazywanie paczek żywnościowych[11].

W okresie realizacji programu wydawane były następujące produkty żywnościowe: powidła śliwkowe, mus jabłkowy, makaron, ryż, płatki owsiane, kasza, herbatniki maślane, artykuły mleczne (mleko UHT, ser), artykuły mięsne i rybne konserwy (szynka wieprzowa mielona, pasztet, filet z makreli), cukier biały, miód oraz tłuszcze – olej rzepakowy.

Warunkiem skorzystania z pomocy żywnościowej w ramach programu było otrzymanie skierowania z Miejskiego Ośrodka Pomocy Społecznej**,** które wydawane jest na podstawie oświadczenia o dochodach z miesiąca poprzedzającego złożenie wniosku. Skierowania po pomoc żywnościową są wydawane przez pracowników Sekcji ds. pierwszego kontaktu MOPS.

W związku z trwającym stanem epidemii COVID-19, możliwe jest również zdalne kwalifikowanie odbiorców pomocy żywnościowej w ramach Programu Operacyjnego Pomoc Żywnościowa 2014-2020[12].

W realizacji PO PŻ 2014-2020, współfinansowanego ze środków Europejskiego Funduszu Pomocy Najbardziej Potrzebującym (FEAD), w którym osoby bezdomne stanowią jedną z grup docelowych, uczestniczą:

1) Federacja Polskich Banków Żywności,
2) Caritas Polska,
3) Polski Komitet Pomocy Społecznej,
4) Polski Czerwony Krzyż.

W przypadku osób bezdomnych placówka udzielająca tymczasowego schronienia może w imieniu osób bezdomnych wystąpić do ośrodka pomocy społecznej, który kwalifikuje do pomocy z PO PŻ, o przyznanie wsparcia w ramach Programu.

W sporadycznych sytuacjach osobom które kwalifikowały się do PO PŻ, a które we własnym zakresie nie były w stanie zgłosić się po żywność, do miejsca zamieszkania za potwierdzeniem odbioru, dostarczał ją pracownik socjalny.

[11] https://mops.nowysacz.pl/program-operacyjny-pomoc-zywnosciowa-2014-2020-wspolfinansowany-z-europejskiego-funduszu-pomocy-najbardziej-potrzebujacym-fead/, [dostęp 28.06.2022].
[12] *Ibidem*.

Na terenie Nowego Sącza zostały wydane łącznie 932 skierowania do otrzymania pomocy żywnościowej. W organizacji transportu żywności zaangażowani byli żołnierze 11 Małopolskiej Brygady Obrony Terytorialnej. Ponadto MOPS nawiązał współpracę z Stowarzyszeniem ODRA-NIEMEN w Tarnowie dzięki, której otrzymał nieznaczną ilość artykułów spożywczych, które zostały dowiezione przez Straż Miejską w Nowym Sączu do 8 rodzin przebywających na kwarantannie domowej.

W okresie zamknięcia placówek edukacyjnych, w których stołówka szkolna była nieczynna, gdy dziecko/uczeń nie spożywało posiłków, kierownik ośrodka pomocy społecznej ma możliwość przyznania na ten okres pomocy w formie świadczenia pieniężnego na zakup posiłku lub żywności, bądź świadczenia rzeczowego w postaci produktów żywnościowych.

Osoby, które korzystały z posiłków przyznanych w ramach Programu „Posiłek w szkole i w domu" w placówkach edukacyjnych w okresie ich zamknięcia zostały zabezpieczone poprzez zmianę miejsca wydawania posiłków w stołówce, która wówczas wydawała posiłki lub formie zmiany przyznanej formy pomocy z posiłku na świadczenie pieniężne przeznaczone na zakup posiłku lub żywności. Z pomocy w postaci posiłku skorzystało: 183 osoby dorosłe, 427 dzieci/uczniów, a dla 141 dzieci na wniosek rodzica zmieniono formę przyznanej pomocy z posiłku na świadczenie pieniężne.

W związku z otrzymywanymi poleceniami oraz instrukcjami Wojewody Małopolskiego, jak również Ministerstwa Rodziny, Pracy i Polityki Społecznej dotyczącymi zapewnienia pomocy osobom wymagającym wsparcia w związku z rozprzestrzenianiem się choroby zakaźnej COVID-19, otrzymano informacje iż: objęcie osoby kwarantanną nie oznacza automatycznie, że dana osoba/rodzina musi być objęta pomocą Ośrodka. Pomoc skierowana jest do osób, które wykorzystując własne zasoby i możliwości (np. rodziny, przyjaciół, sąsiadów, znajomych z pracy, innych osób i podmiotów), nie są w stanie samodzielnie zapewnić sobie wyżywienia. W przypadku uzyskania informacji dotyczącej osoby/ rodziny poddanej kwarantannie Ośrodek Pomocy Społecznej rozeznaje sytuację tych osób w celu sprawdzenia możliwości i konieczności objęcia ich wsparciem. W celu dostarczenia pomocy wszystkim potrzebującym, Ośrodek nawiązał współpracę z Wydziałem Zarządzania Kryzysowego Urzędu Miasta Nowego Sącza, Strażą Miejską. MOPS otrzymał 33 zgłoszenia związane z koniecznością podjęcia stosownych działań wobec osób przebywających na kwarantannie.

W związku z potrzebą odizolowania osób, które potencjalnie mogą być zarażone wirusem, Ministerstwo Cyfryzacji uruchomiło Aplikację kwarantanna domowa[13].

Jedną z opcji, z której mogą skorzystać użytkownicy aplikacji, jest możliwość kontaktu osób odbywających kwarantannę z ośrodkami pomocy społecznej. Korzystając z tej funkcji można np. zwrócić się z prośbą o posiłek, podstawowe artykuły spożywcze,

[13] https://www.gov.pl/web/koronawirus/kwarantanna-domowa, [dostęp 28.06.2022].

leki, pomoc psychologiczną, a także kontakt ze strony pracownika ośrodka pomocy społecznej.

Informacje zbierane przy pomocy aplikacji od osób odbywających kwarantannę są przesyłane do Wydziałów Polityki Społecznej Urzędów Wojewódzkich.

Wydział Polityki Społecznej Małopolskiego Urzędu Wojewódzkiego w Krakowie przesłał do tut. Ośrodka 38 zgłoszeń od mieszkańców Nowego Sącza z prośbą o udzielenie pomocy przez pracowników socjalnych.

W celu oceny sytuacji osób przebywających w kwarantannie, pod kątem zabezpieczenia pomocy w formie posiłku lub produktów żywnościowych, zakupu leków oraz wsparcia psychologicznego powołano zespół koordynujący realizację ww. zadań. Pracownicy MOPS pełnili dyżury pod przekazanym do wiadomości publicznej numerem telefonu każdego dnia, również w soboty i niedziele w godzinach od 7.30-19.00 w celu udzielenie niezbędnych informacji osobom, które potrzebują pomocy, zwłaszcza ludziom starszym, samotnym i niepełnosprawnym. Wskazana godzina podyktowana została poleceniem Ministerstwa Rodziny, Pracy i Polityki Społecznej, które nałożone zostało na ośrodki pomocy społecznej, jednak w praktyce pełniący dyżur pracownicy MOPS Nowym Sączu, udzielali informacji również poza wskazanymi godzinami. MOPS codziennie zdalnie identyfikował potrzeby mieszkańców miasta, bez narażania pracowników socjalnych na ryzyko zakażenia co zgodne było z rekomendacją MRPiPS. W warunkach wyższej konieczności, skrócono do minimum lub też całkowicie uproszczono wszelkie formalności, które zazwyczaj są wymagane, aby pomoc została uruchomiona jak najszybciej.

Zakończenie

Pandemia choroby COVID-19 zaskoczyła i zmusiła niemal cały świat do porzucenia przyzwyczajeń i rozpoczęcia odmiennego życia w „nowej rzeczywistości" maseczek, środków dezynfekujących i ograniczeń. Mimo sugestii niektórych badaczy, jakoby epidemii dało się zapobiec zawczasu, globalna gospodarka zdecydowanie nie była na nią przygotowana. Długotrwałe pozostawanie w sytuacji zagrożenia oraz brak informacji charakterystyczny dla początków pandemii uniemożliwiały skuteczne planowanie programów wsparcia czy zapobiegania. Miejski Ośrodek Pomocy Społecznej w Nowym Sączu, jak wynika z powyższego artykułu podjął liczne działania mające na celu pomoc osobom potrzebującym/seniorom z terenu Miasta Nowego Sącza podczas trwania pandemii wywołanej przez wirus SARS-CoV-2. Starano się działać nieszablonowo, jak najlepiej reagować na szybko zmieniające się warunki.

W tym trudnym okresie Miejski Ośrodek Pomocy Społecznej w Nowym Sączu, wraz z lokalnym Urzędem Miasta, stanęły na wysokości zadania, przygotowując środki ochrony osobistej (maseczki, płyny dezynfekujące), finansując zakup testów oraz organizując

programy pomocy społecznej. Dzięki współpracy ze służbą zdrowia, Strażą Pożarną, Policją oraz Strażą Miejską/Gminną, MOPS mogło dotrzeć ze swoją pomocą do wielu potrzebujących osób.

Reasumując, działalność nowosądeckiego Ośrodka Pomocy Społecznej w analizowanym okresie pandemii wirusa SARS-CoV-2 ocenia się wysoko. Dobre i skutecznie wprowadzane pomysły mogą stanowić wzór dla analogicznych jednostek w całym kraju.

Bibliografia

https://mops.nowysacz.pl/program-operacyjny-pomoc-zywnosciowa-2014-2020-wspolfinansowany-z-europejskiego-funduszu-pomocy-najbardziej-potrzebujacym-fead/, [dostęp 28.06.2022].
https://mops.nowysacz.pl/programy-rzadowe-i/program-wspieraj-seniora-na-rok-2021/, [dostęp 28.06.2022].
https://mops.nowysacz.pl/zawarto-umowe-na-pomoc-finansowa-dla-mops-w-ramach-projektu-kooperacje-3d-model-wielosektorowej-wspolpracy-na-rzecz-wsparcia-osob-i-rodzin/, [dostęp 28.06.2022].
https://pcpropole.pl/pomoc-osobom-niepelnosprawnym-poszkodowanym-w-wyniku-zywiolu-lub-sytuacji-kryzysowych-wywolanych-chorobami-zakaznymi/, [dostęp 28.06.2022] r.
https://www.gov.pl/attachment/7ac31239-462c-429a-92d4-513b9310c510, [dostęp 28.06.2022].
https://www.gov.pl/web/koronawirus/kwarantanna-domowa, [dostęp 28.06.2022].
https://www.mops.katowice.pl/node/3063, [dostęp 28.06.2022].
https://www.power.gov.pl/strony/o-programie/dokumenty/program-wiedza-edukacja-rozwoj-2014-2020/, [dostęp 28.06.2022].
https://znaczenia.com.pl/znaczenie-patogeneza-co-to-jest-pojecie-i-definicja-znaczenia/, [dostęp 28.06.2022].
Zając G., *Wpływ pandemii koronawirusa na działalność organizacji pozarządowych a bezpieczeństwo lokalnych społeczności*, [w:] Górski G., Potoczek A., (red.), *Bezpieczeństwo lokalne – wybrane problemy teorii i praktyki*, Toruń 2022.

Paweł Piotrowski[1]

Jednostka i Rodzina z aspektu zaspokojenia potrzeby bezpieczeństwa
Individual and Family from the aspect of meeting the need for security

Streszczenie

Niniejszy artykuł porusza kwestie związane z zaspokojeniem potrzeby bezpieczeństwa przez jednostkę i rodzinę w aspekcie wielowymiarowym, w tym również w kontekście bezpieczeństwa wewnętrznego. Główne założenia analizy dotyczą kwestii takich jak: zaspokojenie potrzeby bezpieczeństwa w znaczeniu zewnętrznym wobec jednostki i rodziny, zaspokojenie potrzeby transcendentnej na gruncie religii oraz socjalizacji jednostki, tj. przekazania jej w procesie transmisji kulturowej, w toku procesu socjalizacji pierwotnej a następnie wtórnej wartości wyższych w tym wynikających z religii, co ma znaczenie dla homogeniczności nurtu kulturowego społeczeństwa. Przedstawiono również aksjologiczne znaczenie bezpieczeństwa w percepcji społecznej. Omówione zostały tu także pogłębiające się procesy laicyzacji życia, czego skutkiem jest sekularyzacja w przestrzeni społecznej i wpływ kultury masowej promującej konsumpcjonizm, której konsekwencją jest materializm i obniżenie jakości oraz znaczenia relacji międzyludzkich.
Słowa kluczowe: jednostka, rodzina, bezpieczeństwo, religia, moralność, etyka, socjalizacja

Summary

This article addresses issues related to meeting the need for security by an individual and a family in a multidimensional aspect, including in the context of internal security. The main assumptions of the analysis concern issues such as: meeting the need for security in the external sense towards the individual and family, meeting the transcendent need on the basis of religion and socialization of the individual, i.e. passing it on in the process of cultural transmission, in the process of primary and then secondary socialization of higher values in this resulting from religion, which is important for the homogeneity of the cultural

[1] Mgr Paweł Piotrowski, wykładowca, Instytut Nauk o Bezpieczeństwie Staropolskiej Akademii Nauk Stosowanych w Kielcach.

stream of society. The axiological meaning of security in social perception was also presented. It also discusses the deepening processes of secularization of life, which results in secularization in social space and the influence of mass culture that promotes consumerism, the consequence of which is materialism and a reduction in the quality and importance of interpersonal relationships.
Keywords: individual, family, security, religion, morality, ethics, socialization

Wstęp

Jednostka i rodzina[2], to dwie najmniejsze komórki społeczne, przy czym w przypadku rodziny określmy ją jako grupę. Konglomerat potrzeb zaspokajanych przez realizację funkcji rodziny i role rodzinne oraz zawodowe, pełnione w sferach kolektywnych (rodzina i jej interesy oraz praca i interes grupy zawodowej) i indywidualnych (rodzina czas wolny netto oraz praca odpowiedzialność za pełnione obowiązki, przy tym zaspokojenie potrzeby samorealizacji potencjału twórczego) przekłada się na możliwości, czyli potencjał siły nabywczej dochodu rozporządzalnego, tj. koszyka dóbr jaki może nabyć gospodarstwo domowe za osiągany wspólnie (tzn. przez współmałżonków) dochód. Gospodarstwo domowe i zaopatrzenie go w różnorodne dobra, w tym przede wszystkim żywność, energię, media, jest realizowane w aspekcie funkcji ekonomicznej. Udział w kulturze jest realizacją funkcji rodziny związanej ze wspólnym spędzaniem czasu wolnego, czyli rekreacyjno-towarzyskiej. Potrzeba transcendencji powiązana z funkcją religijną, wynika z konieczności odnalezienia swojego bytu, czyli sensu egzystencjalnego, który wyznacza cele do zrealizowania, czyli nadanie życiu sensu. Osnową prawidłowego rozwoju jest poczucie bezpieczeństwa, warunkowane w kwestiach podstawowych przez państwo. Życie człowieka jako egzystencja jest poszukiwaniem jego sensu. W czasie jego trwania zapisuje on swoją biografię poruszając się w przestrzeni społecznej, która stanowi część

[2] Rodzina w naukach humanistycznych, to ukonstytuowany związek kobiety i mężczyzny oraz ich dzieci. Małżonkowie wspólnie prowadzą gospodarstwo domowe i pełniąc role rodzinne oraz zawodowe realizują funkcje rodziny, przede wszystkim takie jak: emocjonalna, seksualna i prokreacyjna. Funkcja emocjonalna zawiązuje i umacnia więzi między małżonkami, seksualna je pogłębia i wzmacnia, natomiast prokreacyjna – łącznie z seksualną – służy do powołania na świat potomstwa. Z uwagi na to że tylko związek małżeński kobiety i mężczyzny ma dar i możliwość powołania nowego życia oraz opieki i socjalizacji dzieci, zapewniającej właściwy rozwój psychiczny i społeczny, nie może odbywać się w innych – nierodzinnych, alternatywnych – formach związku. Wyjątkiem jest oczywiście śmierć współmałżonka i samotne rodzicielstwo lub rodzina zrekonstruowana, czyli kiedy jeden ze współmałżonków (mąż lub żona) odchodzi i pozostały rodzic wchodzi w związek małżeński z inną osobą płci przeciwnej, tj. kobietą lub mężczyzną. W związku z powyższym definicja terminu rodzina, czyli jak zaznaczono na wstępie ukonstytuowanego związku kobiety i mężczyzny oraz ich dzieci, nie podlega żadnemu rozszerzeniu, np. o alternatywne względem rodziny formy związków, *płeć jest zakorzeniona w naturze, psychice, kulturze i wychowaniu człowieka. Dualizm płci (podział na kobiety i mężczyzn) stanowi fundament człowieczeństwa. Płeć ma odzwierciedlenie w większości płaszczyzn ludzkiej egzystencji. Określa naszą tożsamość zaraz po urodzeniu na podstawie zewnętrznych narządów płciowych. W związku z tym ma także specyficzne konotacje społeczne, które znajdują wyraz w podziale ról płciowych, tworzących ramy życia i funkcjonowania nas w społeczeństwie. (...) Na podstawie tych deklaracji realizujemy nasze zadania życiowe, stajemy się odrębnymi jednostkami społecznymi, z innymi prawami i obowiązkami*, w: J. J. Pawłowicz, *Ideologia gender realnym zagrożeniem dla małżeństwa i rodziny*, [w:] *Teologia i Moralność*, tom 11, Poznań 2012, s. 143. Zob. także: P. Piotrowski, *Przemiany Współczesnej Polskiej rodziny – Kryzys rodziny czy poszerzenie definicji jej form*, artykuł opublikowany [w:] M. Chuchrak, T. Iwanek (red.), *Bezpieczeństwo społeczności lokalnych*, Oficyna wydawnicza PWSZ w Nysie, Nysa 2017. Ponadto Konstytucja Rzeczypospolitej Polskiej również określa definicję rodziny i gwarantuje jej ochronę, co zawarte jest w art. 18 *Małżeństwo jako związek kobiety i mężczyzny, rodzina, macierzyństwo i rodzicielstwo znajdują się pod ochroną i opieką Rzeczypospolitej Polskiej*. Zob. *Konstytucja Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 r., Dz.U. 1997 nr 78 poz. 483.

wspólną i jest miejscem wyrażania wartości wyższych w tym religijnych, poprzez podejmowane interakcje w sytuacjach społecznych i własne uczynki.

Bezpieczeństwo

Bezpieczeństwo jest – po zaspokojeniu potrzeb fizjologicznych – jedną z podstawowych potrzeb, jego sens jest rozległy i należy go rozpatrywać również jako wartość. W znaczeniu społecznym, jest ono traktowane jako element wyjściowy prawidłowego funkcjonowania społeczeństwa, *bezpieczeństwo stanowi tę wartość uniwersalną, która dotyczy nieskończonej liczby podmiotów, chociaż największe znaczenie ma bezpieczeństwo jednostki, grupy społecznej i państwa*[3]. Zapewnienie bezpieczeństwa dotyczy sfery prywatnej, przestrzeni publicznej i instytucjonalnej, *troska o wysoką jakość życia mieszkańców, jest podstawowym wyzwaniem dla jednostek samorządu terytorialnego wszystkich szczebli. Już sam charakter jego zadań (edukacja, ochrona zdrowia, pomoc społeczna, rozwój lokalnej infrastruktury itd.) pokazuje, że zasadniczym jego celem jest troska o życie mieszkańców i zapewnienie im jak najlepszych warunków funkcjonowania w społeczeństwie*[4]. Sfera prywata, intymna, to miejsce zaspokajania potrzeb psychologiczno-emocjonalnych, co odbywa się przede wszystkim w przestrzeni fizycznej budynku, czyli domu lub mieszkania. Jest to przestrzeń służąca zaspokojeniu potrzeb rodziny poprzez odtwarzanie wzorów wynikających z danej roli (pełnienia ról) rodzinnych (męża/żony, ojca/matki). W tej sferze zaspokajane są potrzeby zarówno niższego jak i wyższego rzędu, przede wszystkim takie jak: fizjologiczne, bezpieczeństwa, przynależności, szacunku, estetyczne[5]. Zaspokojenie potrzeby bezpieczeństwa na poziomie mikrospołecznym, wymaga zewnętrznego – prewencyjnego oddziaływania na przestrzeń społeczną, czyli pozostawanie specjalnie przygotowanych (wyszkolonych) grup w gotowości do podjęcia reakcji. Taki stan dotyczy przede wszystkim służb takich jak: policja i straż miejska, działające w celu obrony jednostek i małych grup oraz ich dóbr materialnych i intelektualnych w przestrzeni społecznej, przed nieuprawnionym atakiem zagrażającym życiu, zdrowiu i mieniu. Następnie jednostki ratownicze takie jak: straż pożarna i ratownictwo medyczne – w pierwszym przypadku – podejmujące akcje w stanach zagrożenia zdrowia i życia ludności, podczas zdarzeń losowych lub występowania zjawisk naturalnych (np. pożar, powódź, wypadek samochodowy, skażenie chemiczne, itp.) – w drugim przypadku – skoncentrowane na ratowaniu życia i zdrowia ludzi. Działania tych służb odbywają się w lokalnej przestrzeni społecznej. Zaspokojenie potrzeby bezpieczeństwa na poziomie makrospołecznym, dotyczy sfery ponadlokalnej,

[3] M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, *Zeszyty Naukowe KUL* 61 (2018), nr 3 (243), Wydawnictwo Katolickiego Uniwersytetu Lubelskiego, Lublin 2018, s. 16.

[4] M. Klimek, *Samorząd terytorialny w trosce o jakość życia mieszkańców wspólnoty lokalnej*, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*, Petrus, Kraków 2012, s. 156.

[5] Zob. A.H. Maslow, *Motywacja i osobowość*, PWN, Warszawa 2013.

ogólnokrajowej, czyli obrony granicy państwa co realizowane jest przez służby takie jak: straż graniczna i armia. Zadaniem pierwszej z tych służb, jest obrona granicy przed nielegalnym jej przekraczaniem przez uchodźców, natomiast drugiej obrona militarna w przypadku ataku zbrojnego innego państwa. Współdziałanie tych służb na różnym poziomie i w różnej konfiguracji, jest podstawą zapewnienia bezpieczeństwa w przestrzeni społecznej na poziomie mikro i makrospołecznym, a zatem bezpieczeństwa w znaczeniu publicznym, z uwagi na to, że *bezpieczeństwo publiczne dotyczy ochrony porządku prawnego, życia i zdrowia obywateli oraz majątku narodowego, norm i obyczajów oraz zapewnienia warunków sprawnego funkcjonowania organizacji państwowych realizujących ponadjednostkowe zadania przed bezprawnymi działaniami*[6]. W zakresie bezpieczeństwa społecznego z kolei, mieści się pojęcie zaspokojenia potrzeb ekonomiczno-bytowych, co związane jest z poziomem instytucjonalnym funkcjonowania państwa, przez co rozumieć należy realizację polityk społecznych dotyczących zaopatrzenia w żywność w tym wodę pitną, energię, prowadzenie polityki mieszkaniowej umożliwiającej rodzinie zakup mieszkania lub budowę domu, *bezpieczeństwo społeczne dotyczy zatem usuwania wszelkich zagrożeń społecznych. Rozpatrując tę składową bezpieczeństwa wewnętrznego państwa, na pierwszy plan wysuwa się obowiązek zapewnienia podstawowych warunków egzystencjalnych, ale także możliwości zrównoważonego rozwoju. Bezpieczeństwo społeczne będzie dotyczy zarówno zapewnienia dostępu do towarów konsumpcyjnych, ochrony zdrowia, zapewnienia tzw. porządku w przestrzeni publicznej, ale również niesienia pomocy zbiorowej w sytuacjach zagrożeń naturalnych i awarii technicznych*[7]. Zabezpieczenie ekonomiczno-bytowe społeczeństwa, czyli *zapewnienie podstawowych warunków egzystencjalnych*, jest warunkiem prawidłowego funkcjonowania rodzin poprzez zaspokojenie ich potrzeb. Jak więc przedstawiono, bezpieczeństwo jest terminem rozległym ale jego etiologia w różnych kontekstach sfer życia człowieka jest podobna, chodzi o zaspokojenie potrzeb poprzez dostarczenie odpowiednich dóbr, lub zapewnienie ochrony spokoju i porządku publicznego przed nieuprawnionym atakiem zagrażającym zdrowiu i życiu czy obrona granic państwa, *zapewnienie warunków egzystencjalnych i bytowych współczesnemu społeczeństwu nie jest możliwe bez sprawnej infrastruktury krytycznej państwa, również zapewnienie jej funkcjonalności jest warunkiem osiągnięcia pożądanego poziomu bezpieczeństwa społecznego*[8]. Państwo zatem pełni szeroko rozumianą funkcję ochronną wobec swoich obywateli. Ta funkcja nie dotyczy tylko fizycznej obrony granic państwa, ale także ochrony przestrzeni społecznej, co odbywa się w zróżnicowany sposób, przez włączenie w działania odpowiedniej – wyspecjalizowanej służby.

[6] B. Zdrodowski, *Istota bezpieczeństwa państwa*, [w:] *Studia de Securitate* 9(3) (2019), Wydawnictwo Naukowe UP, Kraków 2019, s. 64.
[7] *Ibidem*, s. 64.
[8] *Ibidem*, s. 64.

Z aspektu aksjologicznego bezpieczeństwo jest wartością, czyli stanem oczekiwanym i pożądanym społecznie, którego utrzymanie zapewnia równowagę psychiczną jednostek przez możliwość indywidualnego rozwoju, a także udziału w przestrzeni społecznej. Wartość bezpieczeństwa jako jednego z czynników zabezpieczenia szeroko pojętych potrzeb społecznych, chroni także wartości wyższe, ujęte w kulturze bezpieczeństwa. Zagrożenia wynikające z niskich wartości kultury masowej[9] (tworzenie potrzeb pozornych, konsumeryzm[10]) oraz coraz bardziej niebezpieczny i większy wpływ grup mniejszościowych na przestrzeń społeczną, stanowią niebezpieczeństwo dla wartości wyższych, takich jak religia, tradycje i obyczaje, patriotyzm oraz kształt rodziny naturalnie złożonej z kobiety i mężczyzny oraz ich dzieci[11]. Kultura bezpieczeństwa ma stać na straży tych wartości, poprzez kontrolę społeczną i korygowanie stanów zagrożenia do stanu powtórnego bezpieczeństwa, ponieważ stanowi ona *ogół utrwalonego, materialnego i pozamaterialnego dorobku człowieka, służącego szeroko, zarówno militarnie jak również pozamilitarnie rozumianej samoobronności indywidualnych oraz grupowych podmiotów bezpieczeństwa*[12]. Kultura bezpieczeństwa stanowi trychotomiczny podział współtworzony za przyczyną przenikających się ukierunkowanych strumieni, zbieżnych z procesami kreowania ich przez jednostkę w danym miejscu w przestrzeni społecznej i sytuacji. Strumieniami tymi są: strumień mentalno-duchowy, na który składają się określone idee, wartości i potrzeby wyższe oraz normy moralne. Strumień racjonalny, organizacyjno-prawny to oddziaływania społeczne, organizacje, systemy prawa, wynalazczości oraz innowacje. Strumień materialny, to z kolei fizyczny kontekst egzystencji jednostki. Kultura bezpieczeństwa pomaga monitorować przestrzeń społeczną i kontrolować ją pod kątem wystąpienia zagrożeń, czasu i miejsca ich pojawienia się. Następnie do prowadzenia

[9] Kultura masowa, promuje sferę konsumpcji, w której jednostka i rodzina poruszający się w przestrzeni społecznej, w sposób naturalny uczestniczą w rynku konsumpcji dóbr i usług, *odnosi się do zjawisk współczesnego przekazywania wielkim masom odbiorców identycznych lub analogicznych treści płynących z nielicznych źródeł oraz do jednolitych form zabawowej, rozrywkowej działalności wielkich mas ludzkich*, w: A. Kłoskowska, *Kultura masowa*, PWN, Warszawa 2011, s. 95. Należy jednak stanowczo zaznaczyć, że uczestnictwo w tej sferze także może być niebezpieczne z powodu występujących w niej patologii (zwłaszcza konsumeryzmu czy tworzeniu potrzeb pozornych). Rezultatem tego jest zjawisko popadnięcia w materializm, który m.in. procesami prowadzi do zanegowania wartości wyższych w tym sekularyzacji. Dlatego szczególnie ważny w obecnych czasach jest prawidłowo przebiegający proces transmisji kulturowej w procesie socjalizacji, który jest podstawą prawidłowego ukształtowania tożsamości kulturowej, ponieważ *w warunkach dominacji systemu komercjalnego jednostronne uprzywilejowanie elementów kultury wyższego poziomu nie ma żadnych szans realizacji, ponieważ interes konkurujących ze sobą prywatnych producentów masowej kultury zawsze będzie ich skłaniał przede wszystkim raczej do zaspokajania utartych popularnych zainteresowań aniżeli do podejmowania ryzyka kształtowania nowej publiczności skupionej wokół produkcji artystycznej i intelektualnej wyższego poziomu*, op. cit. s. 391.

[10] Zob. C. Bywalec, *Konsumpcja w teorii i praktyce gospodarowania*, Wydawnictwo Naukowe PWN, Warszawa 2007. Zob. także A. Aldridge, *Konsumpcja*, tłum. M. Żakowski, Wydawnictwo Sic!, Warszawa 2006. Więcej na temat patologicznych zjawisk na rynku konsumpcyjnym piszę w: P. Piotrowski, *Tożsamość kulturowa Polaków na tle przemian pokoleniowych*, Oficyna Wydawnicza AFM Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Kraków 2022.

[11] L. Dyczewski definiuje rodzinę, że *jest wspólnotą osób i instytucją społeczną opartą na miłości i wolnym wyborze kobiety i mężczyzny połączonych małżeństwem, którzy odpowiadając wzajemnie za siebie, rodzą i wychowują następne pokolenie w taki sposób, aby także ono rodziło i wychowywało nowe pokolenie. (...) jest ona podstawowym środowiskiem biologicznego i duchowego rozwoju człowieka*, [w:] L. Dyczewski, *Rodzina, społeczeństwo, państwo*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 1994, s. 27.

[12] J. Piwowarski, *Fenomen bezpieczeństwa. Pomiędzy zagrożeniem a kulturą bezpieczeństwa*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2015, s. 46.

skutecznej obrony w razie pojawienia się zagrożenia i przywrócenie bezpieczeństwa oraz dążenie do optimum kontroli poziomu zagrożeń, w procesie rozwoju hierarchii celów podmiotu. Kolejnym etapem jest aktywizacja świadomości istnienia najwyższej potrzeby człowieka w skali indywidualnej i społecznej, poprzez samokształcenie i kreowanie trychotomicznego rozwoju, mentalnego, społecznego i materialnego, przez ukierunkowanie i wspieranie określonych motywacji i postaw wzmacniających indywidualne oraz kolektywne działania na rzecz potencjału autonomicznej obronności (samoobronności) indywidualnych i grupowych podmiotów bezpieczeństwa[13]. Jednostka, lub jednostki tworzące rodzinę, świadomie poruszają się w przestrzeni społecznej, tzn. z właściwie ukształtowaną tożsamością kulturową, na rynku dóbr i usług zabezpieczają możliwość zaspokojenia potrzeb własnych i rodziny, w czasie teraźniejszym i odroczonym (w przyszłości). Planowanie dotyczy przewidywania problemów i niebezpieczeństw i w związku z tym przygotowanie się na rozwiązanie problemów oraz neutralizację niebezpieczeństwa. Duże znaczenie ma przy tym umiejętność podejmowania decyzji w procesie rozwiązywania problemu, związanego z eliminacją niebezpieczeństwa. Podejmowanie decyzji następuje w pewnych określonych warunkach rodzinnych i społecznych. System ten oparty jest na dojrzałości tożsamości kulturowej, przez co drogi wyboru są zróżnicowane, od dojrzałych do poszukujących właściwego wyboru, co spowodowane jest różnym poziomem dojrzałości społecznej, czyli poziomem kompetencji i umiejętności społecznych. Mowa tu o koncepcji *homo eligens* – człowiek wybierający[14], która przedstawia sześć możliwości dokonywania wyboru i podejmowania decyzji, w oparciu o wybrany i możliwy do realizacji ekonomicznie i intelektualnie styl życia. Wprowadzenie zmian wymaga zastosowania przemyślanych planów działania, które ułatwią rozwiązanie problemu i powrót do stanu bezpiecznego. Decyzje jednostki dotyczą jej samej i zabezpieczenia gospodarstwa domowego, a zatem także rodziny, a zatem aspektu zarówno indywidualnego, jak i kolektywnego. Decyzje dotyczące zmian podejmowane są także na szczeblu znacznie wyższym – państwowym, gdzie celem jest zapewnienie bezpieczeństwa ogółowi jednostek. Oczywiście chodzi tu o szeroko pojęte bezpieczeństwo, od energetycznego, zapewnienia dystrybucji środków podstawowych i ich dostępność, po bezpieczeństwo w przestrzeni społecznej i bezpieczeństwo granic, czyli militarne.

[13] Zob. J. Piwowarski, *Fenomen bezpieczeństwa. Pomiędzy zagrożeniem a kulturą bezpieczeństwa*…, s. 46-48.

[14] Koncepcja wyboru homo eligens zakłada sześć możliwości wyboru: pierwsza forma stylu życia dotyczy wyboru w sytuacji ograniczonych możliwości ekonomicznych. Druga forma stylu życia polega na unikaniu wyborów. Trzecia forma stylu życia to poszukiwanie drogi życiowej, a zatem poszukiwanie takich warunków i możliwości, które zaspokoją potrzeby wyższe jednostki (szczególnie w sferze emocjonalnej i poznawczej). Czwarta forma stylu życia jest to działanie jako cel sam w sobie. Piąta forma stylu życia z kolei nastawiona jest na zachowawczy stosunek do podejmowania działań. Dopiero szósta forma stylu życia nastawiona jest na działanie, które prowadzi do zmiany, [w:] P. Piotrowski, *Tożsamość kulturowa Polaków na tle przemian pokoleniowych*, Oficyna Wydawnicza AFM Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Kraków 2022, s. 38-39. Zob. także: P. Gliński, A. Kościański (red.) *Socjologia* i Siciński. *Style życia, społeczeństwo obywatelskie, studia nad przyszłością*, IFiS PAN, Warszawa 2009.

Kultura w aspekcie bezpieczeństwa

Kultura bezpieczeństwa ma zabezpieczyć wartości wyższe, czyli dogmaty funkcjonowania społeczeństwa[15], które powinny być moralnymi wykładnikami funkcjonowania społeczeństwa, oraz wskaźnikami postępowania w sytuacjach społecznych podczas interakcji w sytuacji w przestrzeni społecznej. Zachowanie w miarę spójnej i jednolitej kultury w danym społeczeństwie, konstytuuje zachowanie homogeniczności wartości w społeczeństwie, ponieważ *w obręb kultury wchodzą zachowania ludzkie podporządkowane wspólnym społecznym wzorom i modelom. Cechą społecznych nawyków jest zdolność generalizowania reakcji odnoszonych do pewnego typu podniet, do typu sytuacji życiowych*[16]. Proces wychowania, czyli transmisji kulturowej w procesie socjalizacji, ma zatem szczególnie ważne znaczenie dla prawidłowego ukształtowania tożsamości kulturowej, czyli kierowania się w dorosłym życiu wachlarzem wartości wyższych w podejmowaniu decyzji, ponieważ *kumulatywny rozwój kultury prowadzi do wzrostu komplikacji środków zaspokajania najbardziej elementarnych potrzeb*[17], a ponadto *wyższość złożonych kulturalnych sposobów działania polega przede wszystkim na lepszej gwarancji zaspokojenia potrzeb*[18]. Homogeniczność społeczna wyznawanych przez dane społeczeństwo wartości kulturowych, ma szczególne znaczenie w jakości teraźniejszego życia społecznego oraz w procesie jego dalszej ewolucji, tj. w rozpoznawaniu zagrożeń podważających wartości, *proces przekazywania i przyjmowania określonych wzorów kulturowych podporządkowany jest normom i uznanym społecznym celom. Pod ich wpływem eliminuje się w historycznym doświadczeniu społeczeństw pewne typy zachowań, wzmacnia się zaś nawyki innych układających się w charakterystyczne wzory*[19]. Procesom negacji wartości wyższych (wymienionych w przypisie 14) sprzyja przekaz promowanych przez kulturę masową treści (zob. schemat nr 1).

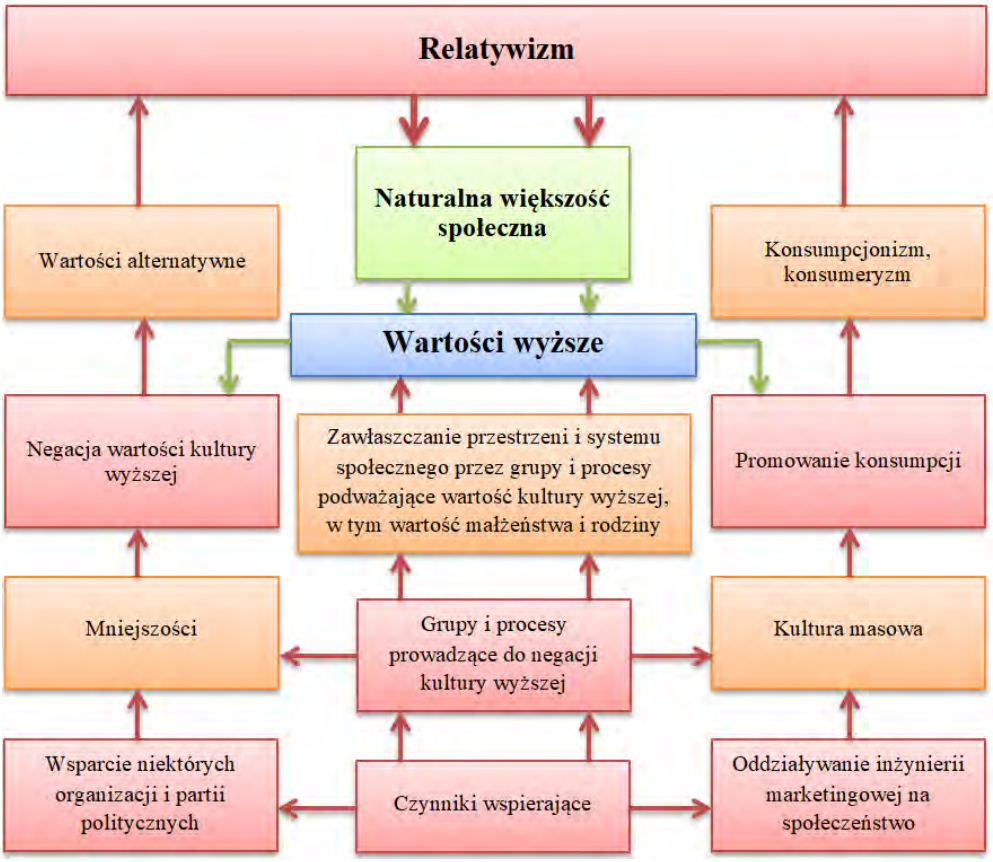
[15] Dogmaty na których oparte są normy funkcjonowania społeczeństwa, są moralnymi wykładnikami, jednak z powodu dokonujących się procesów generujących zmiany społeczne i wymuszanych przez mniejszościowe grupy nacisku relatywistyczne podejście do kultury współczesnej, są negowane i wypierane z rzeczywistości przestrzeni społecznej. Proces ten prowadzi do podważania wartości wyższych, będących dorobkiem kultury wyższej danego społeczeństwa, czyli kształtowanego u jednostki systemu aksjo-normatywnego, przez czynniki takie jak moralność, tradycja, obyczaje i patriotyzm, oparte na historii danego społeczeństwa. Kultura wyższa to całokształt wytworzonych przez dane społeczeństwo aksjomatów, w postaci systemu funkcjonowania społeczeństwa (obyczajowości i tradycji), wytworów intelektualnych i materialnych, takich jak: język, idee, sztuka, praktyki religijne, myśl techniczna, funkcjonujące w społeczeństwie w postaci prac naukowych, literatury pięknej, muzyki, sztuki materialnej (dzieł sztuki), budowli, zabytków techniki i.in. które stanowią spuściznę poprzednich pokoleń i powinny być wartościami budującymi tożsamość kulturową kolejnych. Procesami które prowadzą do negacji kultury wyższej i relatywizacji, są przede wszystkim: sekularyzacja w aspekcie religii oraz profanacja przedmiotów kultu religijnego i uroczystości religijnych, ideologia gender oraz LGBTQ+ w aspekcie rodziny i małżeństwa, oddziaływanie kultury masowej promującej konsumpcję.

[16] A. Kłoskowska, *Kultura masowa*…, s. 29.

[17] *Ibidem*, s. 87.

[18] *Ibidem*, s. 88.

[19] *Ibidem*, s. 51.



Schemat nr 1. Proces negacji kultury wyższej

Źródło: opracowanie własne.

Należy przy tym zwrócić uwagę na to, że etiologia kultury masowej sięga czasów rewolucji przemysłowej. Nastąpiło umasowienie i skomercjalizowanie wartości łatwo przyswajalnych, które przekazują treści wystandaryzowane promujące rozrywkę i radość z konsumpcji przez środki masowego przekazu, które są jej nośnikiem. Standaryzacja powoduje że łatwo przyswajalne treści, nie wymuszające narzucenia samemu sobie nawet minimalnej dyscypliny, stają się wyznacznikami postępowania zastępując wartości wyższe, w tym religię, która z kolei wymusza zachowanie pewnego poziomu ascezy[20]. Treści promowane przez kulturę masową, stają się substytutami[21] kultury wyższej,

[20] Konsumpcja stała się silnym i znaczącym mechanizmem kreowania współczesnej tożsamości jednostki. Konsumpcja, kupowanie, inwestowanie, gospodarowanie, produkowanie określonych dóbr bądź też korzystanie z różnych usług stały się współcześnie tym, co jest obecnie postawą samookreślenia się jednostek, narzędziem realizowania się w uniwersum społecznej przestrzeni ich własnej tożsamości, [w:] A. Radziewicz-Winnicki, Społeczeństwo w trakcie zmiany, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2005, s. 83.

[21] W świecie nowoczesnym wszystko wydawało się zupełnie klarowne, na progu ponowoczesnego wiele rzeczy wygląda nieostro. Dotyczy to zwłaszcza sfery konsumpcji. Implozja tego, co prawdziwe i co sztuczne, wywołuje w nas wrażenie, że różnica między jednym a drugim jest niewyraźna. Praktycznie każdy środek konsumpcji jest miejscem symulowanym lub są w nim symulowane elementy, symulowani ludzie czy symulowane produkty. Nawet rzeczy, które się nadal wydają

kulturowe wytwory społeczeństwa postmodernistycznego nie sięgają głęboko do ukrytych znaczeń. (...) w świecie zmakdonaldyzowanym prawdziwe emocje i uczucia zostały prawie wyeliminowane[22].

Przestrzeń społeczna przez umasowienie kultury, staje się nieprzyjazna dla części społeczeństwa pozostającego w nurcie kultury wyższej w tym biorących udział w praktykach religijnych. Proces relatywizacji prowadzi do negacji wartości o uznanych cechach aksjologicznych. Tożsamość kulturowa, a zatem system aksjo-normatywny w introsystemie jednostki, zostaje poddany próbie na odporność tego skonwencjonalizowanego przekazu, gdzie tylko silnie ukształtowany habitus[23], a za tym gust, jest w stanie utrzymać wysokie oczekiwania zaspokojenia potrzeby estetycznej, *producenci masowej kultury w systemie komercjalnym, którzy dla usprawiedliwienia swojej działalności odwołują się do zasady zaspokajania gustów publiczności, operują obfitym materiałem dowodów wskazującym, że w sytuacji możliwego wyboru atrakcyjne i łatwe treści pozbawione wartości intelektualnych i estetycznych zyskują preferencje znacznej większości odbiorców na niekorzyść dzieł głębokiej myśli i doskonałej sztuki*[24]. Należy przy tym zaznaczyć, że znajomość innych kultur i asymilacja pewnych rytuałów nie jest szkodliwa, o ile nie narusza dogmatycznych podstaw funkcjonowania społeczeństwa[25]. W związku z powyższym szczególne znaczenie dla bezpieczeństwa społecznego, ma zachowanie postawy pełnienia ról społecznych w zgodzie z dogmatami społecznymi. Gwarantuje to ciągłość i powtarzalność oraz replikację (reprodukcję) właściwych wzorów, czego wyrazem jest autonomia własnego indywidualizmu przejawianego w stylu życia i samorealizacji potencjału twórczego. Zapewnia to prawidłowe ukształtowanie tożsamości kulturowej[26], a przez to ułatwia ocenę wartości pod kątem aksjologicznym, tzn. odróżnienia wartości wyższych od pseudowartości, a także próby relatywizacji idei przez mniejszościowe nurty je głoszące, do rangi wartości. Statyka wartości wyższych które są uniwersalne, jest w życiu

prawdziwe, mają coraz więcej elementów sztucznych. W rezultacie nie wiadomo już na pewno, co jest prawdziwe a co sztuczne. Ponadto mamy wokół siebie tyle rzeczy sztucznych, że jest nam dużo lepiej z falsyfikatem niż z oryginałem, [w:] G. Ritzer, G. Ritzer, Magiczny świat konsumpcji, tłum. L. Stawowy, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009, s. 295.

[22] G. Ritzer, *Makdonaldyzacja społeczeństwa*, tłum. L. Stawowy, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009, s. 313-315.

[23] Zob. P. Bourdieu, *Dystynkcja, Społeczna krytyka władzy sądzenia*, Scholar, Warszawa 2005.

[24] A. Kłoskowska, *Kultura masowa*…, s. 390.

[25] Dogmatyczne podstawy funkcjonowania społeczeństwa, to – jak zostało wyjaśnione wcześniej – konwencje kulturowe nabyte w procesie transmisji kulturowej, przebiegającej w procesie socjalizacji. Dogmaty te to obyczaje i tradycje oraz patriotyzm, ukształtowane w toku ewolucji społeczeństwa, oparte na historii i religii.

[26] Tożsamość kulturowa definiuje osobowość i może być definiowana przez pryzmat etosu, który w epoce antycznej *odnosił się (...) do podstawowych cech utożsamianych z osobowością, przeważnie dotyczył on przekonań jednostki, zwyczajów, przyzwyczajeń, ale także sposobów wyrażania własnych ocen, opinii bądź też prezentowanego przez nie zachowania*, [w:] A. Radziewicz-Winnicki, *Społeczeństwo w trakcie zmiany*…, s. 126. Tożsamość z aspektu poznawczego, tj. zinternalizowanych konwencji kulturowych to *koncepcja własnej osoby, „ja" podmiotu, zawiera wiedzę proceduralną lub schematy operacyjne niezbędne do rozwiązywania różnorodnych problemów życiowych oraz konstrukty osobiste, wykorzystywane do zrozumienia wydarzeń i nadawania im sensu poprzez odniesienie do doświadczeń osobistych*, [w:] M. Wróblewska, *Kształtowanie tożsamości w perspektywie rozwojowej i edukacyjnej*, [w:] J. Nikitorowicz, A. Sadowski, J. Muszyńska, M. Sobecki, *Pogranicze. Studia Społeczne*, Tom XVII cz. II (2011), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2011, s. 180.

codziennym odtwarzana dynamicznie, zinternalizowane w konwencjach kulturowych wartości poddawane są interpretacji przez niepowtarzalność i indywidualność introsystemu, co nadaje kontaktom i relacjom międzyjednostkowym zabarwienia emocjonalnego. Kontakty te pomimo swojej schematyczności, są zawsze inne, zaskakujące, czyli spontaniczne, dzieje się tak ponieważ życie społeczne jest dynamiczne. Kultura wyższa nie jest wystandaryzowana czy skonwencjonalizowana, tylko naturalna (do pewnej granicy spontaniczna), chociaż wzory interakcji są powtarzalne, *atutem niezmiennej wagi przyzwyczajeń i codziennej socjalizacji, choć tworzy identyfikacje mniej błyskotliwe, jest regularność: jednostka zawsze do niej wraca. Wbrew nieograniczonej zmienności twórczej socjalizacja ustanawia swego rodzaju barierę ochronną dla bycia sobą, nadając kierunek biograficznym trajektoriom. Niestety, w wypadku nieszczęśliwej jednostki czasów późnej nowoczesności socjalizacja odtwarza się w coraz mniej jednoznacznej formie*[27]. Wyrazem bezpieczeństwa społecznego jest zatem jednoznaczna forma przekazu, pozbawiona relatywizmu kulturowego w stosunku do pseudowartości, które w przypadku uznawania ich przez choćby część społeczeństwa, zaraz znajdują nowych zwolenników i przez swój łatwy przekaz, powodują sztuczną erozję wartości wyższych. Stąd zatem procesy – o których była już mowa – nie wymagające najmniejszej dozy ascezy, gdzie promowane są pseudowartości, *etos infantylizmu kształtuje dziś ideologię i zachowanie naszego radyklanie konsumenckiego społeczeństwa. (...) Konsumpcyjnemu kapitalizmowi trudno się oprzeć i trudno go zmienić, ponieważ stwarza iluzję osobistej wolności, przez co nieformalny przymus staje się niewidzialny, a korzystanie z wolności publicznej jest utrudnione*[28]. Należy przy tym jasno zaznaczyć, że ewolucja kultury wyższej odbywa się tylko na poziomie na którym ona sama jest, przy czym kultury popularna i masowa nie są formami patologicznymi, tylko – jak zostało wyjaśnione wcześniej – są formami o zupełnie innej etiologii[29] a zatem także specyfice, co czyni ich przeznaczenie także innym, ich charakter konsumpcyjny, skonwencjonalizowany i skomercjalizowany sprowadza się do konsumpcji i rozrywki.

Religia w znaczeniu jednostki i rodziny

Jakość życia wymaga oprócz kapitału kulturowego, właściwie ukształtowanego habitusu oraz tożsamości kulturowej, także bogatego życia wewnętrznego (duchowego), co zapewnia bezpieczeństwo egzystencjalne, czyli zaspokojenie potrzeby transcendencji,

[27] Jean-Claude Kaufmann, *Kiedy Ja jest innym*, Oficyna Naukowa, Warszawa 2013, s. 63.

[28] B.R. Barber, *Skonsumowani. Jak rynek psuje dzieci, infantylizuje dorosłych i połyka obywateli*, tłum. H. Jankowska, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009, s. 10-87.

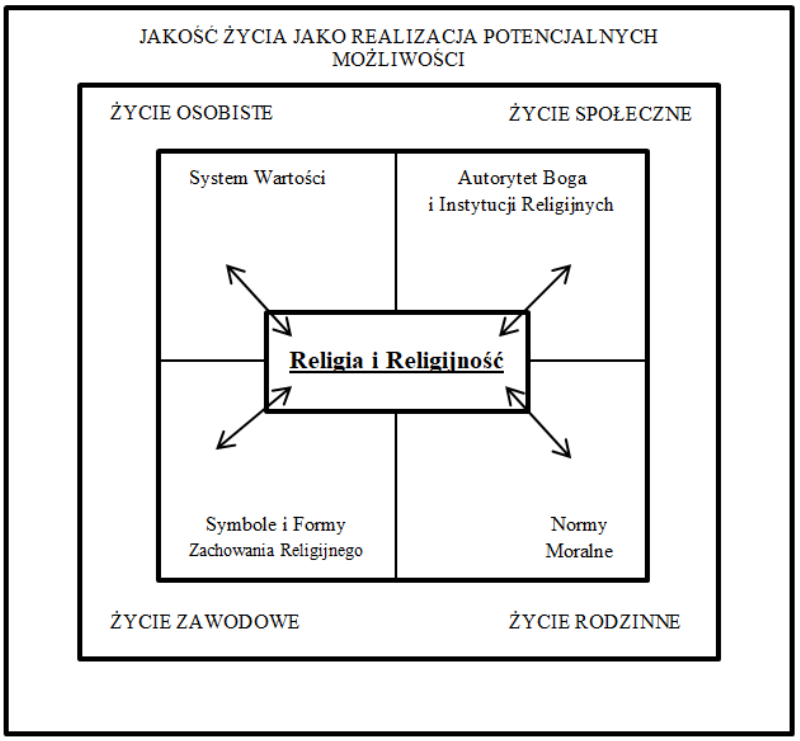
[29] Należy wyjaśnić za A. Kłoskowską, że *społeczeństwo stwarzające warunki powstania kultury masowej charakteryzuje się specyficznymi właściwościami więzi społecznej, które z kolei stanowią funkcje jego ekonomicznego i technicznego rozwoju. Kultura masowa jako dominująca forma organizacji symbolicznej kultury zrodziła się na gruncie społeczeństw uprzemysłowionych i zurbanizowanych. Nie znaczy to, że we współczesnej epoce występowanie kultury masowej ogranicza się wyłącznie do społeczeństw tego typu. Przeciwnie, jej charakterystyczne właściwości sprzyjające szerokiej dyfuzji ułatwiają przenikanie różnych jej form do krajów tzw. słabo rozwiniętych*, w: A. Kłoskowska, *Kultura masowa*…, s. 100-101.

tj. potrzeby religijnej. Potrzeba transcendencji jest zaspokajana na gruncie religii, która jest wyrazem wewnętrznych pragnień jednostki, dotyczących zaspokojenia egzystencjalnego *sensu życia*[30] oraz kodeksem moralnego i etycznego postepowania w codziennej drodze życia. Kultura masowa i promowane przez nią konsumpcjonizm i rozrywka, nie zastąpią w perspektywie czasu doznań duchowych, a doprowadzą do poczucia *pustki egzystencjalnej*[31]. Religia jest psychologicznym korelatem życia wewnętrznego i zewnętrznego, *daje człowiekowi moc, siłę oparcie w chwilach trudnych, nacechowanych niepokojem, obawą w cierpieniu i zwątpieniu. Stanowi także uzasadnienie dla moralności wyrażającej się w dążeniu do własnego rozwoju i poszanowania praw drugiego człowieka i grup społecznych. Pozwala na własną drogę realizowania zadań życiowych*[32]. Niebezpieczeństwo materializmu powodowanego zjawiskami konsumpcjonizmu i konsumeryzmu, skutkuje u jednostki poczuciem złudnego szczęścia, wartości duchowe zatracają sens i są wypierane jako bezwartościowe, z powodu ich nienamacalności i konieczności wdrożenia elementów ascetycznych. Wartość jednostki jako podmiotu, jest oceniana przez wartość posiadanych przez nią dóbr materialnych, co ma świadczyć o rzekomo wyższym statusie nie tylko materialnym, ale także intelektualnym, *nowe środki konsumpcji lepiej charakteryzuje interakcja z rzeczami niż z ludźmi*[33]. Jednak zmiana postrzegania świata przez pryzmat materialny, zmienia poziom relacji międzyludzkich podczas interakcji w sytuacji społecznej w przestrzeni społecznej. Stają się one podporządkowane statusowi materialnemu a nie wartościom humanistycznym, ponieważ *gdy wartości materialistyczne dominują nad innymi stają się pierwszoplanowymi. Człowiek dąży do osiągania zasobów materialnych, a po pewnym czasie to, co posiada znacznie przekracza jego potrzeby egzystencjalne. Koncentrując się na tym, by mieć więcej niż inni, przejawia tendencję do oceniania ludzi przez pryzmat tego, co mają, a nie tego kim są i jakie wartości reprezentują. Rzeczy materialne stają się sposobem zaspokojenia potrzeb jednostki, zaś relacje międzyludzkie mają charakter drugorzędnych, stając się mniej istotnymi*[34]. Dlatego zrozumienie sensu życia w wymiarze egzystencjalnym jest istotnym czynnikiem kształtującym tożsamość kulturową, a dzieje się to przez socjalizację i internalizację wartości religijnych. *Religia i religijność* wyznacza *system wartości* w życiu osobistym, poprzez *autorytet Boga i instytucji religijnych*[35] funkcjonujących w życiu społecznym. Następnie przez religię kształtowane są normy moralne w życiu rodzinnym oraz symbole i formy zachowania religijnego (altruizm społeczny) w życiu

[30] Zob. V.E. Frankl, *Wola sensu. Założenia i zastosowanie logoterapii*, tłum. A. Wolnicka, Czarna Owca, Warszawa 2018.
[31] Zob. S. Kierkegaard, *Bojaźń i drżenie. Choroba na śmierć*, tłum. J. Iwaszkiewicz, Wydawnictwo Naukowe PWN, Warszawa 1981.
[32] D. Buksik, *Znaczenie religijności w życiu człowieka*, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*…, s. 30.
[33] G. Ritzer, *Magiczny świat konsumpcji*…, s. 81.
[34] K. K. Walęcka-Matyja, *Familizm a orientacja wspólnotowa i materializm w okresie dorosłości*, [w:] *Miłość, Małżeństwo, Rodzina. Ujęcie interdyscyplinarne*, Fides es Ratio, Tom 41 Nr 1, Warszawa 2020, s. 243.
[35] D. Buksik, *Znaczenie religijności w życiu człowieka*, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*…, s. 31.

społecznym i zawodowym (zob. schemat nr 2). Altruizm społeczny ma jeszcze inną istotną łączącą i jednoczącą wartość, *ewolucja podpowiada nam, że altruizm i inne nieegoistyczne zachowania mają niezależną użyteczność. W stosunkach społecznych wzajemny altruizm sprzyja przetrwaniu*[36].

Religia nie jest praktyką narzuconą społecznie, tylko wyborem jednostki niezależnie od posiadanego statusu społecznego (przypisanego czy osiągniętego), *nie jest zdominowana przez kulturę, choć wiele z jej religijnego bogactwa czerpie, ale jest autonomiczna, wolna i jednocześnie wciąż poszukująca*[37]. Religia stanowi niezaprzeczalnie zbiór norm etycznych i moralnych o charakterze uniwersalnym, które poprzez doświadczenie wiary są właściwym drogowskazem postępowania, gwarantującym bezpieczeństwo społeczne, *spełnia w osobowości funkcję utrwalającą system uznawanych przez człowieka wartości, daje poczucie bezpieczeństwa, które jest potrzebne dla prawidłowego funkcjonowania osobowości*[38].

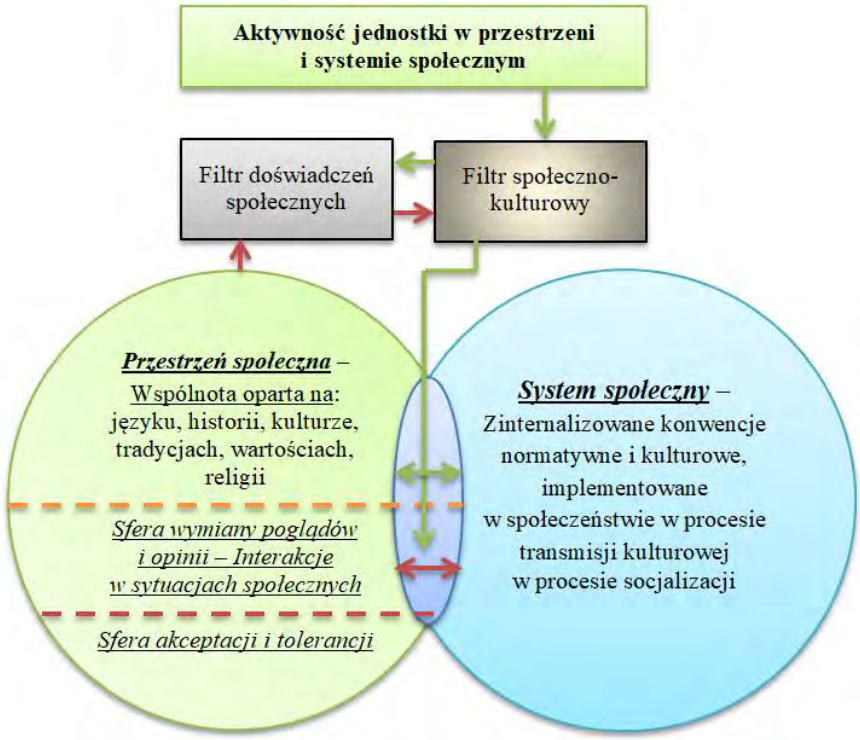


Schemat nr 2. Relacja religii i religijności do jakości życia

Źródło: D. Buksik, *Znaczenie religijności w życiu człowieka*, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*…, s. 32.

[36] R. Patel, *Wartość niczego. Jak przekształcić społeczeństwo rynkowe i na nowo zdefiniować demokrację*, tłum. H. Jankowska, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2010, s. 41.
[37] D. Buksik, *Znaczenie religijności w życiu człowieka*, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*…, s. 28.
[38] Ibidem, s. 30.

Aktywność jednostki w przestrzeni społecznej opiera się wspólnych wartościach uniwersalnych, takich jak język, historia, kultura, tradycje i wartości oraz religia[39] (zob. schemat nr 3), zatem wspólne wartości powinny łączyć członków społeczeństwa polskiego, tymczasem procesy o których była mowa wcześniej dzielą je.



Schemat nr 3. Aktywność jednostki w przestrzeni i systemie społecznym

Źródło: Opracowanie własne.

Podział społeczeństwa spowodowany jest silnym dążeniem pewnych grup do relatywizacji idei nie mających podstaw kulturowych, konstytucyjnych czy prawnych. Powodem tego są wystąpienia mniejszości, a skutkiem zagrożenie bezpieczeństwa wewnętrznego z jednej strony z aspektu kulturowego, z drugiej zagrożenia nasileniem się anarchii.

Socjalizacja w znaczeniu bezpieczeństwa wartości społecznych

Biorąc pod uwagę powyższe rozważania, z których wynika jak ważne jest prawidłowe ukształtowanie tożsamości kulturowej jednostek, widać jak ważny jest proces transmisji kulturowej w przebiegu procesu socjalizacji, odbywający się w fazie pierwotnej na gruncie

[39] Zob. P. Piotrowski, *Tożsamość kulturowa Polaków na tle przemian pokoleniowych*, Oficyna Wydawnicza AFM Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Kraków 2022.

rodziny, następnie w fazie wtórnej w jednostkach edukacyjnych. W rodzinie zaczyna się kształtowanie człowieka jako osoby i jego tożsamości kulturowej, socjalizacja pierwotna ma kluczowe znaczenie do późniejszej wysokiej jakości życia, ponieważ w rodzinie kształtowane są postawy życzliwości i miłości wobec innych. (…) stabilność środowiska rodzinnego stanowi bardzo istotny czynnik równowagi i zdrowia psychicznego dziecka[40]. Od jej jakości zależy bezpieczeństwo społeczne w znaczeniu wspólnoty, czyli wyrażanie i kierowanie się tymi samymi wartościami w przestrzeni społecznej[41], prawidłowa, kochająca się, spójna rodzina, poprzez wpływ na kształtowanie właściwej samooceny, interioryzację systemu wartości, ucząc radzenia sobie ze stresem, mi ze przeciwdziałać wpływom grup dewiacyjnych, może niwelować wpływ niepowodzeń szkolnych[42]. W toku procesów transmisji kulturowej i socjalizacji, jednostka przyswaja konwencje kulturowe (w tym religię) w postaci: języka, zachowania i interakcji w sytuacjach społecznych, kształtowany jest także system aksjonormatywny w którym zawarty jest system moralno-etyczny. Socjalizacja jest procesem zamierzonym jeżeli dziecko nabywa wiedzę i umiejętności w sposób zamierzony, świadomy, niezamierzonym z kolei wtedy, kiedy uczy się w sposób niezamierzony poprzez obserwację i naśladowanie innych. Całokształt procesu socjalizacji (zamierzonej i niezamierzonej) to wychowanie, *czyli proces polegający na formowaniu wychowanka zgodnie z obowiązującymi modelami życia charakterystycznymi dla danej ideologii czy społecznego systemu. Wychowanie w optyce osobowej jest spotkaniem osób, mistrza i ucznia, poprzez które otwiera się horyzont wartości, dzięki którym człowiek staje się człowiekiem, bez względu na ideologię czy system społeczny*[43]. Introsystem jednostki jest kształtowany przez interakcję ze środowiskiem zewnętrznym, przyjęta informacja zwrotna – pozytywna lub negatywna – jest przetwarzana przez filtr społeczno-kulturowy[44] i filtr doświadczeń społecznych, przetworzone treści kształtują osobowość (czyli świadomość pozycji, statusu i ról społecznych), i formują system aksjonormatywny (moralny i etyczny). System motywacji i zaangażowania kształtowany jest przez stymulację potrzeby poznawczej, co przekłada się na kapitał kulturowy (wiedzę i umiejętności), zasoby kulturowe i potencjał kulturowy, czego efektem jest poziom kapitału społecznego (kompetencje społeczne)[45]. Reakcja zwrotna na interakcje, jest kształtowana przez emocje zewnętrzne (wywołane podczas interakcji) i wewnętrzne już ukształtowane, o potencjale pozytywnym lub negatywnym. Formułowaniu reakcji zwrotnej towarzyszą reakcje fizjologiczne organizmu (eustres,

[40] M. Ryś, *Wychowanie do miłości*, [w:] F. Adamski (red.), *Wychowanie osobowe*, Petrus, Kraków 2011, s. 180.
[41] Kultura masowa „socjalizuje" nowych konsumentów, *społeczeństwo konsumpcji jest także społeczeństwem przyuczania do konsumpcji, społecznego tresowania i wdrażania w konsumpcję, innymi słowy, nowym i swoistym modelem uspołecznienia*[41], [w:] J. Baudrillard, *Społeczeństwo konsumpcyjne, jego mity i struktury*, tłum. S. Królak, Wydawnictwo Sic!, Warszawa 2006, s. 94
[42] M. Ryś, *Wychowanie do miłości*, [w:] F. Adamski (red.), *Wychowanie osobowe*…, s. 180.
[43] T. Gadacz, *Wychowanie jako spotkanie osób*, [w:] F. Adamski (red.), *Wychowanie osobowe*…, s. 93-94.
[44] Zob. A. Rębowska, *Elementy socjologii przestrzeni w badaniach empirycznych*, Wydawnictwo Naukowe UP, Kraków 2009.
[45] Zob. P. Piotrowski, *Tożsamość kulturowa Polaków na tle przemian pokoleniowych*, Oficyna Wydawnicza AFM Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Kraków 2022.

dystres, itd.). Przez wyżej wymienione procesy kształtowana jest także tożsamość, czyli prezentowana przez jednostkę jako podmiot osobowy postawa, wyrażająca jej autonomiczną interpretację i opinię, dotyczącą danej kwestii. W przypadku tożsamości kulturowej, dotyczy ona przyjmowania postawy i kierowania się wartościami wyższymi, w tym religijnymi (systemem aksjonormatywnym, moralnością), na które składają się historia, kultura w tym tradycje i obyczaje oraz religia, w opiniowaniu czy podejmowaniu decyzji. W procesie interpretacji i opiniotwórczym, bardzo ważne są filtr kulturowy i filtr doświadczeń społecznych, zawierających zinternalizowane wzory postepowania, które są modyfikowane przez doświadczenia. Dlatego wykładnikiem podmiotowości jednostki, jest jakość jej kapitału kulturowego, ponieważ *tożsamość jako struktura poznawcza (teoria „ja"), służy za osobistą podstawę odniesienia (reference) dla interpretacji osobistego doświadczenia, w tym informacji odnoszących się do „ja", do celów sterujących aktywnością, do sensu życia*[46].

Stawanie się osobą – działającym podmiotem – jest procesem złożonym i długotrwałym, którego podstawą jest wychowanie (czyli procesy socjalizacyjne niezamierzone,), *osobą staje się człowiek wówczas, gdy otwierając się na dobro, prawdę i piękno, uczestniczy w wartościach i je urzeczywistnia, dokonując preferencji zgodnej z ich hierarchicznym układem: od wartości najniższych (materialnych), poprzez wartości duchowe ku wartościom absolutnym*[47]. Formowanie tożsamości, które odbywa się podczas *stawania się osobą* jest procesem kilkuetapowym, gdzie docelowo *Ja* jednostki odkrywa poziom duchowy, *poczucie tożsamości, czyli poczucie tego, kim jesteśmy, kształtuje się z jednej strony na podstawie indywidualnych cech i osobistej historii życia (mówimy wówczas o tożsamości osobistej), z drugiej natomiast – tworzy się w związku z pełnionymi przez dziecko rolami, a więc rolą płciową i innymi rolami społecznymi (jest to wówczas tzw. tożsamość społeczna)*[48].

Fazy kształtowania się *Ja*[49] jednostki, obejmują etapy: *Ja* cielesnego, *Ja* psychicznego i *Ja* duchowego. *Ja* cielesne dotyczy okresu niemowlęctwa, czyli poznania własnego ciała, *Ja* psychiczne dotyczy drugiego i trzeciego roku życia, dziecko mówi o sobie nie w pierwszej osobie „Ja", tylko w trzeciej. Z czasem zaczyna mówić o swoich rzeczach w pierwszej osobie „moje", a w kolejnym etapie w pierwszej osobie już o samym sobie, czyli „Ja". Trzeci etap dotyczy okresu dojrzewania, kiedy „Ja" zaczyna być uświadamiane. Uświadomienie *Ja*, to odkrycie siebie jako indywidualnej i niepowtarzalnej osoby, to okres kiedy następuje akceptacja samego siebie i internalizacja nabytych konwencji kulturowych

[46] M. Wróblewska, *Kształtowanie tożsamości w perspektywie rozwojowej i edukacyjnej*…, s. 180.
[47] T. Gadacz, *Wychowanie jako spotkanie osób*, [w:] F. Adamski (red.), *Wychowanie osobowe*…, s. 89.
[48] M. Wolicki, *Prawdziwość :Ja" a jakość relacji osobowych*, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*…, s. 11.
[49] *Ja jako Ja osobowe jest także Ja świadomym i jako takie właśnie jest nosicielem wolności człowieka*, [w:] R. Kozłowski, *Wewnętrzny nauczyciel człowieka*, Wydawnictwo Psychologii i Kultury Eneteia, Warszawa 2008, s. 31.

oraz samookreślenie siebie jako osoby w przestrzeni społecznej[50]. Świadomość własnego *Ja* jest drogą do kształtowania tożsamości kulturowej, wtedy rozpoczyna się internalizacja nabytych wzorów kulturowych. Kształtowanie uczuciowości wyższej w introsystemie, rozpoczyna się od okresu niemowlęctwa i polega na odczuwaniu przez dziecko potrzeby pierwotnej – uczucia miłości, ponieważ *aby człowiek mógł osiągnąć dojrzałość osobową konieczne jest doświadczanie miłości*[51]. Niepowtarzalność oraz indywidualny charakter człowieka jako osoby z ukształtowaną tożsamością kulturową, wymusza podczas kształtowania jego introsystemu indywidualnego podejścia pedagogicznego, które pozwoli na stymulację potrzeby poznawczej i rozwinięcie jego talentów przez przekaz kapitału kulturowego, w postaci umiejętności kształtujących kompetencje społeczne. Procesy socjalizacji i edukacji mają na celu ukształtowanie osobowości jednostki, przez proces spontanicznych i zaplanowanych oddziaływań bodźcowych na dziecko. Przy czym proces socjalizacji pierwotnej związany jest z przyswajaniem języka, czyli środka komunikacji, zachowań właściwych ze względu na sytuację a także elementarnych umiejętności interakcji w sytuacjach społecznych. Prawidłowy rozwój jednostki jest oprócz procesu socjalizacji pierwotnej, uzależniony od systemu edukacyjnego i nauczyciela, który ma bezpośredni kontakt z wychowankiem w procesie nauczania. Okazywana przez nauczyciela życzliwość, zainteresowanie wychowankiem i umiejętność dotarcia do jego warstwy emocjonalnej, uczy go także miłości do innych ludzi, *miłość zaczyna się zazwyczaj od zwrócenia uwagi na rozmaite wartości estetyczne, intelektualne czy moralne. Ostatecznie jednak miłość jest odpowiedzią na indywidualną, niepowtarzalną wartość drugiego człowieka jako osoby. Znaczenie miłości polega przede wszystkim na tym, że nadaje ona życiu jakość wyższą i dynamiczną, skierowaną ku doskonałości moralnej*[52]. Emocje (pozytywne lub negatywne) wyrażamy za pośrednictwem języka niewerbalnego przez mimikę twarzy i postawę naszego ciała, co jest związane ze spontaniczną reakcją i przekazem niezamierzonym, co najłatwiej dostrzec właśnie u dzieci, dlatego ciało jest dla człowieka *ważnym narzędziem wyrażania miłości wobec innych*[53]. W wieku dojrzałym, po okresie dorastania jednostka osiąga umiejętność wyrażania siebie jako indywidualnego bytu, poprzez posiadany kapitał kulturowy i umiejętności oraz nabyte kompetencje społeczne, samourzeczywistnia swój potencjał kulturowy oraz człowieczeństwo jako podmiot osobowy. Poprzez to doskonali własną tożsamość kulturową, dzięki której jest zdolny do wyrażania miłości wobec innych i docelowo wobec innej osoby jako wybranki czy wybranka życia (żony, męża) oraz dzieci.

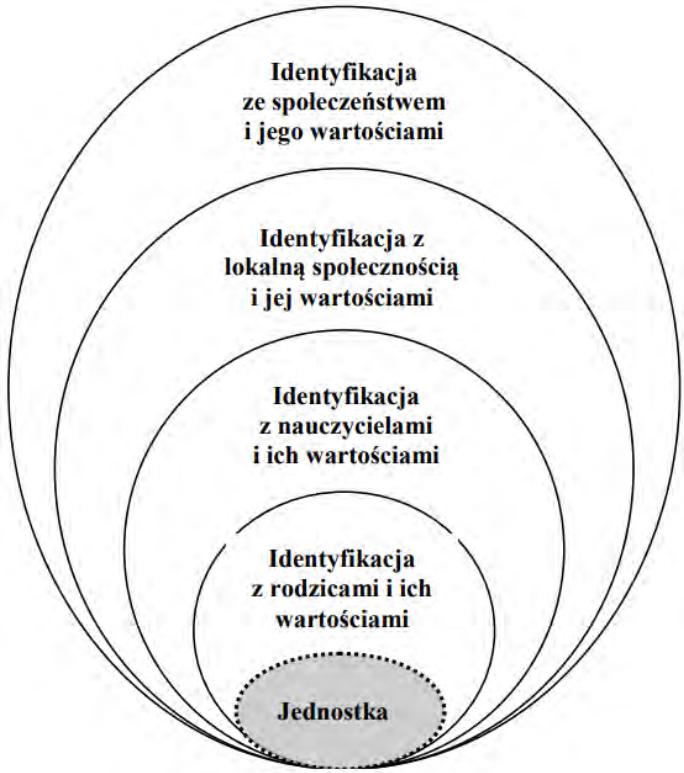
[50] Zob. także cztery fazy rozwoju według F. Adamskiego: sfera biologiczno-popędowa, psychiczno-uczuciowa, społeczno-kulturowa, świadomościowo-moralna, [w:] F. Adamski, *Edukacja, rodzina, kultura. Studia z pedagogiki społecznej*, Wydawnictwo UJ, Kraków 1999.

[51] M. Ryś, *Wychowanie do miłości*, [w:] F. Adamski (red.), *Wychowanie osobowe*…, s. 168

[52] M. Śnieżyński, *Roztropność nauczycielska*, Petrus, Kraków 2020, s. 104.

[53] J. Bagrowicz, *Godność osoby fundamentem wychowania*, [w:] F. Adamski (red.), *Wychowanie osobowe*…, s. 105.

Kształtowanie introsystemu i tożsamości kulturowej, jest złożonym konglomeratem procesów odbywających się w społeczeństwie w skali mikrospołecznej – rodzina i makrospołecznej – grupy społeczne (szkolna, itp.), których finalnym efektem jest ukształtowanie sfery wewnętrznej (zob. schemat nr 4), tj. introsystemu i tożsamości kulturowej, *wewnętrzny układ odniesienia staje się drogowskazem działania i instancją moralną w ocenie siebie, swoich działań oraz postępowania innych ludzi. Po okresie eksploracji ofert działania i kryjących się za nimi wartości musi nastąpić ich uporządkowanie i integracja oraz w efekcie podejmowanych decyzji – identyfikacja z wartościami dla siebie najcenniejszymi ze wszystkich poziomów struktury społecznej*[54]. Działanie filtra kulturowego pomaga inicjować i właściwie wykonać poszczególne czynności zawarte w schematach rytuałów życia codziennego, a filtr doświadczeń społecznych je utrwalić i poprzez nabywanie nowych doświadczeń modyfikować.



Schemat nr 4. Obszary identyfikacji w procesie kształtowania się tożsamości

Źródło: A. Brzezińska, *Dzieciństwo i dorastanie: korzenie tożsamości osobistej i społecznej*…, s. 27.

[54] A. Brzezińska, *Dzieciństwo i dorastanie: korzenie tożsamości osobistej i społecznej*, [w:] A.W. Brzezińska, A. Hulewska, J. Słomska (red.), *Edukacja regionalna*, Wydawnictwo Naukowe PWN, Warszawa 2006, s. 26.

Finalnym efektem socjalizacji powinna być prawidłowo ukształtowana tożsamość kulturowa – czyli introsystem oraz zinternalizowane umiejętności altruistyczne, które mają szczególne znaczenie w małżeństwie, tj. szacunek i odpowiedzialność, troska, dbałość o rozwój współmałżonka, stworzenie warunków oparcia psychicznego, empatii, które tworzą warunki autonomii i możliwości ekspresji w wyrażaniu samych siebie oraz samorealizacji swojego potencjału twórczego. W warunkach wolności poglądów (demokracji) w przestrzeni społecznej, jednostki powinny mieć możliwość wyrażania swojego potencjału, poprzez własne poglądy i opinie, zasady moralne ukształtowane przez wartości wyższe i religię, jednak ze względu na postępujące procesy nowych ruchów społecznych, staje się to coraz bardziej trudniejsze, ale wciąż możliwe i namacalne, ponieważ podczas każdej pojawiającej się w społeczeństwie anomii, jedynymi wartościami do jakich możemy się odwołać, są wartości wyższe, które są uniwersalne.

Wnioski

Elementy składające się na bezpieczeństwo jednostki i rodziny, a w aspekcie społecznym bezpieczeństwo wewnętrzne, to przede wszystkim stały nurt kulturowy, czyli w miarę stała homogeniczność wyznawanych wartości wyższych i religii. Wartości te są jednak podważane przez nowe ruchy społeczne, które relatywizują własne poglądy do poziomu równego z wartościami wyższymi, a procesom tym sprzyjają treści głoszone przez kulturę masową. Zapoczątkowało to procesy, które trwają obecnie i maja tendencję pogłębiania się i przyspieszania, jednak w postulowanej przez mniejszości formie, nie mają one racji bytu. Należy przy tym jasno zaznaczyć, że inne niższe formy kultur współistnieją z kulturą wyższą w pewnej symbiozie, jednak wykorzystywane są w coraz większym stopniu do promowania jedynie konsumpcjonizmu, a przez to pseudowartości. W związku z tym prawidłowo ukształtowana i silna tożsamość kulturowa jednostki, jest filtrem w dokonywaniu prawidłowych wyborów. Umiejętność korzystania z rynku dóbr i usług przez jednostkę, jest jedną z podstaw egzystencji przez którą poszukuje sensu życia. Kierowanie się wartościami wyższymi, czyli dogmatami funkcjonowania społeczeństwa w tym religią, stanowią podstawę bezpieczeństwa społecznego. Przy tym należy zauważyć, że wartości wyższe i religijne nakazują tolerancję dla innych kultur i religii. Proces dyfuzji kultur i czerpanie z innych pewnych rytuałów, nie powodują szkód dla kultury macierzystej (np. rytuał picia kawy i różnych jej rodzajów, co jest nabytkiem kultury polskiej zapożyczonym z włoskiej). Tolerancja dotyczy także mniejszości, którym korzystanie z pełni praw obywatelskich gwarantuje konstytucja Rzeczpospolitej Polskiej, w tym dowolny wybór stylu życia. Jednak równość wynika z praw obywatelskich, tolerancja z wartości kultury i przede wszystkim z przykazania religii, natomiast akceptacja lub jej brak jest wolnym wyborem jednostki. Dlatego nie ma możliwości spełnienia postulatów mniejszości, które nie wynikają z kultury, religii czy prawodawstwa,

w tym konstytucji, która jasno definiuje kwestie funkcjonowania społeczeństwa. Relatywizm kulturowy nie jest remedium na postulaty mniejszości, niezgodne z obowiązującymi w społeczeństwie polskim wartościami, ponieważ *ekspresja wolności nie może naruszać wolności innych. (...) pozytywne nastawienie do wolności „innego" pozwoliłoby na to, by akt wolności wyrażał się w dobrowolnej rezygnacji z części interesów własnych (i ich wolnościowej ekspresji) w imię częściowego uwzględnienia interesów innych ludzi*[55]. Czym innym jest asymilacja pewnych rytuałów zapożyczonych z innych kultur, do kultury macierzystej (np. wspomniany już rytuał picia kawy), które nie zagrażają wartościom wyższym ukonstytuowanym w kulturze, tylko ją wzbogacają. Współistnienie wartości innych kultur poprzez proces dyfuzji (ich przenikania się) jest możliwe, jednak należy przyjąć że te kultury pochodzą z jednego kręgu i ich wartości mają podobne dogmaty funkcjonowania społeczeństwa. W ten sposób – poprzez internalizację rytuałów z innej kultury – ewoluuje kultura macierzysta. W przeciwnym przypadku, nie dokona się dyfuzja, ani asymilacja, nawet przez relatywizację.

Bibliografia:

Barber B. R., *Skonsumowani. Jak rynek psuje dzieci, infantylizuje dorosłych i połyka obywateli*, tłum. H. Jankowska, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009.

Baudrillard J., *Społeczeństwo konsumpcyjne, jego mity i struktury*, tłum. S. Królak, Wydawnictwo Sic!, Warszawa 2006.

Buksik D., *Znaczenie religijności w życiu człowieka*, [w:] Daszykowska J., Rewera M. (red.), *Wokół problemów jakości życia współczesnego człowieka*, Petrus, Kraków 2012.

Czuryk M., *Bezpieczeństwo jako dobro wspólne*, *Zeszyty Naukowe KUL* 61 (2018), nr 3 (243), Wydawnictwo Katolickiego Uniwersytetu Lubelskiego, Lublin 2018.

Dyczewski L., *Rodzina, społeczeństwo, państwo*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 1994.

Gadacz T., *Wychowanie jako spotkanie osób*, [w:] Adamski F. (red.), Wychowanie osobowe, Petrus, Kraków 2011.

Kaufmann Jean-Claude, *Kiedy Ja jest innym*, Oficyna Naukowa, Warszawa 2013.

Klimek M., Samorząd terytorialny w trosce o jakość życia mieszkańców wspólnoty lokalnej, [w:] J. Daszykowska, M. Rewera (red.), *Wokół problemów jakości życia współczesnego człowieka*, Petrus, Kraków 2012.

Kłoskowska A., *Kultura masowa*, PWN, Warszawa 2011.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 nr 78 poz. 483.

Kozłowski R., *Wewnętrzny nauczyciel człowieka*, Wydawnictwo Psychologii i Kultury Eneteia, Warszawa 2008.

Maslow A.H., *Motywacja i osobowość*, PWN, Warszawa 2013.

Patel R., *Wartość niczego. Jak przekształcić społeczeństwo rynkowe i na nowo zdefiniować demokrację*, tłum. H. Jankowska, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2010.

Pawłowicz J. J., *Ideologia gender realnym zagrożeniem dla małżeństwa i rodziny*, [w:] *Teologia i Moralność*, tom 11, Poznań 2012.

Piotrowski P., *Tożsamość kulturowa Polaków na tle przemian pokoleniowych*, Oficyna Wydawnicza AFM Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Kraków 2022.

Piwowarski J., *Fenomen bezpieczeństwa. Pomiędzy zagrożeniem a kulturą bezpieczeństwa*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2015.

Radziewicz-Winnicki A., *Społeczeństwo w trakcie zmiany*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2005.

Ritzer G., *Magiczny świat konsumpcji*, tłum. L. Stawowy, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009.

[55] H. Świda-Ziemba, *Dylematy między wolnością a wspólnotą w demokracji liberalnej*, [w:] I. Jakubowska-Branicka (red.), *O tolerancji we współczesnej demokracji liberalnej*, Wydawnictwo Trio, Warszawa 2010, s. 124.

Ritzer G., *Makdonaldyzacja społeczeństwa*, tłum. L. Stawowy, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009.
Ryś M., *Wychowanie do miłości*, [w:] Adamski F. (red.), *Wychowanie osobowe*, Petrus, Kraków 2011.
Śnieżyński M., *Roztropność nauczycielska*, Petrus, Kraków 2020.
Świda-Ziemba H., *Dylematy między wolnością a wspólnotą w demokracji liberalnej*, [w:] Jakubowska-Branicka I. (red.), *O tolerancji we współczesnej demokracji liberalnej*, Wydawnictwo Trio, Warszawa 2010.
Walęcka-Matyja K. K., *Familizm a orientacja wspólnotowa i materializm w okresie dorosłości*, [w:] *Miłość, Małżeństwo, Rodzina. Ujęcie interdyscyplinarne*, Fides es Ratio, Tom 41 Nr 1, Warszawa 2020.
Wolicki M., *Prawdziwość :Ja" a jakość relacji osobowych*, [w:] Daszykowska J., Rewera M. (red.), *Wokół problemów jakości życia współczesnego człowieka*, Petrus, Kraków 2012.
Wróblewska M., *Kształtowanie tożsamości w perspektywie rozwojowej i edukacyjnej*, [w:] J. Nikitorowicz, Sadowski A., Muszyńska J., Sobecki M., *Pogranicze. Studia Społeczne*, Tom XVII cz. II (2011), Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2011.
Zdrodowski B., *Istota bezpieczeństwa państwa*, [w:] *Studia de Securitate* 9(3) (2019), Wydawnictwo Naukowe UP, Kraków 2019.

ISSN 2956-7424