

AKADEMIA POMORSKA W SŁUPSKU



BEZPIECZEŃSTWO I PROBLEMY PSYCHOSPOŁECZNE W WARUNKACH PANDEMII COVID-19

**Bezpieczeństwo
i problemy psychospołeczne
w warunkach pandemii
COVID-19**

Akademia Pomorska w Słupsku

**Bezpieczeństwo
i problemy psychospołeczne
w warunkach pandemii
COVID-19**

Redakcja naukowa

Ewa Matuska – Arkadiusz Gryko

Recenzenci

Dr hab. Krzysztof Janasz, prof. US

Dr hab. Tomasz Kawka, prof. UG

Dr hab. Małgorzata Sidor-Rządkowska, prof. PW

Dr hab. Edward Stawasz, prof. UŁ

Dr hab. Blanka Tundys, prof. US

Dr hab. Jarosław Waśniewski, prof. UG

Dr hab. Elżbieta Wojnicka-Sycz, prof. UG

© Copyright by Akademia Pomorska w Słupsku, 2021

Fot. na okładce

pixabay.com

Korekta

Stanisław Powąła-Niedźwiecki

Wydawnictwo „Bernardinum” Sp. z o.o.

ul. Biskupa Dominika 11, 83–130 Pelplin

tel. 58 536 17 57, fax 58 536 17 26

bernardinum@bernardinum.com.pl

www.bernardinum.com.pl

Skład, druk i oprawa:

Drukarnia Wydawnictwa „Bernardinum” Sp. z o.o., Pelplin

ISBN 978-83-8127-788-4

Spis treści

Wstęp	7
--------------------	----------

CZĘŚĆ I. WYBRANE KWESTIE BEZPIECZEŃSTWA W ZWIĄZKU Z PANDEMIA COVID- 19	11
---	-----------

Rozdział 1 – Renata Szanter <i>Bezpieczeństwo ICT w polskich przedsiębiorstwach w świetle pandemii COVID-19</i>	13
---	-----------

Rozdział 2 – Joanna Grubicka <i>Bezpieczeństwo cyfrowe organizacji w dobie pandemii COVID-19.....</i>	43
---	-----------

Rozdział 3 – Michał Olejniczak, Aleksandra Jopek, Patrycja Nadolska, Natalia Ostrowska, Agata Sokołowska <i>Bezpieczeństwo ekonomiczne i zarządzanie kryzysowe przedsiębiorców województwa pomorskiego w początkach pandemii koronawirusa</i>	65
---	-----------

Rozdział 4 – Mariola Bartusek <i>Bezpieczeństwo i higiena pracy pielęgniarek w czasie trwania pandemii</i>	83
--	-----------

Rozdział 5 – Rafał Parczewski, Arkadiusz Chomacki <i>Bezzałogowe statki powietrzne w procesie zapewnienia bezpieczeństwa w Polsce</i>	99
---	-----------

**CZĘŚĆ II. WYBRANE KWESTIE PSYCHOSPOŁECZNE
W ZWIĄZKU Z PANDEMIĄ COVID-19 111**

Rozdział 6 – Joanna Grzegorczyk

Działania CSR w obliczu pandemii COVID-19 113

Rozdział 7 – Patryk Toczyński

*E-obywatel a bezpieczny obywatel – stosowanie rozwiązań
technologicznych w okresie pandemii COVID-19 129*

Rozdział 8 – Aleksandra Skrabacz

*Wybrane aspekty zachowań psychospołecznych młodych
Polaków w dobie pandemii koronawirusa 143*

Rozdział 9 – Tadeusz A. Grzeszczyk, Jacek Pelszyński

*Ocena efektów społecznych projektów rozwojowych
podlegających cyfrowej transformacji w warunkach
pandemii COVID-19 163*

Rozdział 10 – Mikhail Kulapov, Sergey Yashin, Svetlana Zakharova

*Life quality change assessment of the population of Russia
in the conditions of COVID-19 pandemics 187*

Wstęp

„Nikt nie jest bezpieczny, dopóki wszyscy nie będą bezpieczni” – Erna Solberg

Pojawienie się wirusa SARS-CoV-2 i jego globalne rozprzestrzenienie oraz ogrom spustoszeń, jaki wniósł on w sferę bezpieczeństwa społecznego i ekonomicznego indywidualnych istnień, grup społecznych i zawodowych oraz przedsiębiorstw, stale nas zaskakuje. Szczególnie bolesne są negatywne reperkusje pandemii COVID-19 w świecie bezpieczeństwa zdrowotnego populacji różnych regionów oraz bezpieczeństwa społecznego, analizowanego w jego różnych aspektach. Kolejne odsłony mutacji wirusa, odkrywanie i wdrażanie do produkcji nowych wariantów szczepionek oraz różne tempo wyszczepialności poszczególnych grup obywateli to zdarzenia, które dzieją się równolegle i tworzą bardzo skomplikowaną trajektorię powiązań, której skutki w dużej mierze są stale nieznanne.

Wirus ponownie konfrontuje nas z rzeczywistością opisaną akronimem VUCA, tj., zmienną (V – *volatile*), niepewną (U – *uncertain*), złożoną (C – *complex*) i niejednoznaczną (A – *ambiguous*)¹ i pokazuje, jak bardzo nie jesteśmy na nią przygotowani jako jednostki, grupy społeczne i zawodowe, regiony czy państwa. Uzmysławia nam to, jak bardzo nasze (analizowane w realiach polskich), dość dobrze okrzepnięte co najmniej od okresu po II wojnie światowej, poczucie bezpieczeństwa personalnego, społecznego, informacyjnego, ekonomicznego czy też regionalnego okazuje się kruche i złudne.

¹ Akronim VUCA: *Volatility* (zmiennność, ulotność), *Uncertainty* (niepewność), *Complexity* (złożoność) i *Ambiguity* (niejednoznaczność) pojawił się pod koniec lat 80. w pracach wojskowych strategów z U.S. Army War College jako opis globalnej sytuacji politycznej, która powstała po zakończeniu „zimnej wojny”. W XXI w termin jest stosowany w koncepcjach zarządzania strategicznego. Por. Bennett N., Lemione G.J., *What a difference a word makes: Understanding threats to performance in a VUCA world*, „Business Horizons” 2014, vol. 3, s. 3.

Konstatacja, iż pandemia COVID-19 naruszyła bezpieczeństwo makro-ekonomiczne, polityczne i psychospołeczne indywidualnych osób, grup czy organizacji, jest tyleż oczywista, co niesatysfakcjonująca. Opis skali i rodzaju chociażby wycinkowych zakłóceń na etapie ciągłej emisji mutacji wirusa jest jednak niezbędnym, także po to, by planować i wdrażać coraz bardziej skuteczne środki ochrony i zabezpieczeń.

Proponowana publikacja pt. *Bezpieczeństwo i problemy psychospołeczne w warunkach pandemii COVID-19* podejmuje próbę wglądu w temat, którego nie sposób zamknąć w łamach jednej pracy monograficznej. Tym niemniej podjęcie tego tematu i jego realizacja nawet w ograniczonym zakresie wydaje się niezwykle aktualna i potrzebna.

Celem pracy jest opis i analiza wybranych zagrożeń bezpieczeństwa społecznego i ekonomicznego oraz cyfrowego, które pojawiły się wraz z rozprzestrzenianiem się pandemii, a także przedstawienie rekomendacji oraz dobrych praktyk, które mogą zostać wykorzystane do minimalizowania zagrożeń, które niesie ze sobą pandemia. Dynamika tych zagrożeń i ich skala postawiły przed badaczami, reprezentującymi różne dyscypliny naukowe, nowe wyzwania związane z opisaniem i wyjaśnieniem zmian zachodzących we wszystkich sferach życia społeczno-gospodarczego. Niniejsza publikacja, zawierająca m.in. wyniki badań prowadzonych zarówno z perspektywy lokalnej, jak i ogólnokrajowej, jest próbą odpowiedzi na te właśnie wyzwania. Oczywiście, z uwagi na skalę i złożoność opisywanych zagrożeń, monografia ta nie wyczerpuje zagadnienia. Należy ją traktować jako kolejny głos w dyskursie naukowym na ten temat.

Autorzy poszczególnych rozdziałów monografii poszukują odpowiedzi na liczne pytania badawcze, m.in.: w jaki sposób pandemia COVID-19 wpłynęła na kondycję ekonomiczną pomorskich przedsiębiorców?, jak polscy przedsiębiorcy przygotowani są do zapewnienia cyberbezpieczeństwa kierowanym przez siebie organizacjom?, w jaki sposób izolacja społeczna wpłynęła na młodych Polaków w kwestii ich relacji z innymi ludźmi, sposób spędzania czasu wolnego oraz pracę i naukę? w jaki sposób zmieniająca się sytuacja pandemiczna wpłynęła na podejmowanie przez przedsiębiorstwa inicjatywy z zakresu społecznej odpowiedzialności biznesu?, jak szeroko rozpowszechnione w okresie pandemii komunikowanie się, m.in. z urzędami administracji publicznej za pośrednictwem kanałów teleinformatycznych, wpływa na bezpieczeństwo danych osobowych użytkowników tych systemów?

Publikację stanowi dziesięć rozdziałów rozdzielonych do dwóch części. Pierwsza część, pt. *Wybrane kwestie bezpieczeństwa w związku z pandemią COVID-19*, składa się z pięciu rozdziałów, poświęconych głównie bezpieczeństwu cyfrowemu, ekonomicznemu oraz bezpieczeństwu pracy. Kolejne pięć opracowań, składających się na część *Wybrane kwestie psychospołeczne w związku z pandemią COVID-19*, poświęconych jest zagadnieniom związanym z sytuacją jednostki w covidowej i postcovidowej rzeczywistości oraz działaniom państwa i organizacji gospodarczych m.in. na rzecz ograniczenia dolegliwości skutków pandemii. Zaprezentowane w publikacji opracowania mają zarówno charakter badawczy, jak i teoretyczny, niejednokrotnie o charakterze studiów przypadków.

W rozdziale pierwszym pt. *Bezpieczeństwo cyfrowe organizacji w dobie pandemii COVID-19* Renata Szanter przedstawia, w jakim zakresie małe, średnie i duże polskie przedsiębiorstwa, które z konieczności musiały szybko przestawić się na korzystanie z narzędzi cyfrowych w znacznie większym niż wcześniej zakresie, wdrażają narzędzia ograniczające ryzyko występowania incydentów bezpieczeństwa. Rozważania na ten temat zawiera także rozdział drugi: *Bezpieczeństwo ICT w polskich przedsiębiorstwach w świetle pandemii COVID-19* autorstwa Joanny Grubickiej. Autorka zwróciła w nim uwagę na konieczność prowadzenia przez przedsiębiorców działań obejmujących rozwiązania technologiczne, organizacyjne oraz w zakresie podnoszenia kompetencji pracowników, które umożliwią wypełnienie luki w systemach bezpieczeństwa cyfrowego. Rozdział trzeci autorstwa Michała Olejniczaka oraz współautorek pt. *Bezpieczeństwo ekonomiczne i zarządzanie kryzysowe przedsiębiorców województwa pomorskiego w początkach pandemii koronawirusa* stanowi próbę zdiagnozowania, w oparciu o przeprowadzone badania, zagrożeń w bezpieczeństwie ekonomicznym przedsiębiorców, do jakich dochodzi w sytuacji gwałtownych zmian w gospodarce. Kwestię zapewnienia bezpiecznych warunków pracy pielęgniarcom zaangażowanym w walkę z koronawirusem podjęła Mariola Bartusek w opracowaniu *Bezpieczeństwo i higiena pracy pielęgniarek w czasie trwania pandemii*. Pierwszą część książki zamyka prezentacja możliwości wykorzystania dronów w działaniach na rzecz bezpieczeństwa przedstawiona w rozdziale *Bezzałogowe statki powietrzne w procesie zapewnienia bezpieczeństwa w Polsce*, przygotowanym przez Rafała Parczewskiego oraz Arkadiusza Chomackiego.

Drugą część publikacji – *Wybrane kwestie psychospołeczne w związku z pandemią COVID-19* – otwiera praca Joanny Grzegorzczak pt. *Działania CSR w obliczu pandemii*, poruszająca bardzo aktualną kwestię ewolucji koncepcji społecz-

nej odpowiedzialności biznesu w obliczu pandemii koronawirusa. W siódmym rozdziale, zatytułowanym *E-obywatel a bezpieczny obywatel – stosowanie rozwiązań technologicznych w okresie pandemii COVID-19*, Patryk Toczyński analizuje rozwój kanałów komunikacji elektronicznej, umożliwiających obywatelom kontakt z urzędami administracji publicznej, m.in. w kontekście bezpieczeństwa danych osobowych. W kolejnym opracowaniu – *Wybrane aspekty zachowań psychospołecznych młodych Polaków w dobie pandemii koronawirusa* – Aleksandra Skrabacz prezentuje wyniki badań przeprowadzonych wśród studentów jednej z warszawskich uczelni, poświęcone wpływowi pandemii na wybrane dziedziny życia tej grupy społecznej, ze szczególnym uwzględnieniem pracy i nauki oraz relacji z ludźmi. Z kolei Tadeusz A. Grzeszczyk i Jacek Pelszyński przedstawiają w rozdziale *Ocena efektów projektów rozwojowych podlegających cyfrowej transformacji w warunkach pandemii COVID-19* studium przypadku transformacji cyfrowej ogólnopolskiej infolinii, przyczyniającej się do ograniczania wpływu negatywnych skutków pandemii COVID-19 na społeczeństwo. Publikację zamyka opracowanie Mikhaila Kulapova, Sergeya Yashina i Svetalany Zakharowej pt. *Life quality change assessment of the population of Russia in the conditions of COVID-19 pandemics* poświęcone zmianom wskaźników życia ludności w okresie pandemii i przeglądowi stosowanych przez państwo środków wsparcia przedsiębiorstw i obywateli w tym czasie.

Opracowania te stanowią przykłady aktualnych naukowych rozważań, które implikują szerokie zagadnienia bezpieczeństwa i problemów społecznych w okresie pandemii COVID-19. Poszukiwane w nich próby wyznaczenia istotnych powiązań na linii zagrożenie–ochrona są bardzo cenne i inspirujące. Identyfikowanie i analiza tych związków, prognozowanie ich skutków bezpośrednich i długofalowych – to ambitne zadanie dla badaczy i materiał dla kolejnych publikacji. Ta, którą tu przedstawiamy, mamy nadzieję, wzbudzi zainteresowanie czytelnika i zachęci go do dalszego zgłębiania wiedzy na ten temat.

Dziękujemy wszystkim, którzy przyczynili się do powstania tej monografii.

Ewa Matuska i Arkadiusz Gryko

CZĘŚĆ I

WYBRANE KWESTIE BEZPIECZEŃSTWA W ZWIĄZKU Z PANDEMIĄ COVID-19

Renata Szanter

Akademia Pomorska w Słupsku

Instytut Bezpieczeństwa i Zarządzania, Katedra Zarządzania

e-mail: renata.szanter@apsl.edu.pl

ORCID: 0000-0002-7864-9497

Rozdział 1

Bezpieczeństwo ICT w polskich przedsiębiorstwach w świetle pandemii COVID-19

Streszczenie: Transformacja cyfrowa wytycza ścieżki na przyszłość, napędzając jednostki biznesowe do szybkiego przyjęcia nowych technologii cyfrowych. Celem niniejszego opracowania jest identyfikacja ryzyka cyfryzacji biznesu w kontekście pandemii COVID-19, poprzez analizę działań podejmowanych przez polskich przedsiębiorców w celu zapewnienia cyberbezpieczeństwa w odniesieniu do zagrożeń pojawiających się w środowisku cybernetycznym. Na potrzeby analizy wykorzystano dane z internetowej bazy Eurostatu: badanie wspólnotowe dotyczące wykorzystania ICT i e-commerce w przedsiębiorstwach – polityka bezpieczeństwa: środki, zagrożenia i świadomość personelu oraz Raport Barometr Cyberbezpieczeństwa 2021 KPMG. Analiza danych pozwala zdiagnozować stopień, w jakim małe, średnie i duże polskie przedsiębiorstwa wdrażają narzędzia ograniczające ryzyko występowania incydentów związanych z bezpieczeństwem, zwłaszcza że dla wielu zmiana modeli biznesowych i konieczność korzystania z rozwiązań cyfrowych stała się w dzisiejszej rzeczywistości koniecznością. Wnioski z analizy mogą stanowić inspirację dla zarządzających przedsiębiorstwami w zakresie konieczności podejmowania konkretnych działań w związku z pojawiającymi się zagrożeniami cybernetycznymi.

Słowa kluczowe: cyberbezpieczeństwo, cyberzagrożenia, cyfryzacja, bezpieczeństwo ICT, pandemia COVID-19

Wprowadzenie

Transformacja cyfrowa toruje drogę dla przyszłości biznesu, wymagając szybkiego przyjęcia nowych technologii cyfrowych. Jest to klucz do sukcesu jutra. Jednak każda zmiana wiąże się z ryzykiem, a cyberataki i naruszenia bezpieczeństwa cybernetycznego są jednymi z największych czynników ryzyka¹. Najnowszy The Global Risks Report 2021 16th Edition wskazuje na globalne ryzyko w obszarze bezpieczeństwa cybernetycznego, zauważając, że infrastruktura i stosowane środki bezpieczeństwa cybernetycznego rządów, przedsiębiorstw i gospodarstw domowych zostaną prześcignięte lub staną się przestarzałe w wyniku coraz bardziej wyrafinowanych i częstych cyberprzestępstw. To z kolei prowadzi do zakłóceń gospodarczych, strat finansowych, napięć geopolitycznych i niestabilności społecznej. Ponadto brak globalnie akceptowanych ram, instytucji lub regulacji dotyczących korzystania z technologii cyfrowych w wyniku przyjęcia przez różne państwa lub grupy państw niekompatybilnej infrastruktury cyfrowej, protokołów i standardów².

Pandemia COVID-19 wywarła wpływ na większość dziedzin życia. Spowodowała, że również polskie przedsiębiorstwa musiały zmierzyć się z wieloma wyzwaniami, takimi jak organizacja pracy zdalnej czy też zmiana w relacjach z klientami bądź dostawcami. W związku z tym musiano wprowadzić bardzo szybko rozwiązania, które być może były planowane w dłuższej perspektywie czasu, jednak musiały zaistnieć tu i teraz, ponieważ taka była potrzeba.

Celem rozdziału jest identyfikacja ryzyka związanego z cyfryzacją przedsiębiorstw poprzez analizę działań podejmowanych przez polskie firmy w celu zapewnienia cyberbezpieczeństwa w odniesieniu do pojawiających się zagrożeń w obszarze cybernetycznym, w kontekście trwającej pandemii COVID-19. Na potrzeby analizy wykorzystano dane z internetowej bazy Eurostatu: badanie wspólnotowe dotyczące wykorzystania ICT i e-commerce w przedsiębiorstwach – polityka bezpieczeństwa: środki, zagrożenia i świadomość personelu (kod danych online ISOC_CISCE_RA) oraz dane zawarte w najnowszym

¹ Fujitsu, *Five key actions to empower secure digital transformation*, <https://www.fujitsu.com/global/services/security/insights/digital-transformation/#5keyactions> (dostęp: 15.05.2021).

² Academic Advisers National University of Singapore, Oxford Martin School, University of Oxford, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, *Global Risks Report 2021 16th Edition*, World Economic Forum In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 2021, s. 89.

Raporcie Barometr Cyberbezpieczeństwa KPMG³. Wykorzystano dane uporządkowane w internetowej bazie danych Eurostatu według roku badania, które odnoszą się do sytuacji na początku tego samego roku, w którym przeprowadzono badanie. Większość z nich pochodzi z badania w 2019 r., wyjątek stanowią dane z grupy wdrożenia polityki bezpieczeństwa ICT w firmach (rok badania 2015). Jednostką miary jest odsetek przedsiębiorstw (przedsiębiorstwo w rozumieniu rozporządzenia EWG nr 696/93), z wyłączeniem sektora finansowego, zatrudniających co najmniej 10 pracowników. W analizie przedstawiono dane w podziale na wybrane wskaźniki społeczeństwa informacyjnego we wszystkich przedsiębiorstwach bez sektora finansowego oraz w podziale na przedsiębiorstwa małe (10–49 pracowników), średnie (50–249 pracowników) i duże (250 i więcej pracowników) bez sektora finansowego w Polsce oraz 27 krajach UE od 2020 r. Dane zostały pogrupowane jako te związane z posiadaniem i aktualizacją polityki bezpieczeństwa teleinformatycznego firmy, stosowaniem określonych środków bezpieczeństwa, wdrażaniem procedur, kierunkami polityki bezpieczeństwa, podejmowaniem działań uświadamiających i szkolących pracowników w zakresie zagrożeń oraz przestrzeganiem procedur związanych z utrzymaniem cyberbezpieczeństwa, a także tym, przez kogo realizowana jest polityka bezpieczeństwa firmy. Drugim źródłem danych poddanych analizie są dane z Raportu Barometr Cyberbezpieczeństwa KPMG. Badanie, zlecone firmie Norstat Polska, przeprowadzono metodą wywiadów telefonicznych CATI wśród osób odpowiedzialnych za bezpieczeństwo IT w firmach (członków zarządu, dyrektorów ds. bezpieczeństwa, prezesów, dyrektorów IT lub innych osób odpowiedzialnych za ten obszar), na próbie 100 organizacji, na przełomie stycznia i lutego 2021 r., z których duże firmy (powyżej 250 osób) stanowiły 54% badanych, średnie (50–249 osób) 43% oraz małe (do 49 osób) 3%. Wykorzystując dostępne źródła danych, przeanalizowano poziom gotowości przedsiębiorstw do funkcjonowania w przestrzeni zdigitalizowanej, w odniesieniu do najczęstszych przyczyn i skutków naruszeń bezpieczeństwa oraz podjęto próbę uchwycenia dynamiki zmian zachodzących w opisywanych działaniach w związku z pojawieniem się pandemii COVID-19. Analiza danych statystycznych daje również obraz poziomu zapewniania cyberbezpieczeństwa przez małe, średnie i duże firmy w Polsce w porównaniu z poziomem zabezpieczeń w krajach UE. Wnioski z analizy mogą stanowić inspirację dla zarządzają-

³ KPMG, *Barometr Cyberbezpieczeństwa. Covid 19 przyspiesza cyfryzację firm*, 2021.

cych przedsiębiorstwami w zakresie konieczności podejmowania konkretnych działań w związku z pojawiającymi się zagrożeniami cybernetycznymi.

Identyfikacja cyberzagrożeń, ich źródeł oraz skutków dla przedsiębiorstw

Cyberbezpieczeństwo wg Ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r. to „odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”⁴. Należy doprecyzować znaczenie pojęcia system informacyjny, który to definiowany jest w Ustawie jako system teleinformatyczny, sprecyzowany wcześniej w Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne jako „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875)⁵, wraz z przetwarzanymi w nim danymi w postaci elektronicznej”. W praktyce system informacyjny to urządzenia, których używają firmy, takie jak: laptopy, komputery, telefony czy też serwery, połączone ze sobą siecią teleinformatyczną, przetwarzające, przechowujące, wysyłające i odbierające różnego rodzaju dane. Analizując definicję cyberbezpieczeństwa, należy zwrócić uwagę na pojęcia poufności danych, integralności danych, dostępności danych oraz ich autentyczności. Wymienione właściwości, wg definicji zawartych w PN-I-13335-12⁶, są następujące:

- „poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
- integralność – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

⁴ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, <https://sap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf> (dostęp: 26.05.2021).

⁵ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20050640565/U/D20050565Lj.pdf> (dostęp: 26.05.2021).

⁶ PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.

- dostępność – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
- autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji)”.

Oczywiście tym, co podlega ochronie, wg definicji, są dane lub związane z nimi usługi.

Priorytety w zakresie bezpieczeństwa cybernetycznego są bardzo zróżnicowane, a różnice te można wyraźnie zaobserwować na poziomie poszczególnych krajów. Ponadto organizacje przestępcze wykorzystują luki w zabezpieczeniach cybernetycznych, czerpiąc z tego zyski. Coraz większa świadomość pojawiających się zagrożeń cybernetycznych pozwala na skuteczną walkę z nimi i ochronę przed utratą danych oraz stratami finansowymi, zarówno na poziomie biznesu, jak i rządu⁷. Allianz Risk Barometr 2021 wskazuje na coraz większą zależność społeczeństwa i biznesu od technologii i aktywów niematerialnych oraz przyspieszenie tego trendu z uwagi na zmianę przez firmy modeli biznesowych i sposobów pracy, co wymusiła poniekąd pandemia. Technologia z jednej strony może być użytecznym narzędziem zapewniającym ciągłość działalności, na przykład poprzez przejście na pracę zdalną i monitorowanie procesów lub sprzedaż i serwis online, z drugiej strony niesie ze sobą również nowe zagrożenia. Przykładowo cyfryzacja łańcuchów dostaw może potencjalnie zmniejszyć częstotliwość występowania zakłóceń w działalności gospodarczej, ale może też prowadzić do poważniejszych zakłóceń w przypadku wystąpienia awarii, powodującej np. przerwę w dostawie, czy właśnie cyberataku. Również pandemia niesie ze sobą ryzyka związane z przerwaniem działalności w sieci, np. awarie chmury spowodowane tym, że wraz z dużym zainteresowaniem na tego typu usługi pojawi się niebezpieczeństwo pracy firm technologicznych na granicy możliwości i nadejdzie moment, w którym technologia i obsługa staną się napięte lub osiągną swoje ograniczenia. Jeśli cyfryzacja nie zostanie przeprowadzona prawidłowo, z należyтым uwzględnieniem ryzyka, scenariusz awarii głównego dostawcy usług w chmurze może stać się rzeczywistością. Raport donosi, że incydenty cybernetyczne spadły wprawdzie na trzecią pozycję, ale obawy z nimi związane są nadal duże. Więcej respondentów w 2020 r. uznało je za główne zagrożenie. Cyberprzestępczość kosztuje obecnie światową

⁷ J. Caracelli, N. Jones, *Cyber Security. Threats and Responses for Government and Business*, PRAEGER 2019, s. 151.

gospodarkę ponad 1 bilion dolarów, więcej niż jeden procent światowego PKB – wzrost o 50% w porównaniu z rokiem 2019⁸. Według respondentów Allianz Risk Barometer firmy najbardziej obawiają się naruszenia danych w ciągu najbliższego roku. Zaraz za tym zagrożeniem, w związku z coraz częstszą pracą zdalną, plasuje się podatność IT na ataki ransomware, których liczba i dotkliwość wzrasta. Trzecie miejsce zajmują błędy pracowników, co odzwierciedla fakt, że błędy i problemy techniczne są najczęstszym generatorem roszczeń. „Naruszenia danych pozostają największym zmartwieniem dla większości firm, szczególnie tych, które mają do czynienia z dużymi ilościami danych osobowych, np. detaliści, dostawcy usług medycznych i banki” – mówi Catharina Richter, globalna szefowa Allianz Cyber Center of Competence. Z kolei ataki ransomware są stałym zagrożeniem dla coraz większej liczby branż, takich jak produkcja i sektor usługowy, i mogą być przyczyną znaczących zakłóceń w działalności. Atakujący nadal wprowadzają innowacje, podczas gdy egzekwowanie przepisów i kary za naruszenie danych kontynuują swój trend wzrostowy. Dominujące formy oprogramowania ransomware – m.in. Sodinokibi, Maze, Ragnarok i Ryuk – spowodowały poważne zakłócenia dla producentów, podmiotów sektora publicznego i podmiotów świadczących usługi opieki zdrowotnej, firm przewozowych, przedsiębiorstw użyteczności publicznej, firm technologicznych i firm świadczących usługi profesjonalne. Prawie pół miliona incydentów ransomware zostało zgłoszonych globalnie w 2019 r. i trend ten ma się utrzymywać. Dla przestępców jest to bardzo atrakcyjny sposób ataku – niski koszt i niskie ryzyko. Takie ataki stają się również coraz bardziej ambitne. Podczas gdy kiedyś hakerzy atakowali małe i średnie firmy, teraz ich celem są również duże firmy, gdzie nagrody są najwyższe. Zaważalnym ostatnio trendem jest dodanie prywatności i gotowość hakerów do wykorzystywania marki i reputacji. Cyberprzestępcy grożą ujawnieniem danych lub upublicznieniem naruszenia, jeśli żądania nie zostaną spełnione. Żądania ransomware wzrosły o prawie jedną trzecią między drugim i trzecim kwartałem 2020 r., jak podaje Coveware⁹, firma reagująca na incydenty, podczas gdy prawie 50% przypadków zawierało groźbę ujawnienia skradzionych danych. Wiele zmian jest wymuszanych na firmach, a tempo ich wprowadzania będzie tylko rosło wraz z pandemią. Cyberbezpieczeństwo i ciągłość biznesowa mogą

⁸ Allianz Global Corporate & Specialty SE, *Identifying the major business risks for 2021*, Allianz Risk Barometer, 2021, s. 17–19.

⁹ CoveWare, *The Coveware Quarterly Ransomware Report 2020*, <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report> (dostęp: 17.05.2021).

mieć trudności z dotrzymaniem kroku. Przejściu na pracę zdalną we wczesnych fazach etapów blokady towarzyszyło obniżenie poziomu cyberbezpieczeństwa – niektóre firmy wyłączyły wieloczynnikowe uwierzytelnianie – podczas gdy pracownicy pracujący z domu są bardziej podatni na ataki phishingowe¹⁰. W szczytowym momencie ryzyko cybernetyczne było kiedyś postrzegane wyłącznie jako problem dotyczący komputerów i oprogramowania, ale wraz z przyspieszeniem cyfryzacji w coraz większym stopniu obejmuje wszystko – od samochodów przez fabryki po inteligentne urządzenia w naszych domach. Pojawiają się obszary, takie jak sztuczna inteligencja (AI), np. *deepfakes*, gdzie realistyczne treści medialne (zdjęcia, audio i wideo) są zmodyfikowane lub sfalszowane przez AI. Cyfryzacja łańcuchów dostaw, automatyzacja i „Internet rzeczy”, a także nowe sposoby pracy mogą stwarzać możliwości dla hakerów i otwierać nowe podatności¹¹. Anne Adams i Martina Angela Sasse z University College London przeprowadziły badania, które wykazały, że użytkownicy mogą naruszać mechanizmy bezpieczeństwa komputera, takie jak uwierzytelnianie za pomocą haseł, zarówno świadomie, jak i nieświadomie. Przyczyną takiego zachowania jest często sposób implementacji mechanizmów bezpieczeństwa oraz brak wiedzy użytkowników. Stwierdziły, że aby zmienić ten stan rzeczy, działy bezpieczeństwa powinny w większym stopniu komunikować się z użytkownikami¹². Podsumowując, zachęcają do zwrócenia uwagi na to, że bezpieczeństwo systemu musi być widoczne i dostrzegane, aby organizacja traktowała je poważnie. Zwracają również uwagę na informowanie użytkowników o istniejących i potencjalnych zagrożeniach dla systemów organizacji oraz wrażliwości zawartych w nich informacji, aby użytkownicy systemu nie postrzegali tych działań jako zło konieczne, przez które muszą przejść. Również osoby odpowiedzialne za kwestie bezpieczeństwa powinny być widoczne w działaniu całej organizacji¹³. Celem badania przeprowadzonego w 2017 r. przez Lee Hadlingtona¹⁴ było ustalenie, czy impulsywność, uzależnienie od internetu i stosunek pracowników do cyberbezpieczeństwa służą do przewidywania częstotliwości podejmowania ryzykownych zachowań związanych z cyberbezpieczeństwem. Jednym z klu-

¹⁰ Allianz Global Corporate & Specialty SE, *Identifying the major business risks for 2021*, Allianz Risk Barometer, 2021, s. 17–19.

¹¹ Tamże, s. 19.

¹² A. Adams, M.A. Sasse, *Users are not the enemy*, Communications of the ACM, 1999, s. 1.

¹³ Tamże, s. 7.

¹⁴ L. Hadlington, *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*, Heliyon, 2017, s. 13–14.

czowych wniosków było to, że zdolność do zaszczepienia dobrych zachowań w zakresie cyberbezpieczeństwa należałoby postrzegać jako nadrzędne dla wszystkich organizacji, niezależnie od ich wielkości i złożoności. Około 98% ankietowanych scedowało odpowiedzialność za cyberbezpieczeństwo firmy na kierownictwo, a dalsze 58% stwierdziło, że nie wie, w jaki sposób mogą chronić firmę przed cyberprzestępczością. Badania wykazały, że stopień, w jakim osoby angażują się w ryzykowne zachowania związane z cyberbezpieczeństwem, jest również ściśle powiązany z poziomem problematycznego lub uzależniającego korzystania z internetu. Dowiedziono również, że element impulsywności niezwiązany z planowaniem jest istotnym negatywnym zwiastunem ryzykownych zachowań związanych z cyberbezpieczeństwem. Autor zwrócił też uwagę na element edukacji w zakresie bezpieczeństwa informacji, która musi wykra-
czać poza zwykłe dostarczanie informacji użytkownikom. Informacje muszą być ukierunkowane, muszą być przydatne, istotne i musi wystąpić *feedback*, aby osoby mogły ocenić, jak dobrze sobie radzą. Takie środki dają także możliwość zidentyfikowania osób, które stanowią większe ryzyko dla organizacji pod względem nieprzestrzegania dobrych praktyk w zakresie cyberbezpieczeństwa oraz przeszkolenie ich w tym zakresie.

Cyberbezpieczeństwo w polskich przedsiębiorstwach – zagrożenia i podejmowane działania

Wyeliminowanie wszystkich zagrożeń dla systemów informatycznych nie jest oczywiście możliwe. Świadomość zagrożeń, ich źródeł, stała aktualizacja zabezpieczeń technicznych oraz rozwój systemu bezpieczeństwa danych jest podstawowym obowiązkiem współczesnych organizacji. Budując politykę bezpieczeństwa, firmy opierają się na wytycznych zawartych w unijnych aktach prawnych oraz przede wszystkim prawie krajowym.

Zarządzanie bezpieczeństwem informacji, zasobu posiadającego wymier-
ną wartość i narażonego na różnego rodzaju zagrożenia, nie dotyczy jedynie ochrony systemów informatycznych. Zapewnia również bezpieczeństwo danych osobowych, informacji handlowych oraz innych danych stanowiących tajemnicę przedsiębiorstwa. Podmioty prowadzące działalność gospodarczą są zobli-
gowane prawnie do ochrony informacji, a niewywiązanie się z tego obowiązku pociąga za sobą skutki prawne. Szczególne znaczenie wśród obowiązujących aktów prawnych ma oczywiście ustawa o ochronie danych osobowych, która

obliguje przedsiębiorców do dostosowania systemów informatycznych oraz procedur postępowania w organizacji do obowiązującego prawa. Ma to na celu zapewnienie najwyższego poziomu ochrony przetwarzanych informacji. Jeśli firma chce go zapewnić, musi myśleć o wdrożeniu systemu zarządzania bezpieczeństwem informacji, które to powinno odbywać się zgodnie z obowiązującymi normami. Polska norma PN-ISO/IEC 27001 przedstawia model systemu zarządzania bezpieczeństwem informacji, a także określa wymagania dla ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia systemu. Takie zintegrowane działania podnoszą świadomość pracowników, pomagają w zarządzaniu ryzykiem oraz ustanawiają cele i zasady bezpieczeństwa informacji¹⁵. Idąc w ślad za obowiązującym przepisami, należy zwrócić uwagę na ustawę o krajowym systemie cyberbezpieczeństwa, obowiązującą od 28 sierpnia 2018 r. i implementującą Dyrektywę Parlamentu Europejskiego i Rady Europejskiej w sprawie środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium UE, tzw. Dyrektywa NIS, która nakłada na przedsiębiorców nowe obowiązki. Ustawa określa ramy krajowego systemu cyberbezpieczeństwa, który ma za zadanie zapewnić bezpieczeństwo cyfrowe na poziomie krajowym i głównie dotyczy organów państwa, operatorów kluczowych, dostawców usług cyfrowych, podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, podmiotów publicznych, samorządów terytorialnych i spółek komunalnych. Ponadto wspomniana już ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, w tym akt wykonawczy Krajowe Ramy Interoperacyjności, przepisy z zakresu RODO, czy też ustawa o ochronie informacji niejawnych nie mogą być traktowane pojedynczo, ale muszą ze sobą współgrać i się uzupełniać. Bezpieczeństwo systemów teleinformatycznych, zarządzanie i ochrona informacji, jak i ochrona danych osobowych muszą tworzyć spójny system. Oczywiście przedsiębiorcy nienależący do podmiotów objętych ww. ustawami nie są zobligowani do wdrażania wymogów w nich zawartych. Niemniej nie powinni tych przepisów ignorować i uznawać za nieistotne. Każde przedsiębiorstwo jest narażone na cyberataki, a jeżeli tak, to powinno podejmować kroki, które zminimalizują to ryzyko. Realne działania podejmowane przez polskie firmy w związku z zapewnieniem cyberbezpieczeństwa ich przedsiębiorstw zostały zestawione w tabeli 1.

¹⁵ Polskie Centrum Badań i Certyfikacji, <https://www.pcbc.gov.pl/pl/uslugi/certyfikacja-systemow-zarzadzania/pn-iso-iec-27001> (dostęp: 26.05.2021).

Tabela nr 1. Działania podjęte przez polskie oraz unijne przedsiębiorstwa w celu zapewnienia cyberbezpieczeństwa

Wskaźnik społeczeństwa informacyjnego	Wszystkie polskie przedsiębiorstwa, bez sektora finansowego (10 lub więcej osób zatrudnionych)	Małe polskie przedsiębiorstwa (10–49 osób zatrudnionych), bez sektora finansowego	Średnie polskie przedsiębiorstwa (50–249 osób zatrudnionych), bez sektora finansowego	Duże polskie przedsiębiorstwa (250 lub więcej osób zatrudnionych), bez sektora finansowego	Wszystkie przedsiębiorstwa UE, 27 krajów, bez sektora finansowego (10 lub więcej osób zatrudnionych)
Zastosowany środek bezpieczeństwa ICT: silne uwierzytelnianie za pomocą hasła	76%	73%	88%	95%	76%
Zastosowany środek bezpieczeństwa ICT: utrzymywanie aktualnego oprogramowania (w tym systemów operacyjnych)	81%	78%	93%	97%	87%
Zastosowany środek bezpieczeństwa ICT: identyfikacja i uwierzytelnianie użytkownika za pomocą metod biometrycznych wdrożonych przez przedsiębiorstwo	7%	6%	10%	17%	10%
Zastosowany środek bezpieczeństwa ICT: techniki szyfrowania danych, dokumentów lub poczty elektronicznej	37%	32%	54%	75%	38%
Zastosowany środek bezpieczeństwa ICT: tworzenie kopii zapasowych danych w oddzielnym miejscu (w tym tworzenie kopii zapasowych w chmurze)	57%	53%	74%	86%	76%

Zastosowany środek bezpieczeństwa ICT: kontrola dostępu do sieci (zarządzanie dostępem urządzeń i użytkowników do sieci przedsiębiorstwa)	61%	56%	82%	94%	65%
Zastosowany środek bezpieczeństwa teleinformatycznego: VPN (Virtual Private Network rozszerza sieć prywatną na sieć publiczną w celu umożliwienia bezpiecznej wymiany danych w sieci publicznej)	30%	24%	53%	86%	42%
Zastosowany środek bezpieczeństwa ICT: utrzymywanie plików dziennika w celu analizy po incydentach bezpieczeństwa	29%	22%	51%	79%	45%
Zastosowany środek bezpieczeństwa ICT: Ocena ryzyka ICT, tj. okresowa ocena prawdopodobieństwa i konsekwencji wystąpienia incydentów bezpieczeństwa ICT	24%	20%	41%	64%	33%
Stosowany środek bezpieczeństwa ICT: testy bezpieczeństwa ICT	27%	21%	47%	70%	35%
Przedsiębiorstwa stosujące dowolny środek bezpieczeństwa ICT	87%	85%	96%	99%	92%
Przedsiębiorstwa posiadały formalnie zdefiniowaną politykę bezpieczeństwa ICT (od 2015 r.)	13%	9%	28%	53%	31%
Polityka bezpieczeństwa ICT w przedsiębiorstwie została zdefiniowana lub ostatnio poddana przeglądowi w ciągu ostatnich 12 miesięcy	18%	14%	30%	49%	24%

Polityka bezpieczeństwa ICT w przedsiębiorstwie została zdefiniowana lub poddana ostatniemu przeglądowi ponad 12 miesięcy i do 24 miesięcy temu	4%	3%	7%	12%	6%
Polityka bezpieczeństwa ICT przedsiębiorstwa została zdefiniowana lub ostatnio przeglądana ponad 24 miesiące temu	2%	1%	3%	5%	2%
Polityka bezpieczeństwa ICT przedsiębiorstwa została zdefiniowana lub ostatnio przeglądana w ciągu ostatnich 24 miesięcy	22%	17%	37%	61%	30%
Przedsiębiorstwa posiadają dokumenty dotyczące środków, praktyk lub procedur w zakresie bezpieczeństwa ICT	23%	18%	40%	66%	33%
Dokumenty dotyczące środków, praktyk lub procedur w zakresie bezpieczeństwa TIK, dotyczy: zarządzania prawami dostępu do korzystania z TIK	17%	12%	34%	61%	30%
Dokumenty dotyczące środków, praktyk lub procedur z zakresu bezpieczeństwa TIK dotyczy: przechowywania, ochrony, dostępu lub przetwarzania danych	22%	17%	39%	64%	31%

Dokumenty dotyczące środków, praktyk lub procedur w zakresie bezpieczeństwa TIK: procedury lub zasady zapobiegania incydentom bezpieczeństwa lub reagowania na takie incydenty	16%	12%	29%	53%	24%
Dokumenty dotyczące środków, praktyk lub procedur z zakresu bezpieczeństwa TIK, dotyczy: odpowiedzialności, praw i obowiązków osób zatrudnionych w dziedzinie TIK	20%	15%	35%	60%	28%
Dokumenty dotyczące środków, praktyk lub procedur w zakresie bezpieczeństwa ICT dotyczy: szkolenia osób zatrudnionych w zakresie bezpiecznego korzystania z ICT	16%	12%	28%	50%	22%
Polityka bezpieczeństwa TIK uwzględniła ryzyko zniszczenia lub uszkodzenia danych w wyniku ataku lub nieoczekiwanego zdarzenia (2015)	12%	8%	26%	49%	28%
Polityka bezpieczeństwa ICT uwzględniła ryzyko ujawnienia poufnych danych w wyniku włamania, phishingu, ataków phishingowych lub przypadkowo (2015)	9%	6%	20%	38%	25%
Polityka bezpieczeństwa teleinformatycznego uwzględniła ryzyko niedostępności usług teleinformatycznych w wyniku ataku z zewnątrz (np. ataku typu Denial of Service) (2015)	9%	6%	19%	37%	22%

Polityka bezpieczeństwa teleinformatycznego uwzględniała ryzyko zniszczenia lub uszkodzenia danych, ujawnienia danych poufnych oraz niedostępności usług teleinformatycznych w wyniku ataku lub przypadkowej ingerencji (2015)	8%	5%	17%	33%	20%
Przedsiębiorstwa uświadamiają osoby zatrudnione o ich obowiązkach związanych z bezpieczeństwem ICT poprzez dobrowolne szkolenia lub wewnętrznie dostępne informacje (np. informacje)	26%	21%	43%	70%	42%
Przedsiębiorstwa uświadamiają osoby zatrudnione o ich obowiązkach w zakresie bezpieczeństwa ICT poprzez obowiązkowe szkolenia lub oglądanie obowiązkowych materiałów	32%	27%	46%	65%	22%
Przedsiębiorstwa uświadamiają osoby zatrudnione o ich obowiązkach w zakresie bezpieczeństwa ICT	49%	44%	68%	87%	61%
Działania związane z bezpieczeństwem ICT są wykonywane przez własnych pracowników	34%	29%	48%	83%	40%
Działania związane z bezpieczeństwem ICT są wykonywane przez dostawców zewnętrznych	69%	67%	76%	76%	65%

Źródło: Opracowanie własne na podstawie danych Eurostatu (Eurostat's online database, 2019), Polska, Unia Europejska – 27 państw (od 2020 r.).

Z danych wynika, że firmy generalnie zwracają uwagę na ograniczanie ryzyka związanego z wykorzystaniem nowych technologii, jednak stosowanie metod wykorzystywanych do osiągnięcia tego celu jest zróżnicowane. Poszczególne metody można pogrupować w sześć kategorii (oznaczonych kolorami w tabeli), do których należą: aktualizacja polityki bezpieczeństwa cybernetycznego firmy, stosowanie konkretnych zabezpieczeń, wdrażanie konkretnych procedur, ukierunkowanie polityki bezpieczeństwa, szkolenie pracowników w zakresie zagrożeń i przestrzegania procedur związanych z utrzymaniem bezpieczeństwa cybernetycznego oraz przez kogo realizowana jest polityka bezpieczeństwa firmy. Interpretacja danych przedstawionych w tabeli prowadzi do kilku wniosków. Jeśli chodzi o firmy posiadające formalnie zdefiniowaną politykę bezpieczeństwa teleinformatycznego, to według stanu na 2015 r. wskaźnik wynosi 13%. Widoczna jest wyraźna dysproporcja pomiędzy podmiotami dużymi (73%), średnimi (28%) i małymi (9%). Jest ona również znacznie częściej przeglądana i weryfikowana w dużych firmach. Jakielwiek zabezpieczenia stosuje 87% przedsiębiorstw, odpowiednio: 99% dużych 96% średnich i 85% małych firm. Najczęściej stosowane zabezpieczenia to utrzymanie aktualnego oprogramowania (81% wszystkich przedsiębiorstw), a także silne uwierzytelnianie hasłem (76%) oraz tworzenie kopii zapasowych danych w oddzielnej lokalizacji, w tym w chmurze (57% wszystkich przedsiębiorstw). Dla 61% przedsiębiorstw ważna jest kwestia kontroli dostępu do sieci. Dane sugerują, że firmy przywiązują mniejszą wagę do tego, aby dokumenty i związane z nimi procedury były na bieżąco aktualizowane w celu zapobiegania incydentom bezpieczeństwa lub reagowania na zagrożenia. Jedynie 18% wszystkich firm zadeklarowało, że kwestie te są dla nich ważne, przy czym duże firmy przywiązują do tych zagadnień największą wagę (49%). Jeśli chodzi o politykę bezpieczeństwa realizowaną w poszczególnych firmach w niewielkim stopniu, w 12% wszystkich firm dotyczy ona ryzyka zniszczenia lub uszkodzenia danych w wyniku ataku lub niespodziewanego zdarzenia. Tylko 9% badanych podmiotów odnosi swoją politykę bezpieczeństwa do ryzyka ujawnienia poufnych danych w wyniku ataków hakerskich, phishingowych i phishingowych. Uświadamianie i szkolenie pracowników w zakresie zagrożeń oraz przestrzegania procedur związanych z cyberbezpieczeństwem koncentruje się na uświadamianiu pracowników i ich odpowiedzialności za bezpieczeństwo teleinformatyczne. Takie działania podjęło 49% firm, z czego 87% dużych, 68% średnich i 44% małych. Jeśli chodzi o działania wykonywane w związku z bezpieczeństwem teleinformatycznym,

to 83% dużych firm wykonuje je z własnymi pracownikami, 76% firm średnich i 67% firm małych zleca te zadania podmiotom zewnętrznym. Porównując intensywność stosowania poszczególnych środków bezpieczeństwa we wszystkich polskich przedsiębiorstwach ze średnią UE, dostrzegamy, iż zasadniczo nie odbiega ona znacząco, choć w niektórych przypadkach jest niższa o kilka procent. W zakresie formalnie zdefiniowanej polityki bezpieczeństwa wartość wskaźnika jest dużo niższa – 13% PL, 31% UE. W zakresie posiadanych przez przedsiębiorstwa dokumentów dotyczących środków, praktyk lub procedur bezpieczeństwa ICT różnica jest dość duża na minus dla rodzimych firm – 23% PL, 33% UE. Polskie przedsiębiorstwa mają na tle średniej unijnej dość duże braki w polityce bezpieczeństwa ICT w zakresie uwzględnienia ryzyka ujawnienia poufnych danych w wyniku włamania, pharmingu, ataków phishingowych lub przez przypadek – 9% PL, 25% UE. W kwestii posiadania przez przedsiębiorstwa zdefiniowanej polityki bezpieczeństwa średnia europejska wynosi 31%, w Polsce wskaźnik kształtuje się na poziomie 13%. W zakresie uświadamiania pracowników o ich obowiązkach związanych z bezpieczeństwem ICT poprzez dobrowolne szkolenia lub wewnętrznie dostępne informacje wskaźnik jest niższy (26%) od średniego unijnego (42%), natomiast obowiązkowe szkolenia odbywają się częściej, średnio u 32% firm, w UE średnia ta wynosi 22%. Oczywiście przyglądając się danym z poszczególnych krajów Unii Europejskiej, wyraźnie można dostrzec, że są kraje, w których zaawansowanie w stosowaniu narzędzi występuje na wysokim poziomie, należą do nich: Finlandia, Dania, Niemcy, Belgia. Kraje o niskim stopniu zaawansowania w tej materii to: Rumunia, Bułgaria, Grecja, Węgry.

Dane zawarte w najnowszym Raporcie KPMG Barometr Bezpieczeństwa dostarczają istotnych informacji o źródłach cyberzagrożeń i cyberzagrozeniach stanowiących największe ryzyko dla organizacji, liczbie zarejestrowanych przez firmy incydentów cyberbezpieczeństwa. W kontekście tych danych należy przywrócić się temu, jak firmy oceniają dojrzałość poszczególnych obszarów zabezpieczeń, w jakie obszary planują zainwestować w przyszłości oraz co ogranicza możliwość osiągnięcia odpowiedniego poziomu zabezpieczeń. Tabela 2 prezentuje grupy, które stanowią realne zagrożenie dla organizacji.

Tabela nr 2. Grupy stanowiące realne zagrożenie dla organizacji

		2019	2020	2021
Cyberprzestępczość		96%	90%	85%
	Pojedynczy hakerzy	84%	72%	57%
	Zorganizowane grupy cyberprzestępcze	58%	43%	54%
	Cyberterroryści	54%	43%	18%
	Tzw. skryptowe dzieciaki (ang. <i>Script kiddies</i>)	34%	36%	19%
	Haktywiści	27%	21%	12%
Niezadowoleni lub podkupieni pracownicy		57%	58%	39%
Grupy wspierane przez inne państwa		28%	24%	19%
Inne		0%	1%	0%

Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

Szeroko rozumiana cyberprzestępczość stanowi największe zagrożenie w opinii firm. Zauważalny jest spadek procentowy pomiędzy rokiem 2019 a 2021, w którym to zdaniem ankietowanych stanowiły one 85% wśród wszystkich grup stanowiących zagrożenie. Największe niebezpieczeństwo stanowią w dalszym ciągu pojedynczy hakerzy (57%) oraz zorganizowane grupy przestępcze (54%). Do cyberzagrożeń zidentyfikowanych w badaniu, niosących największe ryzyko dla firm, należą: wycieki danych za pośrednictwem złośliwego oprogramowania (malware), kradzież danych przez pracowników, ataki typu odmowa usługi, wyłudzenie danych uwierzytelniających (phishing), wyciek danych w wyniku kradzieży lub zgubienia nośników lub urządzeń mobilnych, kradzież danych na skutek naruszenia bezpieczeństwa fizycznego. Tabela 3 prezentuje cyberzagrożenia stanowiące ryzyko dla organizacji, zaprezentowane w skali od 0 do 5 (gdzie 0 to brak zagrożenia, 5 najwyższe ryzyko).

Tabela nr 3. Cyberzagrożenia stanowiące największe ryzyko dla organizacji

	0	1	2	3	4	5
Wycieki danych za pośrednictwem złośliwego oprogramowania (malware)	13%	19%	15%	21%	24%	8%

Wyludzanie danych uwierzytelniających (phishing)	16%	19%	17%	22%	16%	10%
Ogólne kampanie ransomware	15%	21%	20%	20%	16%	8%
Wyciek danych w wyniku kradzieży lub zgubienia nośników lub urządzeń mobilnych	12%	26%	22%	13%	17%	10%
Kradzież danych przez pracowników	21%	19%	18%	17%	14%	12%
Podśluchiwanie ruchu i ataki Man-in-the-Middle (MitM)	16%	21%	20%	18%	22%	3%
Ataki typu odmowa usługi (DoS/DDoS)	26%	18%	14%	14%	15%	13%
Kradzież danych na skutek naruszenia bezpieczeństwa fizycznego	19%	24%	16%	17%	14%	10%
Zaawansowane ukierunkowane ataki (tzw. Advanced Persistent Threat – APT)	23%	18%	13%	25%	13%	8%
Ataki na sieci bezprzewodowe	21%	20%	14%	26%	12%	7%
Ataki wykorzystujące błędy w aplikacjach	22%	21%	16%	22%	12%	7%
Włamania do urządzeń mobilnych	22%	22%	25%	11%	13%	7%

Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

W tabeli 4 zaprezentowano liczbę zarejestrowanych cyberataków. W 2020 r. 64% firm objętych badaniem zarejestrowało incydent polegający na naruszeniu bezpieczeństwa. W porównaniu z rokiem 2019 zwiększyła się ich liczba. Zdecydowanie mniej przedsiębiorstw nie zaobserwowało w 2020 r. żadnego ataku.

Tabela nr 4. Liczba zarejestrowanych przez firmy incydentów bezpieczeństwa

	2019	2020
0	46%	36%
1-3	29%	26%
4-9	14%	23%
10-29	6%	11%
30 i więcej	5%	4%

Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

Jak polskie firmy aktualnie oceniają dojrzałość poszczególnych obszarów zabezpieczeń? Tabela 5 zawiera takie zestawienie (0 – brak zabezpieczeń, 5 – pełna dojrzałość). Najwyższy poziom w badanych podmiotach osiągnęły zabezpieczenia na styku z siecią internetową, posiadana ochrona przed złośliwym oprogramowaniem, zapewnienie ciągłości działania, reagowanie na incydenty bezpieczeństwa oraz zarządzanie tożsamością i dostępem. Słabe punkty to poziom zabezpieczeń w obszarach zarządzania podatnościami, klasyfikacja i kontrola aktywów oraz bezpieczeństwo w procesach wytwarzania oprogramowania.

Tabela nr 5. Ocena przez firmy dojrzałości poszczególnych obszarów zabezpieczeń

	0	1	2	3	4	5
Bezpieczeństwo styku z siecią Internet	1%	5%	4%	13%	42%	35%
Ochrona przed złośliwym oprogramowaniem	3%	4%	6%	10%	42%	35%
Plany zapewnienia ciągłości działania	2%	3%	7%	14%	50%	24%
Reagowanie na incydenty bezpieczeństwa	2%	4%	4%	17%	46%	27%
Zarządzanie tożsamością i dostępem	3%	2%	5%	17%	46%	27%
Bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu)	3%	2%	7%	17%	40%	31%

Monitorowanie bezpieczeństwa	2%	4%	10%	16%	35%	33%
Ochrona przed wyciekami danych (tzw. Data Leakage Prevention – DLP)	2%	5%	8%	22%	35%	28%
Zarządzanie bezpieczeństwem partnerów biznesowych	8%	7%	5%	17%	39%	24%
Zarządzanie bezpieczeństwem urządzeń mobilnych (technologie MDM)	8%	7%	9%	20%	26%	30%
Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa	4%	5%	7%	34%	35%	15%
Zarządzanie podatnościami	5%	7%	7%	30%	31%	19%
Klasyfikacja i kontrola aktywów	11%	2%	10%	20%	37%	20%
Bezpieczeństwo w procesach wytwarzania oprogramowania	17%	3%	11%	15%	33%	21%

Źródło: Opracowanie własne na podstawie Barometru Cyberbezpieczeństwa 2021.

Idąc krok dalej, w tabeli 6 zaprezentowano obszary, w które firmy zamierzają inwestować w najbliższym czasie. Mimo że dojrzałość na tej płaszczyźnie ochrony przed złośliwym oprogramowaniem jest wysoka, firmy dostrzegają potrzebę dalszego inwestowania. Widzą również konieczność zapewnienia bezpieczeństwa sieci wewnętrznej, ochrony przed wyciekami danych oraz reagowania na pojawiające się coraz częściej incydenty bezpieczeństwa. Choć dojrzałość z zakresu bezpieczeństwa w procesach wytwarzania oprogramowania, klasyfikacja i kontrola aktywów oraz zarządzanie bezpieczeństwem urządzeń mobilnych, w ocenie badanych podmiotów, osiągnęły najniższą dojrzałość, nie dostrzegają one potrzeby przeznaczania środków na te właśnie cele. Może dziwić fakt, że firmy nie dostrzegają dużej potrzeby przeznaczania środków na programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa, zwłaszcza że dojrzałość w tym zakresie nie jest przez nie oceniana wysoko.

Tabela nr 6. Obszary zabezpieczeń, w które firmy zamierzają inwestować (0 – brak inwestycji, 5 – znaczące inwestycje)

	0	1	2	3	4	5
Ochrona przed złośliwym oprogramowaniem	10%	15%	20%	14%	17%	24%
Bezpieczeństwo sieci wewnętrznej (segmentacja, kontrola dostępu)	12%	11%	15%	21%	24%	17%
Ochrona przed wyciekami danych (tzw. Data Leakage Prevention – DLP)	15%	12%	15%	17%	25%	16%
Reagowanie na incydenty bezpieczeństwa	15%	14%	13%	20%	22%	16%
Monitorowanie bezpieczeństwa	10%	16%	15%	23%	24%	12%
Plany zapewnienia ciągłości działania	19%	10%	15%	16%	24%	16%
Bezpieczeństwo styku z siecią Internet	17%	10%	15%	24%	22%	12%
Zarządzanie tożsamością i dostępem	15%	20%	16%	14%	21%	14%
Programy podnoszenia świadomości pracowników w zakresie bezpieczeństwa	11%	20%	18%	24%	15%	11%
Zarządzanie podatnościami	16%	16%	16%	26%	19%	7%
Zarządzanie bezpieczeństwem partnerów biznesowych	23%	15%	11%	22%	22%	7%
Zarządzanie bezpieczeństwem urządzeń mobilnych (technologie MDM)	17%	19%	16%	25%	11%	12%
Klasyfikacja i kontrola aktywów	22%	19%	15%	18%	18%	8%
Bezpieczeństwo w procesach wytwarzania oprogramowania	30%	17%	8%	20%	18%	7%

Źródło: Opracowanie własne na podstawie Barometru Cyberbezpieczeństwa 2021.

Ograniczenia, jakie dostrzegają badane podmioty w zakresie możliwości uzyskania oczekiwanego poziomu zabezpieczeń, to: trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników – tendencja rosnąca w 2020/2021 r., brak wystarczających środków – tendencja malejąca w 2021 r. w porównaniu z rokiem 2020. Można przewidywać, że w związku z planami przeznaczenia przez polski rząd środków na cyfryzację w postaci programów (np. KPO¹⁶, FENG¹⁷, FERC¹⁸), w tym na poprawę bezpieczeństwa cyfrowego, firmy będą w stanie doinwestować wymagane obszary.

Tabela nr 7. Najważniejsze ograniczenia w możliwości uzyskania oczekiwanego poziomu zabezpieczeń

	2020	2021
Trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników	43%	60%
Brak wystarczających budżetów	64%	42%
Brak dobrze zdefiniowanych mierników	37%	25%
Brak wsparcia najwyższego kierownictwa	32%	24%
Brak zaangażowania biznesu	32%	22%
Brak właściwego przypisania odpowiedzialności w zakresie bezpieczeństwa	24%	20%

Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

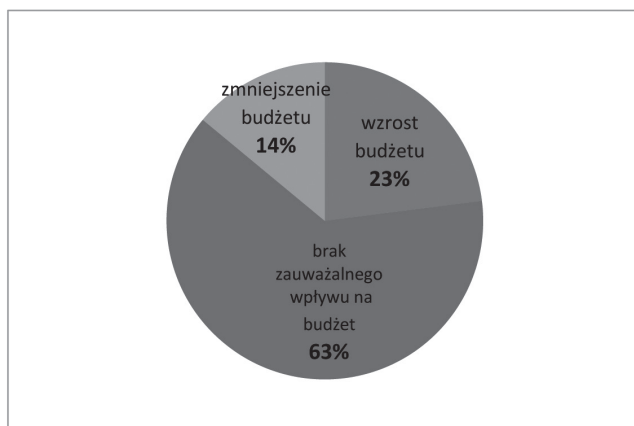
W jaki sposób pandemia wpłynęła na poziom środków przeznaczanych na działania związane z zapewnieniem bezpieczeństwa cyfrowego? W 23% badanych podmiotów zwiększono budżet na cyberbezpieczeństwo, a wzrost o 10% i więcej odnotowało 22% z nich. W 14% przypadków środki finansowe w tym obszarze zostały zmniejszone. Zdecydowana większość badanych firm (63%) nie zwiększyła budżetu na ten cel.

¹⁶ Krajowy Plan Odbudowy.

¹⁷ Fundusze Europejskie dla Nowoczesnej Gospodarki.

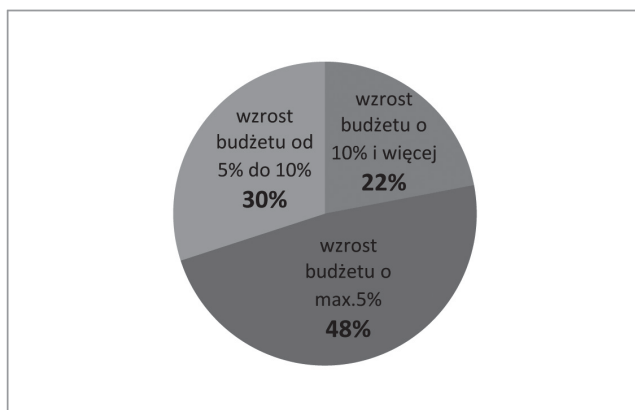
¹⁸ Fundusze Europejskie na Rozwój Cyfrowy.

Wykres nr 1. Wpływ COVID-19 na budżet w zakresie cyberbezpieczeństwa



Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

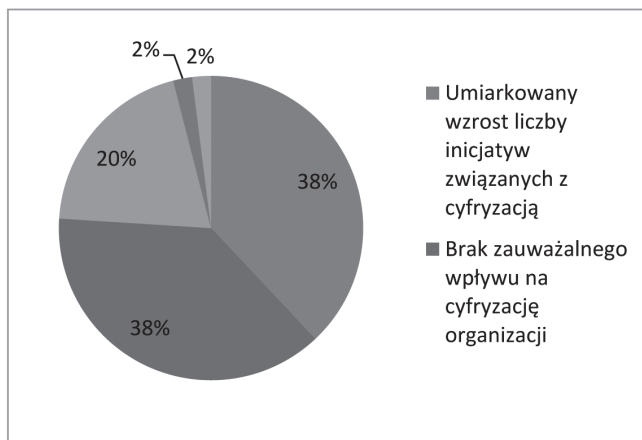
Wykres nr 2. Poziom wzrostu budżetu



Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

Pandemia wywarła wpływ na aktywność przedsiębiorców w działaniach ogólnie związanych z cyfryzacją. Dwadzieścia procent firm znacząco zwiększyło liczbę cyfrowych inicjatyw. Autorzy raportu zauważają, że więcej tego typu inicjatyw podjęły średnie i mniejsze firmy, zatrudniające do 250 pracowników, co może oznaczać, że były one nieco gorzej przygotowane do warunków pracy w trybie zdalnym oraz na potrzebę zmiany dotychczasowych modeli biznesowych.

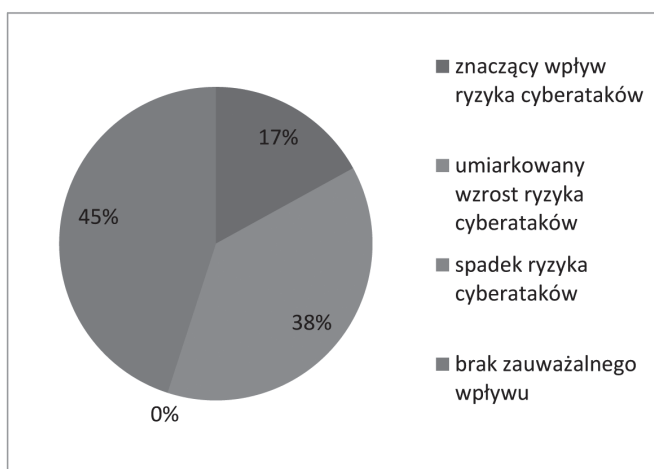
Wykres nr 3. Wpływ pandemii COVID-19 na działania związane z cyfryzacją organizacji



Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

Ponad połowa przedsiębiorców zauważa, że pandemia przyczyniła się do wzrostu ryzyka występowania cyberataków, 45% respondentów nie dostrzega żadnego ryzyka. Większość mniejszych firm zauważa niebezpieczeństwo, ale również duże firmy (50%), zatrudniające powyżej 250 pracowników, dostrzegają wzrastające ryzyko cyberataków.

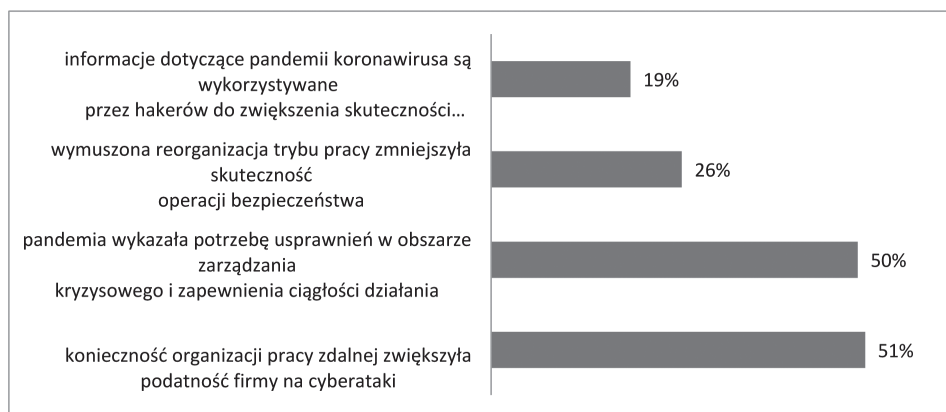
Wykres nr 4. Ocena wpływu pandemii COVID-19 na bezpieczeństwo cyfrowe



Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

W następstwie zmiany organizacji pracy i pojawiających się w związku z tym zagrożeń i zmniejszenia skuteczności operacji bezpieczeństwa, przedsiębiorstwa zmuszone zostały do wprowadzenia usprawnień w obszarze zarządzania kryzysowego i zapewnienia ciągłości działania, tym bardziej że hakerzy skrupulatnie wykorzystują „pojawiające się możliwości”. Wykres 5 prezentuje obserwacje firm w odniesieniu do cyberbezpieczeństwa w kontekście pandemii.

Wykres nr 5. Cyberbezpieczeństwo a pandemia koronawirusa – spostrzeżenia firm



Źródło: Opracowanie własne na podstawie Barometr Cyberbezpieczeństwa 2021.

Wnioski

Przedstawienie najczęściej występujących cyberzagrożeń oraz analiza podejmowanych przez przedsiębiorstwa działań w związku z pojawiającymi się zagrożeniami w kontekście trwającej pandemii pozwala na skonstruowanie ogólnych wniosków. W jaki sposób firmy podejmują lub nie określone działania, stosują bądź nie określone narzędzia, jak były przygotowane na funkcjonowanie i jak poradziły sobie z bezpiecznym zorganizowaniem pracy w trudnych warunkach pandemicznych? Wniosek, który nasuwa się jako pierwszy w odniesieniu do wszystkich rodzajów cyberzagrożeń, to zdecydowana przewaga u dużych firm w stosowaniu narzędzi zapobiegających lub eliminujących te zagrożenia. Wynika to z faktu konieczności wdrażania określonych rozwiązań i procedur ze względu na rodzaj i wielkość przeprowadzanych operacji oraz działań, zatrudniania specjalistów z zakresu bezpieczeństwa ICT i co za tym idzie

przeznaczania na ten cel znacznych nakładów finansowych. Średnie i małe przedsiębiorstwa, zazwyczaj w związku z brakiem środków lub brakiem świadomości pojawiających się zagrożeń lub też niedoinformowaniem, znacznie rzadziej podejmują działania w kierunku zapewnienia cyberbezpieczeństwa, a tym samym stają się częstszym celem cyberprzestępców. Kolejny wniosek dla wszystkich przedsiębiorstw to brak sformułowanej polityki bezpieczeństwa teleinformatycznego. Średnio 9% małych firm deklaruje, że posiada sformalizowaną strategię działania w tym obszarze, w przypadku średnich przedsiębiorstw już 28%, zaś dużych – 53%. Wobec pojawiającego się zagrożenia naruszenia danych na dość wysokim poziomie w polskich przedsiębiorstwach, średnio 76%, kształtuje się kontrola dostępu użytkowników do urządzeń i sieci przedsiębiorstwa. Z kolei stosowanie narzędzi z zakresu przeprowadzania testów bezpieczeństwa oraz technik szyfrowania odsetek małych firm stosujących to narzędzie jest stosunkowo niski – 21%, firmy średnie – 47%, duże – 70%. W sytuacji przejścia w wielu przedsiębiorstwach na tryb pracy zdalnej, co zwiększa podatność na ataki, firmy częściej powinny kontrolować aktywności pracowników, udzielać dostępu tylko do tych zasobów IT, które pozwolą im realizować wyznaczone zadania, opracować dokumenty i wdrażać procedury w zakresie przechowywania, ochrony, dostępu lub przetwarzania danych. Tylko 17% małych firm i 39% średnich deklaruje kroki podejmowane w tym kierunku. W przypadku cyberzagrożenia w postaci ataków ransomware czy spoofing dość wysoki odsetek dużych przedsiębiorstw wykonuje kopie zapasowe danych (86% dużych, 74% średnich oraz tylko nieco więcej niż połowa małych firm). O aktualizację oprogramowania troszczy się średnio 81% podmiotów, zbyt rzadko dokonywana jest aktualizacja dokumentów zawierających procedury w przypadku zapobiegania niebezpieczeństwom oraz reagowania na nie – średnio 18% wszystkich przedsiębiorstw. Ryzyko pojawienia się niebezpiecznego incydentu w wyniku błędów popełnianych przez zatrudnionych powinno być eliminowane dzięki uświadamianiu pracowników, zwiększeniu kontroli w zakresie przestrzegania obowiązujących procedur oraz poprzez zapewnienie obowiązkowych szkoleń w zakresie bezpiecznego korzystania z ICT. Konieczne jest tutaj nadrobienie zaległości. Obowiązkowe szkolenia dla pracowników prowadzi 27% małych firm, 46% średnich oraz 65% dużych. Zdaniem ponad połowy polskich firm pandemia COVID-19 przyczyniła się do wzrostu ryzyka cyberataków. W związku z tym 23% z nich zwiększyło budżet na działania w zakresie cyberbezpieczeństwa. Konieczność przejścia na pracę zdalną spowo-

dowała, że w 58% przedsiębiorstw pandemia zwiększyła aktywność w obszarze cyfryzacji. Dużo firm przyznaje, że taki tryb pracy zwiększył niebezpieczeństwo wystąpienia cyberataków, a co za tym idzie istnieje potrzeba zintensyfikowania działań w obszarze zarządzania kryzysowego.

Podsumowanie

Sprawne działanie w zakresie zapewnienia bezpieczeństwa cyfrowego to dziś warunek skutecznego prowadzenia biznesu. Każda firma może stać się celem ataku, a żadne zabezpieczenia nie zapewniają całkowitego bezpieczeństwa. Zrównoważona i dostosowana do celów przedsiębiorstwa strategia cyberbezpieczeństwa niewątpliwie jest narzędziem, które wspiera skuteczne działania firm, a tym samym wprowadza równowagę między ograniczeniem ryzyka i wprowadzaniem innowacji biznesowych. Narzędzia i metody, które były stosowane w obrębie przedsiębiorstwa, aktualnie często wychodzą poza jego zasięg. Analiza zagrożeń uświadamia, jak wiele z nich skierowanych jest właśnie w kierunku często nieświadomych użytkowników, dlatego tak istotne jest, aby pracownicy mieli świadomość tych zagrożeń, stosowali określone procedury, co w ostateczności umożliwi im bezpieczną i wydajną pracę. Dla dobra firmy oraz konsumenta konieczne jest również znalezienie równowagi pomiędzy ochroną i obsługą klienta. Przedsiębiorstwo wprowadzając odpowiednie narzędzia zapewniające cyberbezpieczeństwo, buduje zaufanie wśród swoich klientów. To zaufanie może przekładać się na uzyskanie przewagi konkurencyjnej. Nie ma wątpliwości, że transformacja cyfrowa przyczynia się do budowania modeli biznesowych, dzięki którym firma zdobywa klienta i buduje przewagę konkurencyjną a cyberbezpieczeństwo wspiera w dużym stopniu te działania. Pandemia zdecydowanie przyczyniła się do wzrostu tempa wprowadzania rozwiązań cyfrowych w wielu polskich przedsiębiorstwach – digitalizacja dokumentów, elektroniczny obieg faktur czy umów, korzystanie z chmury obliczeniowej, automatyzacja procesów biznesowych, e-sprzedaż to tylko niektóre z nich. W ślad za tymi zmianami musi iść świadomość pojawiających się zagrożeń i podejmowanie adekwatnych działań w tym obszarze. Zdecydowanie pozytywnym następstwem będą środki finansowe, które zostaną przeznaczone na cyfryzację w ramach funduszy europejskich, a co za tym idzie na prewencyjne działania w zakresie cyberbezpieczeństwa.

Bibliografia

- Academic Advisers National University of Singapore, Oxford Martin School, University of Oxford, Wharton Risk Management and Decision Processes Center, University of Pennsylvania, *Global Risks Report 2021 16th Edition*, World Economic Forum In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 2021.
- Adams A., Sasse M.A., *Users are not the enemy*, „Communications of the ACM”, 1999.
- Allianz Global Corporate & Specialty SE, *Identifying the major business risks for 2021*, „Allianz Risk Barometer”, 2021.
- Caracelli J., Jones N., *Cyber Security*, „Threats and Responses for Government and Business”, Praeger, 2019.
- CoveWare, *The Coveware Quarterly Ransomware Report 2020*, <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>.
- Eurostat, „Security policy: measures, risks and staff awareness”, https://c.europa.eu/eurostat/databrowser/view/ISOC_CISCE_RA__custom_661041/default/table?lang=en.
- Fujitsu, *Five key actions to empower secure digital transformation*, <https://www.fujitsu.com/global/services/security/insights/digital-transformation/#5keyactions>.
- Hadlington L., *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*, Heliyon, 2017.
- KPMG Advisory spółka z o.o., *Barometr Cyberbezpieczeństwa. Covid 19 przyspiesza cyfryzację firm*, 2021.
- PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.
- Polskie Centrum Badań i Certyfikacji, <https://www.pcbc.gov.pl/pl/uslugi/certyfikacja-systemow-zarzadzania/pn-iso-iec-27001>.
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, <https://sap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf>.
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20050640565/U/D20050565Lj.pdf>.

ICT security in Polish enterprises in the light of the COVID-19 pandemic

Abstract: Digital transformation blazes paths for the future, driving business units to rapidly adopt new digital technologies. The purpose of this study is to identify the risk of business digitization in the context of the COVID-19 pandemic by analysing the actions taken by Polish entrepreneurs to ensure cybersecurity in relation to threats appearing in the cyber environment. For the purposes of the analysis, data from the Eurostat online database were used—a Community study on the use of ICT and e-commerce in enterprises—security policy: measures, threats and awareness of personnel and the KPMG Cybersecurity Barometer 2021 Report. Data analysis allows to diagnose the degree to which small, medium and large Polish enterprises implement tools limiting the risk of security incidents, especially since for many the change of business models and the need to use digital solutions has become a necessity in today's reality. Conclusions from the analysis may inspire company managers in terms of the need to take specific actions in connection with emerging cyber threats.

Key words: cybersecurity, cyber threats, digitization, ICT security, COVID-19 pandemic

dr Joanna Grubicka

Akademia Pomorska w Słupsku
Instytut Bezpieczeństwa i Zarządzania
Katedra Bezpieczeństwa Narodowego
e-mail: joanna.grubicka@apsl.edu.pl
ORCID: 0000-0001-7934-6044

Rozdział 2

Bezpieczeństwo cyfrowe organizacji w dobie pandemii COVID-19

Streszczenie: Pandemia COVID-19 spowodowała największe zakłócenia w funkcjonowaniu organizacji od czasu II wojny światowej, a jej implikacje dla cyberbezpieczeństwa systemów sterowania są większe, niż ktokolwiek mógł przewidzieć. Publikacja bazuje na aktualnych badaniach z zakresu cyberbezpieczeństwa przeprowadzonych w okresie pandemii COVID-19. Autorka zwróciła w niej uwagę na konieczność prowadzenia działań przybierających formę trzypunktowej strategii, zawierającej rozwiązania technologiczne, organizacyjne oraz kompetencje pracowników, która umożliwia wypełnienie luki w systemach bezpieczeństwa cyfrowego, zwłaszcza w warunkach COVID-19.

Słowa kluczowe: bezpieczeństwo cyfrowe, organizacja, zagrożenia, cyberbezpieczeństwo

Wprowadzenie

Epidemia koronawirusa jest jednym z tych wstrząsów, które stymulują tempo zmian procesów gospodarczych. Przez ostatnie 15–20 lat systemy sterowania powoli ewoluowały w kierunku rozwiązań zintegrowanych z całym systemem produkcyjnym. I pewnie rozwój ten w dalszym ciągu powoli postępowałby naprzód, gdyby nie pandemia COVID-19. W ciągu 4–6 tygodni zdalne zarządzanie zakładami produkcyjnymi stało się koniecznością. Aby bezpiecznie kontynuować działalność, należało zredukować do minimum liczbę personelu pracującą na miejscu, a także odłożyć w czasie lub realizować zdalnie zadania z zakresu cyberbezpieczeństwa. Drastyczne ograniczenie możliwości podróży i przebywania na terenie obiektów przemysłowych spowodowało, że w ciągu zaledwie sześciu miesięcy poczyniono większe postępy w zakresie zdalnego dostępu do zasobów niż przez ostatnie lata. Spowodowało to natychmiastowy wzrost okazji i cyberataków zarówno na organizacje, jak i na osoby prywatne. Celem rozdziału jest zatem wskazanie różnych aspektów zapewnienia cyberbezpieczeństwa organizacji w warunkach pandemii koronawirusa, jak i po niej.

Bezpieczeństwo cyfrowe organizacji

Subdyscyplina nauk o bezpieczeństwie, jaką jest „bezpieczeństwo cyfrowe”, w ogólnym zarysie ma na celu poprawę zrozumienia tego, jakie aspekty przedmiotowe i podmiotowe systemu informatycznego wykorzystywanego przez danych użytkowników tworzą sfery potencjalnych zagrożeń dla potencjalnego nieetycznego ich wykorzystania. W swoich założeniach klasyczna nauka o cyberbezpieczeństwie ma dostarczać nie tylko prognoz, kiedy potencjalne ataki na system informatyczny mogą się powieść, ale także ujawniać ich przyczynę i spodziewane efekty oraz wskazywać opcje zabezpieczeń¹.

Za każdym razem, kiedy poprawia się system jako całość, wpływa się na wszystkie jego elementy jednocześnie. Zwiększa to skuteczność osiągnięcia zamierzonego efektu zmiany. Dlatego nowoczesne koncepcje zarządzania skupiają się na koordynowaniu połączeń i relacji pomiędzy ogniwami, zamiast kontroli

¹ National Academies of Sciences, Engineering, and Medicine. 2017. Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions. Washington, DC: The National Academies Press. <https://doi.org/10.17226/24676>.

zachowań jednostek. Dotychczasowe papierowe środowisko różnego rodzaju dokumentów, faktur, pism, wniosków, podań czy umów można zastąpić już cyfrowymi formularzami i automatycznymi przepływami pracy. Dokumenty podpisuje się elektronicznym podpisem kwalifikowanym, a inteligentne OCR+AI, inaczej optyczne rozpoznawanie tekstu (z ang. *Optical Character Recognition*) plus sztuczna inteligencja (ang. *Artificial Intelligence*), wspiera użytkownika w automatyzacji pracy, którą może wykonać w biurze lub w domu. Cyfryzacja ma kluczowe znaczenie dla przetwarzania, przechowywania i transmisji danych, ponieważ „umożliwia przenoszenie wszelkiego rodzaju informacji we wszystkich formatach z taką samą wydajnością, a także ich przenikanie”². Dane cyfrowe mogą być łatwiej udostępniane, w łatwiejszy i szybszy sposób można do nich dotrzeć, wykorzystać je i udostępniać praktycznie w sposób nieograniczony. Nie dziwi zatem fakt, że organizacje na całym świecie preferują ten właśnie sposób przechowywania informacji.

Kontekst ciągłych zmian biznesu i ewolucji nowoczesnych technologii wywarł jednak znaczący wpływ na to, co dotąd nazywano „cyberbezpieczeństwem” (ang. *cyber security*)³ i spowodował, iż powoli zastępuje się go terminem o szerszym zakresie, jakim jest „bezpieczeństwo cyfrowe” (ang. *digital security*). „Bezpieczeństwo cyfrowe” („bezpieczeństwo w środowisku cyfrowym”) zazwyczaj rozumiane jest jako bezpieczeństwo informacyjne, „[...] jako element systemu informatycznego [...], jako synonim bezpieczeństwa komputerowego, telekomunikacyjnego, czy bezpieczeństwa sieciowego”⁴. Bezpieczeństwo cyfrowe ma na celu zapewnianie bezpiecznej aktywności różnego rodzaju podmiotów w środowisku cyfrowym oraz przeciwdziałanie zagrożeniom odnoszącym się do bezpieczeństwa sieci, serwerów, danych na urządzeniach itp. Ten ogólny opis zakresu bezpieczeństwa cyfrowego w istocie zawiera postulat posiadania odpowiedniej wiedzy, umiejętności i postaw użytkowników urządzeń i narzędzi komputerowych, informatycznych czy sieciowych. Należy więc ujmować bezpieczeństwo cyfrowe w szerokiej perspektywie koncepcyjnych ram kompetencji użytkowników cyfrowych systemów. Ułatwia to dobrze rozwinięty system pojęciowy i operacyjny dotyczący priorytetu rozwoju i promocji nowoczesnych

² D. McQuail, *McQuail's Mass Communication Theory* (czwarte wydanie), Sage, Londyn 2000, s. 16–34.

³ Zob. C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 27–33.

⁴ L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego*, „Zeszyty Naukowe” 2014, nr 2(10), s. 212.

kompetencji cyfrowych obecnych i przyszłych użytkowników tych systemów, zawarty w strategicznych dokumentach rozwoju instytucji globalnych, regionalnych czy krajowych.

Dla nowoczesnych organizacji wykorzystujących cyberprzestrzeń i wymiar bezpieczeństwa określa się tzw. organizacyjną przestrzeń bezpieczeństwa, która powoduje istotne zmiany społeczno-kulturowe, gospodarcze i polityczne. Zmiany te stwarzają nowe możliwości, ale także wyzwania i obawy dla ludzkich zbiorowości. Cyberbezpieczeństwo jest krytyczną częścią biznesu cyfrowego, z jego szerokim i nowym ekosystemem zewnętrznym, które staje się wyzwaniem w cyfrowym świecie. Gdy organizacje przechodzą na biznes cyfrowy, zagadnienie cyberbezpieczeństwa musi zająć się brakiem własnej infrastruktury i dominacją usług funkcjonujących poza własnym systemem IT. Bezpieczeństwo staje się problemem na przecięciu technologii i świata fizycznego – IT/technologie operacyjne (OT)/Internet rzeczy (IoT).

Można wyodrębnić kilka aspektów efektywnego podejścia do tematyki bezpieczeństwa cybernetycznego w przedsiębiorstwach produkcyjnych. Dużą rolę odgrywa tu kwestia zapewnienia widoczności wszystkich elementów występujących w systemach. Integracji OT i IT towarzyszy bowiem pojawienie się wielu nowych urządzeń i sterowników, podłączonych bezpośrednio do systemu produkcyjnego. Mowa tu przede wszystkim o wykorzystaniu czujników IoT do kontroli i analizy danych z maszyn produkcyjnych, które badają parametry środowiska ich pracy. Dzięki IoT przedsiębiorstwa zyskują chociażby możliwość analizy predykcyjnej stanu maszyn, mogą efektywniej planować wydajność produkcji, jej jakość, przestoje, konserwację urządzeń. Jednak z racji specyfiki sensorów IoT (np. podatności na przejęcie kontroli dostępu) wystawiają się na potencjalne ryzyko ataku hakerskiego. Wiele przedsiębiorstw ma podstawowy problem z urządzeniami i sensorami IoT. Po prostu nie są w stanie zidentyfikować wszystkich swoich urządzeń podłączonych do sieci. Tempo biznesu zwiększa prędkości algorytmiczne, ponieważ algorytmy zastępują interwencję człowieka w podejmowaniu decyzji biznesowych. Zagrożenia bezpieczeństwa cyfrowego, realne czy potencjalne, stanowią wyzwanie dla organizacji.

Badanie bezpieczeństwa cyfrowego i ich uwarunkowań w organizacjach różnego typu są niezwykle potrzebne i ważne, zwłaszcza w kontekście nowej ery zachowań organizacyjnych w związku z kryzysem wywołanym zagrożeniem epidemiologicznym COVID-19.

Bezpieczeństwo personalne w cyberprzestrzeni a bezpieczeństwo cyfrowe organizacji

Bezpieczeństwo personalne w obliczu bezpieczeństwa cyfrowego organizacji jest ujmowane jako zjawisko, które można, a wręcz należy analizować jako jeden z wymiarów bezpieczeństwa. Nurt ten jest stale mało rozpoznany, ale wydaje się niezmiernie ważny w kontekście obecnie rozwijanej gospodarki cyfrowej i towarzyszących jej wyzwań. Z dnia na dzień rośnie zapotrzebowanie na nowe aplikacje, które wspierają przedsiębiorstwa i organizacje w cyfrowej transformacji, automatyzacji procesów biznesowych i rozwiązywaniu bieżących problemów. W praktyce jest niemal niemożliwe, by dokonać analizy zagrożeń w obszarze bezpieczeństwa strukturalnego bez ingerencji w aspekt personalny. Bezpieczeństwo organizacji jest tożsame z bezpieczeństwem w sferze personalnej (pracownicy, właściciele, dostawcy, klienci itp.), gdyż głównym podmiotem, reprezentującym różne kategorie interesariuszy indywidualnych i zbiorowych na terenie danej organizacji, jest człowiek⁵. „Wszelkie rozważania prowadzone na temat bezpieczeństwa mają głęboki sens tylko wówczas, jeśli dotyczą one człowieka i wielkości relacji, jakie są tu właściwe w kategorii jednostkowej, społecznej, instytucjonalnej i globalnej”⁶. Człowiek, jako istota społeczna i zarazem jednostka większej zbiorowości ludzkiej, z reguły dąży do samorozwoju. Jednak w sytuacji braku bezpieczeństwa, koncentrować się będzie głównie na zaspokajaniu potrzeb związanych z przetrwaniem.

Pandemia COVID-19 sprawiła, że większość ludzi na świecie przeszła na system pracy zdalnej, z reguły w domu, stąd też technologia cyfrowa stała się istotną przysłowiową „deską ratunkową”. Ta nagła zależność od pracy zdalnej otworzyła jednak zupełnie nowy asortyment zagrożeń bezpieczeństwa i prywatności. Praca zdalna stanowi wyjątkowe wyzwanie dla bezpieczeństwa informacji, ponieważ środowiska pracy zdalnej zwykle nie mają takich samych zabezpieczeń, jak w biurze. W świetle tych zmian istotne jest, aby narzędzia, na których opiera się komunikacja wrażliwa i o wysokim ryzyku, zostały poddane dokładnej kontroli. Bezpieczeństwo cyfrowe podczas pracy zdalnej sprowadza się do wielu zasad. Oprócz wyżej wymienionych należy do nich:

⁵ A. Urbanek, *Pojęcie, istota i klasyfikowanie patologii społecznych*, w: *Patologie społeczne – wymiar personalny i strukturalny*, A. Urbanek, J. Grubicka, D. Zbroszczyk (red.), Słupsk 2021.

⁶ W. Pokruszyński, *Filozofia bezpieczeństwa*, Wydawnictwo Wyższej Szkoły Gospodarki Euro-regionalnej, Józefów 2013, s. 121.

- unikanie publicznego Wi-Fi. Jeśli to konieczne, należy użyć osobistych hotspotów lub innego sposobu szyfrowania połączenia internetowego;
- w przypadku wielu aplikacji do zdalnego dostępu powinno się używać sieci VPN. Sieci VPN zapewniają bezpieczne łączenie się z różnymi usługami cyfrowymi (strony internetowe, poczta e-mail, serwer SQL itp.).

Choć przestępstwa z wykorzystaniem skradzionej tożsamości mają miejsce najczęściej w internecie, to sam proces kradzieży tożsamości nie zawsze się tam odbywa. Generalnie tożsamość jest kradziona w celu popełnienia innych przestępstw. Można ją wykorzystać do popełnienia oszustwa, odsprzedaży innym osobom lub organizacjom, które planują dopuścić się oszustwa, do sfabrykowania aktów urodzenia, prawa jazdy lub na przykład paszportu. Można też posłużyć się nią w celu uzyskania dostępu do niektórych miejsc w internecie. Ofiara może nawet nie wiedzieć, że ktoś używa jej nazwiska. Najczęściej sprawa nie zostaje wykryta aż do momentu, gdy otrzymuje wyciąg z banku lub gdy ktoś nie zacznie się dopominać zapłaty za usługi i towary, których dana osoba nie zamawiała. Nawet jeśli ureguluje te opłaty, wkrótce pojawiają się nowe. W międzyczasie może starać się o przyznanie kredytu lub kupić na przykład samochód przy pomocy karty kredytowej, a wtedy okazuje się, że kredytu nie otrzyma, a za wszystko trzeba płacić gotówką. Dodatkowo osoba poszkodowana ponosi straty moralne i jest traktowana jak oszust.

Bardzo często zdarza się, że przestępca na podstawie zdobytych wcześniej informacji o danej osobie, takich jak: imię i nazwisko, data urodzenia, adres czy też nazwisko rodowe matki otwiera nowe konto bankowe. Tego typu informacje mogą być uzyskane z danych dostępnych w internecie, od firm przechwytyjących je za pomocą „ciasteczek”, a także na przykład w koszach na śmieci. Zdarza się, że przestępca dokonuje przejęcia konta bankowego swojej ofiary. Do przejęcia konta potrzebne są przestępcy pewne dane osobowe, które może uzyskać na kilka sposobów:

- wykorzystując istniejące chat-roomy. Przestępca umieszcza na oficjalnej liście z informacjami o chat-roomach odniesienie do witryny, gdzie można porozmawiać na dany temat. Jest nią faktycznie strona, na której osoby są proszone o wypełnienie formularza. Znajdują się w nim pytania, na które odpowiedzi dadzą oszustowi wszystkie potrzebne informacje do popełnienia przestępstwa. Graficznie strona ta wygląda jak oryginalny chat-room i dlatego łatwo wprowadzić inne osoby w błąd;

- kopiując stronę sprzedawcy lub dostawcy usług. Jest to metoda podobna do opisanej wyżej, jednakże tym razem przestępca tworzy stronę bliźniaczo podobną do istniejącej już oryginalnej strony. Przestępca zbiera zamówienia, potwierdza je i uzyskuje przelew, ale nigdy nie realizuje zamówienia;
- tworząc strony zwykle o treściach pornograficznych, za korzystanie z których nie płaci się, ale warunkiem koniecznym jest przedstawienie karty kredytowej. Taka strona pozostaje bezpłatna, ale po uzyskaniu niezbędnych informacji przestępca dokonuje zakupów na innych stronach.

Najczęściej popełnianymi przestępstwami dotyczącymi kradzieży tożsamości są oszustwa związane z transakcjami, które uderzają w tzw. e-business. Polegają one na wypełnianiu formularza zamówieniowego, ale na nazwisko innej osoby. Zasadniczą różnicą odróżniającą tego typu przestępstwo od tradycyjnie popełnianego oszustwa jest to, że w wirtualnym świecie możliwy jest atak na większą liczbę sklepów w bardzo krótkim czasie, często bezkarnie.

Technologia chmur to kolejny przykład na koncepcję, która z jednej strony przyniosła ogromną wygodę (kopie zapasowe, synchronizacja danych, rezygnacja z dużych dysków fizycznych), a z drugiej wielkie zagrożenie. Wysyłając swoje pliki na zewnętrzny serwer (czyli chmurę), nie dostajemy 100% gwarancji, że nie ma do nich dostępu (albo nie uzyska go na drodze włamania czy wycieku) ktoś niepowołany. Dlatego rozsądnym rozwiązaniem jest szyfrowanie danych przed synchronizacją. Do dyspozycji jest wiele aplikacji, m.in. DiskCryptor, TrueCrypt czy Gpg4win. Istnieją również kompletne programy do synchronizacji z chmurami, które posiadają wbudowany moduł szyfrowania, takie jak CloudFogger, który współpracuje z popularnymi dyskami sieciowymi: Google Drive, DropBox i OneDrive. Ciekawe możliwości oferuje SpiderOak – program zintegrowany z firmowym dyskiem w chmurze, oferujący wysoki poziom ochrony przesyłanych plików. Jeśli niepotrzebna jest zewnętrzna przestrzeń na dane, a pragnie się w bezpieczny sposób zsynchronizować swoje urządzenia, dobrym pomysłem jest instalacja BitTorrent Sync, opartego na technologii *peer-to-peer*.

Oprogramowanie szpiegujące jest jednym z głównych zagrożeń i ataków, które stają się powszechne i niebezpieczne w zakresie bezpieczeństwa informacji oraz komputerów. W wyniku złośliwego użycia programów szpiegujących wszyscy użytkownicy domowi i korporacyjni próbujący skorzystać z technologii komputerowych są narażeni na poważne straty. Oprócz typowych szkodliwych

programów, takich jak wirusy, robaki, trojany, backdoory, pakiety użytkowników root, dialery telefoniczne, systemy nasłuchiwania i oprogramowanie szpiegujące szeroka gama różnych złośliwych programów infekuje coraz większą liczbę użytkowników oraz organizacji. Zbiór problemów, które nazywamy „oprogramowaniem szpiegującym”, sam w sobie jest coraz bardziej różnorodny i jest szczególnym wyrazem złożoności współczesnego świata.

Termin „oprogramowanie szpiegujące”⁷ obejmuje szeroki zakres oprogramowania, które monitoruje użycie komputera bez wiedzy i zgody użytkownika. Niektóre wersje programów szpiegujących pojawiają się w wyskakujących reklamach, podczas gdy inne śledzą aktywność online, kradną hasła, a nawet przejmują kontrolę nad komputerem użytkownika⁸. „Oprogramowanie szpiegujące” często dzieli się na cztery typy oprogramowania: (1) system monitors, (2) trojany, (3) adware i (4) śledzące pliki cookie. System monitorowania stanowi poważne zagrożenie dla prywatności, ponieważ może potajemnie przechwytywać i przysyłać dane osobowe użytkownika oraz hasła wpisywane w transakcjach online. Trojany wydają się być legalnym oprogramowaniem, ale można ich używać do kradzieży poufnych informacji, instalowania złośliwych programów, przejmowania kontroli nad komputerem lub narażania na szwank dodatkowych komputerów lub sieci. Adware śledzi aktywność online użytkowników, aby wyświetlać ukierunkowane wyskakujące reklamy. Śledzące pliki cookie to małe pliki tekstowe pobierane na komputer użytkownika, które zachowują preferencje na określonych stronach internetowych. Wiele renomowanych stron internetowych używa plików cookie, ale osoby trzecie, takie jak twórcy oprogramowania reklamowego, używają plików cookie do ukierunkowanego marketingu internetowego⁹. Te kategorie programów szpiegujących nie wykluczają się wzajemnie, a różne rodzaje programów szpiegujących często dzielą podobne taktyki w zakresie instalowania i unikania wykrywania oraz usuwania. Zasadniczo oprogramowanie szpiegujące z tych czterech kategorii można zainstalować w jeden z pięciu sposobów: (1) bez wiedzy i zgody użytkownika, poprzez wykorzystanie luk w systemie operacyjnym lub przeglądarce; (2) za zgodą użytkownika wywołaną zwodniczymi lub wprowadzającymi w błąd

⁷ L. Sun, *Who Can Fix Ie Spyware Problem?*, „Berkeley Technology Law Journal” 2007, Vol. 22, s. 555.

⁸ *First do no Harm: Xe Problem of Spyware*, by ed. S.P. Crawford, „Berkeley Technology Law Journal” 2005, Vol. 20, s. 1473–1474.

⁹ Tamże, s. 556–557.

wyskakującymi komunikatami; (3) za zgodą użytkownika uzyskaną przez wprowadzające w błąd lub niewystarczające ujawnienie, co robi oprogramowanie lub jakie inne oprogramowanie zawiera; (4) za zgodą użytkownika i ujawnieniem, ale skierowane do dzieci, które mogą nie docenić szkodliwych konsekwencji instalacji; bądź (5) bez wiedzy lub zgody za pośrednictwem innego oprogramowania szpiegującego już zainstalowanego w systemie¹⁰. Po zainstalowaniu oprogramowanie szpiegujące wymyka się wykrywaniu i jest odporne na usunięcie. Większość programów szpiegujących nie jest dostarczana z oprogramowaniem do odinstalowywania i co więcej pozostawia komponenty po odinstalowaniu. Nawet po odinstalowaniu niektóre programy szpiegujące automatycznie pobierają się ponownie po ponownym uruchomieniu komputera. Oprogramowanie szpiegujące może również wyłączać wewnętrzne oprogramowanie zabezpieczające użytkowników lub stale mutować, aby uniknąć wykrycia przez konwencjonalne rozwiązania antyspyware. Większość programów szpiegujących należy do łagodniejszej kategorii oprogramowania reklamowego, które zapewnia ukierunkowane wyskakujące reklamy oparte na nawykach przeglądania internetu przez użytkowników. Bardziej złośliwy rodzaj oprogramowania szpiegującego śledzi każde naciśnięcie klawisza użytkownika i wysyła te informacje do swoich właścicieli. Informacje takie mogą być wykorzystywane do legalnych celów eksploracji danych lub mogą być wykorzystywane przez inne osoby do kradzieży tożsamości i przestępstw finansowych.

W przeciwieństwie do innych szkodliwych programów spawnowanych przez internet, takich jak wirusy komputerowe, które powodują bezpośrednie szkody w organizacjach o wartości czasem milionów dolarów, oprogramowanie szpiegujące wydaje się wywoływać bardziej łagodne reakcje użytkowników, pomimo przewidywanych tragicznych konsekwencji. Wydaje się, że wielu użytkowników akceptuje oprogramowanie szpiegujące jako cenę uzyskania *freeware* i *shareware* online lub po prostu nie zdaje sobie sprawy z jego konsekwencji. Wraz ze wzrostem zależności od sieci i niemal wszechobecną dostępnością internetu istnieje nowy paradygmat rozprzestrzeniania programów szpiegujących, wirusów i innego złośliwego oprogramowania. W rzeczywistości wiele uwagi poświęcono oprogramowaniu szpiegowskiemu w popularnej literaturze, a raporty z wielu źródeł wskazują, że oprogramowanie szpiegujące prawdopodobnie dotarło do 90% komputerów użytkowników domowych. Jednym

¹⁰ Tamże, s. 557.

z najnowocześniejszych oprogramowań szpiegujących jest obecnie Pegasus, które może zostać zainstalowane na urządzeniach działających pod kontrolą iOS (system operacyjny firmy Apple dla urządzeń mobilnych) oraz Android. Oprogramowanie umożliwia dostęp do wszystkich treści telefonu, a także do głośnika i kamery. System Pegasus zezwala także na pobieranie treści rozmów prowadzonych przez komunikatory, SMS-ów, e-maili, a także dostęp do gromadzonych w telefonie zdjęć i nagrań. Oprogramowanie szpiegujące o nazwie Pegasus to niezwykle wyrafinowana i niebezpieczna cyberbroń, która pozwala jej operatorowi na przejęcie całego smartfonu, łącznie z usługą WhatsApp¹¹.

Szpiegostwo cyfrowe przeciwko społeczeństwu obywatelskiemu, dokumentowanie filtrowania internetu oraz innych technologii i praktyk stanowią coraz częstsze przykłady zagrożeń wynikających z naruszania prywatności w sieci. Przytoczone przykłady bezprawnego analizowania danych i kontroli przepływu informacji mają ogromny wpływ na sferę zarówno naszej wolności słowa, jak i sferę prywatności. Zakres działań w internecie, a także korzystanie z popularnych aplikacji oraz badanie mechanizmów przejrzystości i odpowiedzialności, istotnych dla relacji między korporacjami i agencjami państwowymi w zakresie danych osobowych i innych działań nadzorczych, stały się podstawą badań w Citizen Lab.

W dniu 3 kwietnia 2020 r. Citizen Lab opublikował raport na temat analizy technicznej poufności komunikacji w popularnej aplikacji do czatów i wideokonferencji Zoom¹². Następnie 8 kwietnia br. wydał raport uzupełniający zawierający szczegółowe informacje na temat luki w zabezpieczeniach funkcji poczekalni w Zoom¹³. Początkowy raport wykazał, że szyfrowanie w Zoom nie wydawało się być dobrze zaprojektowane lub skutecznie wdrożone, a jego publiczna dokumentacja zawierała kilka mylących twierdzeń na temat protokołów szyfrowania Zoom, które nie pasowały do tego, co zaobserwowali eksperci dokonujący analizy. Znaleziono zostały także potencjalne problemy w zakresie bezpieczeństwa, związane z generowaniem i przechowywaniem informacji kryptograficznych Zoom. W niektórych testach badacze zaobserwowali, że klucze szyfrujące są dystrybuowane przez serwery Zoom w Chinach, nawet

¹¹ A. Winstanley, *Israeli spyware targeted Americans*, „Electronic Intifada” 2019, vol. 11/6, s. 1.

¹² B. Marczak, J. Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, The Citizen Lab, April 3, 2020, <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings>.

¹³ B. Marczak, J. Scott-Railton, *Zoom's Waiting Room Vulnerability*, The Citizen Lab, April 8, 2020, <https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability>.

gdy wszyscy uczestnicy spotkania byli poza Chinami. W raporcie opublikowanym 3 kwietnia 2020 r. zwrócono również uwagę na problem bezpieczeństwa z funkcją „poczekalni” Zooma. W szczególności stwierdzono, że serwery Zoom dostarczyły zarówno kluczy szyfrowania, jak i strumień wideo na żywo spotkania Zoom wszystkim użytkownikom w poczekalni, nawet jeśli oczekujący użytkownicy nie zostali zatwierdzeni do przyłączenia się do spotkania. Ten problem umożliwiłby dowolnemu nieautoryzowanemu użytkownikowi Zoom w poczekalni przechwycenie i odszyfrowanie „zaszyfrowanej” treści wideo¹⁴. Po opublikowaniu raportu przez Citizen Lab Zoom podjął szereg działań dotyczących bezpieczeństwa.

Systemy komunikacji, na których polegamy, rzadko były projektowane z myślą o bezpieczeństwie. Bezpieczeństwo rutynowo uważano za spowalniające tempo innowacji lub niemożliwe do narzucenia podstawowym systemom, które mają chroniczne awarie i które wymagałyby całkowitej przebudowy infrastruktury komunikacyjnej w celu „zabezpieczenia”. Konsekwencją takich rozwiązań w zakresie kontaktów online jest fakt, że istnieje szeroki wachlarz niezafatanych systemów, które pozostawiają ciągłe luki w zabezpieczeniach. Ryzyko to obejmuje najbardziej podstawowe warstwy użytkowanej przez nas infrastruktury informatycznej. Na przykład sieci telekomunikacyjne i komórkowe nadal polegają na dziesięcioletnim protokole wymiany informacji, zwanym SS7, który okazał się wysoce niepewny i podatny na nadużycia i nielegalny nadzór podczas wysyłania uwierzytelnień. Oznakami wskazującymi na ataki cyberprzestępcze, na które warto zwrócić uwagę podczas korzystania z komputera podłączonego do sieci są np.:

- pojawienie się nowych programów, które nie zostały przez nas zainstalowane;
- zwalnianie pracy komputera;
- wyskakujące reklamy pojawiające się na ekranie;
- utrata kontroli nad myszą lub klawiaturą.

Pomocą w powyższej sytuacji może okazać się proste rozwiązanie polegające na aktualizacji nowoczesnych oprogramowań antywirusowych. Najlepiej gdyby pracownicy mieli do dyspozycji komputery robocze, które są szybkie, dobrze

¹⁴ M. Kenyon, *Ronald Deibert Delivers Testimony to the House of Commons on Parliamentary Duties and the COVID-19 Pandemic*, <https://citizenlab.ca/2020/04/> (dostęp: 23.09.2020).

utrzymane i przeznaczone do odpowiednich zadań¹⁵. Warto pamiętać, by dane korporacyjne i osobowe były przechowywane osobno.

Jeśli chodzi o cyberzagrożenia w firmie, to pracownicy są zawsze najsłabszym ogniwem. Około 90% włamań i problemów związanych z cyberbezpieczeństwem jest spowodowanych błędem ludzkim, co oznacza, że najlepszym sposobem ochrony pracowników zdalnych przed zagrożeniami cybernetycznymi jest inwestowanie w odpowiednie szkolenie IT. Dbając o swoją prywatność w sieci, warto zwrócić uwagę na każdy detal.

Bezpieczeństwo organizacji w kontekście pandemii COVID-19 w świetle raportów

Sytuacja wywołana wystąpieniem wirusa COVID-19 zmusiła wiele przedsiębiorstw do przejścia na zarządzanie kryzysowe i niejednokrotnie przestawienie się na pracę zdalną. Praca zdalna nie jest oczywiście niczym nowym, jednak skala niezbędnych do podjęcia działań zaskoczyła wielu. Pierwszym problemem okazała się dostępność sprzętu nadającego się do pracy. Okazało się też, że procesy i procedury obowiązujące w niektórych firmach nie były właściwie przystosowane do nowych warunków. Kolejną przeszkodą było zarządzanie zespołami w nowych warunkach. Jednak elementem, który okazał się jednym z większych wyzwań nowej rzeczywistości, jest zapewnienie cyberbezpieczeństwa. Jak pokazuje raport Komisji Europejskiej, blisko połowa Europejczyków nie jest świadoma istnienia cyberzagrożeń. W tym samym czasie, według danych Accenture, liczba naruszeń bezpieczeństwa IT wzrasta z roku na rok o kilkanaście procent¹⁶. Niski poziom świadomości istnienia zagrożeń, w połączeniu ze wzrostem ataków, w szczególności typu *phishing* i *ransomware*, sprawia, że wiele przedsiębiorstw staje się podatnych na incydenty. Korzystanie z domowych routerów Wi-Fi, bardzo często z niezmiennymi fabrycznymi ustawieniami, wykonywanie na jednym komputerze zadań służbowych i prywatnych, wysoka podatność na działania socjotechniczne spowodowane obawami przed narastającą falą zakażeń – to tylko niektóre elementy sprzyjające tym wszystkim, którzy postanowili zwiększyć częstotliwość ataków hakerskich, wyczuwając

¹⁵ J. Grubicka, *Information society in the context of threats to personal security in cyberspace*, „Zeszyty Naukowe Politechniki Śląskiej Organizacja i Zarządzanie”, z. 141, Gliwice 2019, s. 96–97.

¹⁶ *Ninth Annual Cost of Cybercrime Study*, <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study> (dostęp: 12.05.2021).

w pandemii nadarzającą się okazję. Wyniki raportu IBM pokazują, że złośliwe oprogramowanie odpowiada za 52% wszystkich badanych przypadków. Z tych 52% aż 14% można przypisać atakom typu *phishing*, a 19% przypadkom przejęcia danych upoważniających do dostępu do danych. Na podstawie raportu *Cost of A Data Breach 2020*¹⁷ prawie 80% badanych przedsiębiorstw jest przekonana, że pandemia wpłynęła na pogorszenie stanu cyberbezpieczeństwa. Wśród ponad 500 badanych przedsiębiorstw z kilkunastu krajów na świecie, które padły ofiarą hakerów, średnia wielkość szkody wyrządzona tymi atakami wynosi prawie 3,9 mln dolarów.

Cyberbezpieczeństwo nie należało na ogół do priorytetów działań podejmowanych przez firmy dotknięte ograniczeniami związanymi z pandemią. Dla większości zarządzających zmiany wywołane przez COVID-19 stanowiły przede wszystkim zagrożenie dla stabilności finansowej firm – ryzyko gwałtownej utraty przychodów przy jednoczesnej konieczności utrzymywania niezmiennego poziomu kosztów. Jednak ponad 40% szkód wynikających z ataków hakerskich stanowią utracone przychody przedsiębiorstwa. Związek pomiędzy koniecznymi nakładami na cyberbezpieczeństwo a przychodami wydaje się więc dość oczywisty.

Na podstawie „Barometru Cyberbezpieczeństwa 2021”¹⁸ KPMG w opinii ponad połowy badanych firm pandemia COVID-19 przyczyniła się do wzrostu ryzyka cyberataków. Z drugiej strony 45% organizacji nie zauważa żadnego wpływu pandemii na bezpieczeństwo firmy. Mniejsze firmy, zatrudniające mniej niż 250 pracowników, w większym stopniu (60% wskazań) dostrzegają negatywny wpływ pandemii na bezpieczeństwo. W przypadku większych firm, zatrudniających powyżej 250 pracowników, negatywny wpływ pandemii na bezpieczeństwo zauważa połowa respondentów badania.

Szeroko rozumiana cyberprzestępczość niezmiennie od kilku lat pozostaje najczęściej wskazywaną grupą stanowiącą realne zagrożenie dla organizacji w Polsce. W 2021 r. wskazało na nią 85% firm. Największym zagrożeniem dla większości wciąż pozostają pojedynczy hakerzy oraz zorganizowane grupy

¹⁷ Raport *Cost of Data Breach 2020*, <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/> (dostęp: 12.05.2021).

¹⁸ Raport KPMG 2021(03), *Barometr cyberbezpieczeństwa COVID-19 przyspiesza cyfryzację firm*, s. 4–20. Badanie zostało zrealizowane metodą wywiadów telefonicznych CATI wśród osób odpowiedzialnych za bezpieczeństwo IT w firmach (członków zarządu, dyrektorów ds. bezpieczeństwa, prezesów, dyrektorów IT lub innych osób odpowiedzialnych za ten obszar). Badanie przeprowadzono na próbie 100 organizacji na przełomie stycznia i lutego 2021 r. przez firmę Norstat Polska.

cyberprzestępcze, na które wskazuje ponad połowa badanych firm. Pozostałe grupy są rzadziej postrzegane jako niebezpieczne. W 2021 r. zdecydowanie mniej firm niż w poprzednich edycjach badania wskazało na potencjalne niebezpieczeństwo utraty danych w wyniku działania podkupionych lub niezadowolonych pracowników. Wycieki danych za pośrednictwem złośliwego oprogramowania (*malware*) są postrzegane przez firmy w Polsce jako największe ryzyko w kontekście cyberzagrożeń. W następnej kolejności organizacje wskazują na wyludzenia danych uwierzytelniających (*phishing*) oraz wycieki danych w wyniku kradzieży lub zgubienia nośników bądź urządzeń mobilnych. Jako najmniej zagrażające organizacje wymieniają przede wszystkim włamanie do urządzeń mobilnych, ataki wykorzystujące błędy w aplikacjach oraz ataki na sieci bezprzewodowe. Warto jednak zauważyć, że różnice w ocenie największych i najmniejszych cyberzagrożeń są stosunkowo niewielkie. Dla firm w Polsce największym ograniczeniem w zakresie uzyskania odpowiedniego poziomu zabezpieczeń są trudności w zatrudnieniu i utrzymaniu wykwalifikowanych pracowników.

Kolejnym ograniczeniem jest brak wystarczających budżetów, na które wskazuje 42% badanych przedsiębiorstw. Jednocześnie widać znaczącą zmianę w porównaniu z rokiem 2019, kiedy na brak wystarczających finansów, które ograniczają możliwości uzyskania oczekiwanego poziomu zabezpieczeń, wskazało 64% firm. Warto zwrócić uwagę, że zbyt mały budżet jest większym problemem w przypadku mniejszych firm. Z kolei problemy związane z zasobami ludzkimi są większym wyzwaniem dla dużych organizacji. Coraz więcej firm w Polsce zaczyna dostrzegać istotne znaczenie prawidłowego przypisania odpowiedzialności za bezpieczeństwo informacji w organizacji. O 8 p.p., do 11%, wzrósł odsetek firm, w których za bezpieczeństwo informacji odpowiada niezależna jednostka organizacyjna: *Chief Security Officer* lub *Chief Information Security Officer*. W blisko połowie badanych firm bezpieczeństwo informacji spoczywa na dyrektorsze IT lub innym, skierowanym do tego pracowniku w strukturach IT.

Na podstawie badania KPMG w 2020 r. większość firm (64%) działających w Polsce zarejestrowała incydent polegający na naruszeniu bezpieczeństwa. Oznacza to, że kolejny rok okazał się być bardziej niebezpieczny pod względem prób cyberataków w porównaniu z 2019 r. Wyraźnie mniej organizacji nie zaobserwowało w 2020 r. żadnego ataku. W 2020 r. wzrost liczby prób cyberataków zauważyło 19% przedsiębiorców, natomiast ich

spadek odnotowało 4% respondentów badania. Warto zaznaczyć, że średnie firmy częściej obserwowały w 2020 r. próby cyberataków niż duże przedsiębiorstwa, zatrudniające powyżej 250 pracowników.

Priorytetowymi inwestycjami w zabezpieczenia planowanymi przez firmy w najbliższym czasie są przede wszystkim ochrona przed złośliwym oprogramowaniem, zapewnienie bezpieczeństwa sieci wewnętrznej w postaci segmentacji lub kontroli dostępu oraz ochrona przed wyciekami danych. Najmniejszych inwestycji firmy w najbliższym czasie planują dokonywać w obszarze klasyfikacji i kontroli aktywów oraz zapewnienia bezpieczeństwa w procesach wytwarzania oprogramowania.

Zmiany legislacyjne i rekomendacje instytucjonalne w zakresie bezpieczeństwa cyfrowego w okresie pandemii

Zgodnie z art. 675 § 1 Kodeksu pracy telepraca to regularne wykonywanie pracy poza zakładem pracy z wykorzystaniem środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną. Telepracownik wyniki swojej pracy, którą wykonuje poza zakładem, przekazuje pracodawcy zwłaszcza za pośrednictwem komunikacji elektronicznej, jednakże nie jest to wymóg konieczny. Możliwe jest przekazywanie efektów pracy w inny, ustalony w porozumieniu zawierającym pomiędzy pracownikiem i pracodawcą sposób. Ustawodawca wprowadził do obrotu instytucję pracy zdalnej w efekcie wybuchu pandemii koronawirusa na podstawie art. 3 § 1 Ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych. Zgodnie z przywoływanym przepisem pracodawca może polecić pracownikowi wykonywanie, przez czas oznaczony, pracy określonej w umowie o pracę poza miejscem jej stałego wykonywania w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie trzech miesięcy po ich odwołaniu.

Ustawienie cyberbezpieczeństwa na odległym miejscu na liście priorytetów działań antykryzysowych w przedsiębiorstwach miało jeszcze jeden skutek. Niewiele firm zdecydowało się na przeanalizowanie modelu pracy zdalnej pod kątem przystosowania jej do nowej skali i do nowych zagrożeń. Analizując zapisy kolejnych zmian legislacyjnych związanych z pandemią, można pokusić się o stwierdzenie, że takiej refleksji zabrakło także ustawodawcy.

Pomimo tego, że faktycznie duża część pracodawców wprowadzała możliwość wykonywania epizodycznie pracy poza lokalem przedsiębiorstwa na długo przed COVID-19, przez szereg lat w Polsce nie wprowadzano żadnych przepisów regulujących tę kwestię.

W całkowitej opozycji do tego znajdowała się telepraca, która została wprowadzona do Kodeksu pracy już blisko 13 lat temu. Telepraca, ze względu na ograniczenie tej regulacji wyłącznie do pracy świadczonej regularnie poza zakładem pracy, a także wprowadzenie rozbudowanych obowiązków spoczywających po stronie pracodawcy, nie znalazła jednak do dzisiaj wielu zwolenników. Dotychczas pracodawcy wprowadzając możliwość świadczenia części pracy w formie zdalnej, tworzyli wewnętrzne procedury, bazując na przepisach dotyczących telepracy oraz zagranicznych przykładach, przeważnie jednak głównie na swojej intuicji. Dzisiaj na skutek COVID-19 zaczynają pojawiać się elementarne regulacje i wytyczne bezpośrednio odnoszące się do pracy zdalnej.

Brytyjskie Narodowe Centrum Cyberbezpieczeństwa¹⁹ zwraca dodatkowo szczególną uwagę na konieczność uświadamiania pracowników o zagrożeniach związanych z pracą zdalną. Przykładem takim może być korzystanie z nośników USB, zwracanie uwagi na kontrolowanie urządzeń, z których korzystają, dbanie o ich bezpieczeństwo i natychmiastowe zgłaszanie faktu ich kradzieży.

Zgodnie z wytycznymi ENISA (Europejskiej Agencji ds. Cyberbezpieczeństwa)²⁰ przedsiębiorcy powinni pamiętać o:

- zapewnieniu bezpiecznych wideokonferencji;
- używaniu oprogramowania firmowego jedynie za pomocą zaszyfrowanych kanałów (SSL, VPN, IPSec);
- zapewnieniu natychmiastowej asysty działu IT w razie zagrożenia cyberatakami;
- edukacji personelu na temat zagrożeń, jakie mogą pojawić się w trakcie pracy zdalnej oraz przygotowanie polityki firmy w razie kradzieży danych osobowych.

W kontekście zapewnienia cyberbezpieczeństwa organizacji w warunkach pracy zdalnej istotne dla każdego pracodawcy będą wytyczne Międzynarodowej

¹⁹ *National Cyber Security Centre*, <https://www.ncsc.gov.uk/files/home%20working%20v1.pdf> (dostęp: 12.05.2021).

²⁰ *ENISA*, <https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home> (dostęp: 12.05.2021).

Organizacji Pracy²¹, która w swoim praktycznym poradniku dotyczącym pracy zdalnej podczas pandemii COVID-19 oraz po niej wskazuje na szczególnie istotny obowiązek informowania pracowników o wszelkich prawach i obowiązkach, których przestrzegać należy w czasach pandemii, zapewniania im odpowiedniego sprzętu do pracy oraz edukacji w obszarze możliwych cyberataków.

Zagadnienia związane z cyberbezpieczeństwem to element stosunkowo nowy w europejskiej i polskiej praktyce legislacyjnej oraz jurysprudencji. Wobec braku rozbudowanych przepisów jednoznacznie regulujących wymogi bezpieczeństwa pracy zdalnej istotne znaczenie dla pracodawców mogą odgrywać wytyczne wydawane przez organy regulacyjne i odnoszące się do bezpieczeństwa przetwarzania danych (w tym danych osobowych), także w zakresie pracy zdalnej. Świadome tej sytuacji władze zacieśniają współpracę międzynarodową, na przykład poprzez inicjatywę „Partnerstwo przeciwko cyberprzestępczości” Światowego Forum Ekonomicznego. Jego misją, która rozpoczęła się w kwietniu 2020 r., jest zbadanie sposobów zacieśnienia współpracy publiczno-prywatnej i zwalczania globalnej cyberprzestępczości. Wzmocniona współpraca między krajowymi organami ścigania przyniosła już pewne znaczące sukcesy, takie jak demontaż EncroChat (szyfrowanej sieci telefonicznej szeroko wykorzystywanej przez przestępczość zorganizowaną) przez francuską i holenderską policję i organy sądowe, Europol i Eurojust. Jednocześnie organy ścigania wzmagają wysiłki, aby ułatwić zgłaszanie cyberprzestępczości. Na przykład w brytyjskim National Cyber Security Center (NCSC) specjalnie stworzony do tego celu adres e-mail do zgłaszania oszustw internetowych zarejestrował ponad milion skarg w mniej niż dwa miesiące. Zakłada się, że współpraca między krajowymi i międzynarodowymi organami ścigania w obszarze inwigilacji cybernetycznej zostanie zoptymalizowana i stanie się bardziej wydajna, co umożliwi pociągnięcie do odpowiedzialności większej liczby cyberprzestępców.

Z początkiem pandemii Urząd Ochrony Danych Osobowych, opierając się na wytycznych swojego irlandzkiego odpowiednika, przedstawił szereg rekomendacji dotyczących bezpiecznego przetwarzania danych²². W zakresie wykorzystywanych urządzeń UODO zaleca:

²¹ ILO, https://www.ilo.org/wcmsp5/groups/public/--ed_protect/--protrav/--travail/documents/publication/wcms751232.pdf (dostęp: 12.05.2021).

²² Rozporządzenie Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, t. jedn.: Dz.U. z 2017 r. poz. 2247 ze zm., <https://uodo.gov.pl/pl/138/1459>.

- wprowadzanie przez pracodawców odpowiednich procedur bezpieczeństwa oraz obligowanie pracowników do stosowania się do nich;
- nieinstalowanie dodatkowych aplikacji i oprogramowania niezgodnych z procedurą bezpieczeństwa organizacji;
- bieżące aktualizacje systemu operacyjnego, oprogramowania oraz systemu antywirusowego;
- unikanie dostępu do danych zgromadzonych na komputerze poprzez uniemożliwianie zapoznawania się z nimi przez osoby postronne, przez obserwowanie naszego monitora, jak i blokowanie urządzeń, gdy od nich odchodzimy;
- stosowanie silnych haseł dostępu oraz wielopoziomowego uwierzytelniania;
- zwracanie szczególnej uwagi na to, aby urządzenia, na których gromadzone są dane, w tym dyski zewnętrzne, nie zostały zgubione, a w przypadku kradzieży: natychmiastowe podejmowanie odpowiednich kroków, aby, o ile to możliwe, zdalnie wyczyścić pamięć danego urządzenia.

W zakresie korzystania ze służbowej poczty elektronicznej:

- postępowanie zgodnie z obowiązującymi zasadami w organizacji dotyczącymi korzystania ze służbowej poczty elektronicznej;
- używanie przede wszystkim służbowych kont e-mail;
- odpowiednie szyfrowanie e-maili i załączników, gdy przekazujemy w ich treści dane osobowe;
- upewnianie się przed wysłaniem e-maila, że wysyłamy go do właściwego adresata, zwłaszcza jeśli wiadomość zawiera dane osobowe lub dane wrażliwe;
- dokładne sprawdzanie nadawców e-maili oraz nieotwieranie wiadomości od nieznanych adresatów, a zwłaszcza nieotwieranie załączników oraz nieklikanie w linki zawarte w takiej wiadomości;
- przysyłanie hasła do zaszyfrowanego pliku odrębnym kanałem komunikacyjnym.

W zakresie korzystania z sieci i chmury:

- korzystanie tylko z zaufanego dostępu do sieci lub chmury oraz przestrzeganie wszelkich zasad i procedur organizacyjnych dotyczących logowania i udostępniania danych;
- gdy nie mamy dostępu do sieci lub chmury, dbanie, aby przechowywane dane były w bezpieczny sposób zarchiwizowane.

Przydatność zaleceń UODO będzie różna w zależności od stopnia przygotowania do realizacji zagadnienia ochrony bezpieczeństwa danych. Podmioty, które już mają rozwinięte systemy, zapewne skorzystają niewiele, natomiast przedsiębiorstwa, dla których zagadnienie cyberbezpieczeństwa jest stosunkowo mało znanym, mogą traktować zalecenia UODO jako dobry punkt wyjściowy do dalszych prac.

Niezależnie od wytycznych UODO na szczególną uwagę zasługują także inne rekomendacje wypracowywane przez odpowiednie organy opracowujące zasady bezpiecznej pracy zdalnej w okresie COVID-19. The Cybersecurity and Infrastructure Security Agency (CISA) postuluje²³:

- zapewnianie połączenia VPN swoim pracownikom i sprawdzenie, jak działa w sytuacji dużej liczby korzystających z niego użytkowników (w razie problemów zapewnienie priorytetu użytkownikom posiadającym dostęp do większej bazy danych);
- stworzenie systemu monitorowania, który wykrywa nietypowe działania mające miejsce na urządzeniach pracowników;
- aktualizowanie zapór sieciowych na urządzeniach oraz instalowanie oprogramowania do wykrywania szkodliwego oprogramowania typu *malware* i IPS (*Intrusion Detection Systems*);
- informowanie pracowników o możliwych atakach phishingowych;
- przygotowanie wewnętrznych działów IT na kontrolowanie logowań na urządzeniach, wykrywanie cyberataków oraz szybkie reagowanie na podejrzone działania;
- wdrożenie uwierzytelnienia wielopoziomowego, zapewniającego bezpieczeństwo w razie logowania na urządzeniach, w trakcie pracy zdalnej, a w przypadku braku MFA (uwierzytelniania wielopoziomowego), używanie silnych haseł do logowania.

Na poziomie funkcjonowania organizacji różnego rodzaju ujawniane są coraz to nowe oblicza cyberzagrożeń, a ich natura i skutki od dawna wykroczyły poza zakres kontroli zaplecza technicznego o odpowiednią infrastrukturę posiadanego sprzętu i urządzeń ICT. Obecnie największe obawy związane z bezpieczeństwem cyfrowym dotyczą szerokiej gamy zagrożeń techniczno-behawioralnych, a osiągnięcie zadowalającego poziomu bezpieczeństwa cyfro-

²³ CISM, https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf (dostęp: 12.04.2021).

wego stanowi kluczowe wyzwanie dla decydentów instytucji oraz właścicieli czy menedżerów podmiotów gospodarczych.

Podsumowanie

Bezpieczeństwo cyfrowe to jednak nowego rodzaju „pole walki”, w którym podmiotom aktywnie stwarzającym zagrożenia (niestety generowanym głównie przez czynnik ludzki) stale trzeba jeszcze aktywniej się przeciwstawiać. Zarówno poprzez technologię, jak i kreowanie odpowiednich – bezpiecznych – zachowań cyfrowych różnych interesariuszy nowej digitalnej rzeczywistości: obywateli, pracowników, klientów. Pomimo posiadania znaczących zasobów intelektualnych i technologicznych oraz wydatkowania coraz poważniejszych nakładów finansowych, bezpieczeństwo cyfrowe jest obszarem, w którym niepewność i świadomość ryzyka nie maleje, a systematycznie wzrasta.

Przykładem sytuacji, w której waga cyberbezpieczeństwa zyskała nowy, globalny wymiar, jest kryzys spowodowany wirusem SARS-CoV-2.

Cyberbezpieczeństwo to dynamiczny proces, w którym z jednej strony aktywny udział biorą podmioty stwarzające zagrożenia, a z drugiej podmioty przeciwstawiające się im. Znany z realiów militarnych układ: atakujący–broniący się nie może jednak oznaczać defensywy tego drugiego. Ochrona bezpieczeństwa cyfrowego organizacji to przede wszystkim prewencja, doskonalenie, innowacja. Współczesne osiągnięcia techniczne w dziedzinie przetwarzania danych, pamięci masowej i łączności z internetem jeszcze wyraźniej podkreślają potrzebę lepszego zrozumienia warunków bezpieczeństwa systemów, na których polegamy.

Bibliografia

- McQuail D., *McQuail's Mass Communication Theory*, Sage, Londyn 2000.
- Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.
- First do no Harm: Xe Problem of Spyware*, Crawford S.P. (ed.), „Berkeley Technology Law Journal” 2005.
- Grubicka J., *Information society in the context of threats to personal security in cyberspace*, „Zeszyty Naukowe Politechniki Śląskiej Organizacja i Zarządzanie” 2019, z. 141.
- Kenyon M., Deibert R., *Delivers Testimony to the House of Commons on Parliamentary Duties and the COVID-19 Pandemic*, <https://citizenlab.ca/2020/04>.
- Pokruszyński W., *Filozofia bezpieczeństwa*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2013.
- Sun L., *Who Can Fix Ie Spyware Problem?*, „Berkeley Technology Law Journal” 2007.
- Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego*, „Zeszyty Naukowe” 2014, nr 2(10).
- CISM, https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf.
- ENISA, <https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home>.
- ILO, https://www.ilo.org/wcmsp5/groups/public/--ed_protect/--protrav/--travail/documents/publication/wcms_751232.pdf.
- National Cyber Security Centre, <https://www.ncsc.gov.uk/files/home%20working%20v1.pdf>.
- Ninth Annual Cost of Cybercrime Study*, <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>.
- Raport Cost of Data Breach 2020*, <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>.

Digital security of organizations in the time of the COVID-19 pandemic

Abstract: The COVID-19 pandemic has caused the most disruption to the organization since World War II, and its implications for cybersecurity in control systems are greater than anyone could have predicted. The publication is based on current cybersecurity research conducted during the COVID-19 pandemic. The author drew attention to the need to conduct activities in the form of a three-point strategy – technological and organizational solutions as well as employees' competences, which enable filling the gap in digital security systems, especially in the COVID-19 conditions. The COVID-19 pandemic has caused the most disruption to the organization since World War II, and its implications for cybersecurity in control systems are greater than anyone could have predicted. The publication is based on current cybersecurity research conducted during the COVID-19 pandemic. The author drew attention to the need to conduct activities in the form of a three-point strategy - technological and organizational solutions as well as employees' competences, which enable filling the gap in digital security systems, especially in the COVID-19 conditions.

Key words: digital security, organization, cybersecurity threats

mgr Michał Olejniczak, opiekun Koła Naukowego Studentów Zarządzania „IBIZA”

Akademia Pomorska w Słupsku

Instytut Bezpieczeństwa i Zarządzania, Katedra Zarządzania

e-mail: michal.olejniczak@apsl.edu.pl

ORCID: 0000-0001-9868-3601

licencjatki Aleksandra Jopek, Patrycja Nadolska, Natalia Ostrowska, Agata Sokołowska

Absolwentki kierunku zarządzanie Akademii Pomorskiej w Słupsku, członkinie Koła Naukowego Studentów Zarządzania „IBIZA”

Rozdział 3

Bezpieczeństwo ekonomiczne i zarządzanie kryzysowe przedsiębiorców województwa pomorskiego w początkach pandemii koronawirusa

Streszczenie: Celem pracy jest przedstawienie sytuacji ekonomicznej przedsiębiorców z woj. pomorskiego w początkowym okresie pandemii koronawirusa. Dla realizacji tego założenia w publikacji wykorzystano narzędzie ankiety. Zostały one wypełnione przez przedsiębiorców reprezentujących głównie działalność usługową. Wyniki ankiet wskazują, iż przedsiębiorcy nie byli odpowiednio przygotowani na ograniczenia związane z sytuacją epidemiologiczną. Przedsiębiorcy musieli szybko reagować, aby utrzymać działalność. Część z nich skorzystała z pomocy państwa. W pracy podjęto próbę zdiagnozowania zagrożeń w bezpieczeństwie ekonomicznym przedsiębiorców w momencie gwałtownych zmian w gospodarce. Firmy zmuszone były do dokonywania zmian w sytuacjach kryzysowych. Ważne, aby przedsiębiorcy, głównie rozpoczynający prowadzenie działalności, systematycznie koncentrowali się na obszarze ryzyka. Publikacja zwraca uwagę na aspekty, których zaniechanie może prowadzić do utraty stabilności firmy w sytuacjach kryzysowych.

Słowa kluczowe: COVID-19, bezpieczeństwo ekonomiczne, przedsiębiorcy, lockdown w Polsce

Wprowadzenie

W dniu 4 marca 2020 r. podczas konferencji prasowej minister zdrowia prof. Łukasz Szumowski ogłosił pierwszy potwierdzony przypadek zakażenia koronawirusem SARS-CoV-2 w Polsce¹. Ten moment stał się datą zwrotną, kolejną był dzień 12 marca 2020 r., kiedy to ten sam minister poinformował o pierwszej ofierze śmiertelnej w Polsce². Pokłosiem tych wydarzeń były ograniczenia prawne dotyczące obywateli, ale również i przedsiębiorców. Warto wspomnieć m.in. o Ustawie z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, która weszła w życie już 8 marca 2020 r.³, decyzji Rządowego Zespołu Zarządzania Kryzysowego z dnia 10 marca 2020 r. o zakazie imprez masowych⁴, kontrolach na granicach wprowadzonych w dniu 13 marca 2020 r.⁵, ogłoszeniu w dniu 20 marca stanu epidemii w Polsce⁶, czy też zakazie przemieszczania się z dnia 24 marca 2020 r.⁷ Kolejne ograniczenia prawne dotyczyły m.in. zamknięcia z dniem 31 marca 2020 r. działalności gastronomicznej, rekreacyjnej i hotelowej oraz niektórych działalności usługowych, a także ograniczeń ilości klientów w sklepach⁸. Celem niniejszej pracy jest zobrazowanie sytuacji ekonomicznej przedsiębiorców z woj. pomorskiego w początkowym okresie pandemii koronawirusa. Dla realizacji przedmiotowego celu badawczego posłużono się metodą sondażu diagnostycznego (szczegóły poniżej w „metodologii badań”).

¹ <http://www.gov.pl/web/zdrowie/pierwszy-przypadek-koronawirusa-w-polsce> (dostęp: 28.04.2020).

² <http://www.hellozdrowie.pl/koronawirus-w-polsce-stwierdzono-pierwszy-smiertelny-przypadek-zakazenia-wirusem-sars-cov-2/> (dostęp: 28.04.2020).

³ Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. 2020 poz. 1842).

⁴ <http://gov.pl/web/mswia/rzadowy-zespol-zarzadzania-kryzysowego-podjal-decyzje-o-odwołaniu-imprez-masowych> (dostęp: 28.04.2020).

⁵ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2020 r. w sprawie przywrócenia tymczasowo kontroli granicznej osób przekraczających granicę państwową stanowiącą granicę wewnętrzną (Dz.U. 2020 poz. 434).

⁶ Rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz.U. 2020 poz. 491).

⁷ Rozporządzenie Ministra Zdrowia z dnia 24 marca 2020 r. zmieniające rozporządzenie w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz.U. 2020 poz. 522).

⁸ Rozporządzenie Rady Ministrów z dnia 31 marca 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz.U. 2020 poz. 566).

Pandemia koronawirusa

Zagrożenia epidemiczne dla człowieka są znane od zarania dziejów. Bakterie, wirusy lub pierwotniaki wywołują choroby zakaźne, które towarzyszą ludzkości od zawsze. Dowody można odnaleźć w źródłach historycznych. Najważniejsze i najgroźniejsze dla ludzkości są epidemie lub pandemie, ponieważ wpływają one na życie ludzi. Pandemie dziesiątkują ludność na różnych kontynentach, decydują o losach wojen lub przyczyniają się do masowej migracji. Przemierzając się po różnych miejscach, ludzie łatwo przenosili choroby na nowe obszary. Walka z chorobami zakaźnymi jest niezwykle trudna, ponieważ istniejące szczepionki są zazwyczaj nieskuteczne i powodują objawy niepożądane. Okres oczekiwania na skuteczną szczepionkę jest bardzo długi, co powoduje, że pandemia nie ustępuje i ciągle rozszerza obszar swojego działania. W przypadku dobrze znanych nam chorób, na przykład AIDS i malarii, wciąż brakuje profilaktyki. Od samego początku pojawienia się chorób próbowano walczyć z nimi znanymi metodami, opierając się na obserwacjach⁹.

Szybkość szerzenia się pandemii jest pokaźna, na przykład po wtargnięciu cholery do Peru w styczniu 1991 r. w lutym choroba była już w Ekwadorze, w marcu w Kolumbii, a w kwietniu dotarła już do Chile i zarejestrowano pierwsze zachorowania na terenie Brazylii. W ciągu roku epidemie cholery wystąpiły w większości krajów Ameryki Środkowej i Ameryki Południowej¹⁰.

Polska od marca 2020 r. zmaga się z pandemią koronawirusa. Ta niebezpieczna choroba łatwo rozprzestrzeniała się, co powodowało wysoki odsetek śmiertelności i poważne zagrożenie dla zdrowia publicznego. Wymagała specjalnych metod zwalczania. Choroby zakaźne zaliczane są do szczególnie niebezpiecznych i objęte są kwarantanną, co oznacza odosobnienie osoby zdrowej, która była narażona na zakażenie. Czas trwania kwarantanny zależy od okresu wylęgania choroby. COVID-19 to zespół ostrej ciężkiej niewydolności oddechowej, rodzaj zapalenia płuc. Do zakażenia może dochodzić poprzez drogę kropelkową lub zanieczyszczonymi przedmiotami z otoczenia zakażonego¹¹.

⁹ W. Baturo, *Katastrofy i zagrożenia we współczesnym świecie*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 154.

¹⁰ Tamże, s. 288.

¹¹ J. Duława, *Vademecum medycyny wewnętrznej*, PZWL Wydawnictwo Lekarskie, Warszawa 2015, s. 1488.

W czasach koronawirusa wiele przedsiębiorstw musiało zmierzyć się z różnorodnymi problemami ekonomicznymi.

Bezpieczeństwo ekonomiczne

Bezpieczeństwo jest potrzebą, która jest lokowana na jednym z pierwszych miejsc w hierarchii potrzeb człowieka. Nie zawsze jednak tak było. Wynikać może to z faktu, iż bezpieczeństwo nie jawiło się jako sprawa społeczeństwa, niepewnego i bezsilnego wobec żywiołów i plag, lecz jako sprawa Boga i losu. Wzrost znaczenia bezpieczeństwa jest związany z poczuciem zagubienia człowieka w chaosie zdarzeń, natłoku informacji czy zmian, jakie dokonują się w kwestii sił gospodarczych i politycznych na świecie. Człowiek od zawsze stawał w obliczu zarówno zagrożeń naturalnych (fizycznych, materialnych), jak i zagrożeń duchowych (irracjonalnych, niematerialnych)¹².

Termin „bezpieczeństwo” jest trudny do zdefiniowania, co wynika z faktu, iż na jego definicję ma wpływ wiele aspektów związanych z takimi dziedzinami nauki, jak: psychologia, historia, nauki prawne, socjologia czy politologia. Za najbardziej ogólną definicję bezpieczeństwa uznaje się tę zaproponowaną przez Daniela Lereñera: „w najbardziej dosłownym znaczeniu bezpieczeństwo jest właściwie identyczne z pewnością i oznacza brak zagrożenia fizycznego albo ochronę przed nim”. Zaspokojenie takich potrzeb, jak: przetrwanie, tożsamość, istnienie, spokój, posiadanie czy pewność rozwoju i niezależność obejmuje bezpieczeństwo. Stan poczucia zagrożenia oraz ogólny niepokój jest wywołany przez brak bezpieczeństwa¹³. Jednocześnie należy zwrócić uwagę, że powyższa definicja poddawana jest krytyce¹⁴.

Bezpieczeństwo ekonomiczne jest różnie definiowane, jednak elementem zasadniczym jest zachowanie możliwości rozwoju gospodarki danego kraju (w aspekcie makroekonomicznym), zaś w aspekcie mikroekonomicznym należałoby odnieść to do możliwości rozwoju danej organizacji. Bezpieczeństwo

¹² A. Wawrzusiszyn, *Pojęcie i istota bezpieczeństwa*, w: J. Stawnicka, B. Wiśniewski, R. Socha (red.), *Zarządzanie kryzysowe. Teoria, praktyka, konteksty, badania*, Wydawnictwo Wyższej Szkoły w Szczytnie, Szczytno 2011, s. 9.

¹³ D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego analiza wybranych przepisów*, Centrum Naukowo-Badawcze Ochrony Przeciwpowodziowej, Józefów 2014, s. 16.

¹⁴ A. Bralewski, *Zagrożenie bezpieczeństwa ekonomicznego Polski*, „Zeszyty Naukowe SGSP” 2018, nr 68/4, s. 210.

ekonomiczne jest ściśle powiązane z bezpieczeństwem gospodarczym. Należy zwrócić uwagę, że zagrożenia bezpieczeństwa gospodarczego mogą być tożsame z zagrożeniami bezpieczeństwa ekonomicznego. Pojęcia te często są stosowane zamiennie¹⁵.

Wśród głównych elementów bezpieczeństwa ekonomicznego organizacji należy wskazać: finansowe, polityczno-prawne, techniczne i technologiczne, informacji, środowiska i energii¹⁶.

Zarządzanie kryzysowe

Zarządzanie kryzysowe jest mianem określającym działalność organów administracji publicznej. Działalność ta jest jednym z elementów odpowiedzialnych za kierowanie bezpieczeństwem narodowym. Zgodnie z Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym polega ono na „zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej”¹⁷.

W związku ze stale zmieniającym się stanem bezpieczeństwa i realizacją celu, jakim jest utrzymanie zdolności do reagowania, zarządzanie kryzysowe wymaga stałego dostosowywania sił i środków. Niezwykle istotne jest monitorowanie zmieniającego się otoczenia i dostosowywanie do aktualnych warunków systemu zarządzania kryzysowego.

Poszczególne elementy struktury zarządzania kryzysowego muszą mieć właściwie zdefiniowane role i zadania. W sytuacjach zagrożenia niezbędne jest posiadanie jasno sprecyzowanych i zaplanowanych działań, istotne jest również podejmowanie czynności bez zbędnej zwłoki¹⁸.

¹⁵ Tamże, s. 211–213.

¹⁶ O. Chepik, E. Mishanova, G. Kalinina, A. Gracheva, *Economic Security of Economic Entities in Crises*, w: Sh. Gimbatov, Z. Abdulaeva, A. Bashirova, D. Denevizyuk, *Proceedings of the VIII International Scientific and Practical Conference “Current problems of social and labour relations” (ISPC-CPSLR 2020)*, „Advances in Social Science, Education and Humanities Research” 2021, vol. 527, s. 145.

¹⁷ Ustawa dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst ujednolicony: Dz.U. 2007 nr 89 poz. 590 z późn. zm.) (dalej jako: ustawa zarz. kryzys.).

¹⁸ D. Wróblewski (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem...*, dz. cyt., s. 20.

Odnosząc się do firm, źródeł sytuacji kryzysowej można poszukiwać wewnątrz przedsiębiorstwa (czynniki endogeniczne) oraz w jego bliższym i dalszym otoczeniu (czynniki egzogeniczne). Kryzysy wynikają zarówno z uwarunkowań makroekonomicznych, jak i globalnych, na które przedsiębiorstwo nie ma bezpośredniego wpływu, a które wpływają na działalność przedsiębiorstwa¹⁹. Można pokusić się o stwierdzenie, że z perspektywy przedsiębiorcy sytuacja kryzysowa jest nieodłącznym elementem jego działania. Tym samym zarządzanie kryzysowe w przedsiębiorstwie to proces, który ma na celu zapobieganie sytuacjom kryzysowym i ich eskalacji, redukovanie wpływu kryzysu na zasoby i wartości, podejmowanie kontroli nad przebiegiem kryzysu, przywracanie stabilizacji²⁰.

Metodologia badań

Ograniczenia prawne wprowadziły sporo niepewności w zakresie prowadzenia działalności gospodarczej. Krótko po tym, jak wprowadzono ograniczenia w zakresie prowadzenia działalności gospodarczej, a bezpieczeństwo zdrowia publicznego wymagało pozostawania w domach i ograniczenia poruszania się, rozesłano do losowo wybranych przedsiębiorców woj. pomorskiego (z różnych branż) link do anonimowej ankiety, która składała się z 12 pytań. Podstawą przeprowadzonych badań było sformułowanie następujących hipotez:

1. COVID-19 wpłynie na bezpieczeństwo ekonomiczne firm, w szczególności na prognozowane przychody;
2. Wśród największych zagrożeń przedsiębiorców będzie konieczność redukcji etatów oraz zmniejszenie produkcji/usług;
3. Pandemia wymusi zmiany w funkcjonowaniu firm;
4. Wprowadzone zmiany mogą nie być respektowane przez pracowników.

Pierwsze trzy pytania dotyczyły rodzaju dominującej działalności przedsiębiorstwa, okresu działalności firmy oraz jej wielkości. Kolejne pytania miały na celu zbadanie m.in.: oczekiwań przedsiębiorców w zakresie pomocy państwa, planów w zakresie redukcji etatów, zmian wprowadzonych w firmach, a wynikających z przebiegu epidemii oraz ograniczeń i zakazów prawnych, oceny zagro-

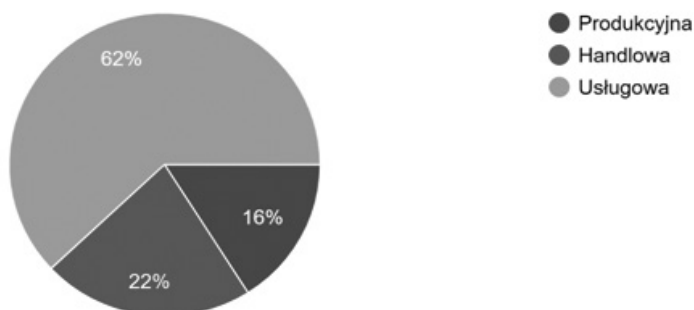
¹⁹ M. Michałowska, D. Stankiewicz, W. Danielak, *Zarządzanie sytuacją kryzysową w przedsiębiorstwie*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze” 2015, nr 2, s. 111–112.

²⁰ Tamże, s. 116.

zeń dla działalności gospodarczej. Wyniki badań były zbierane od 19 kwietnia do 14 maja 2020 r. Na pytania ankietowe odpowiedziało 50 przedsiębiorców.

Wyniki badań

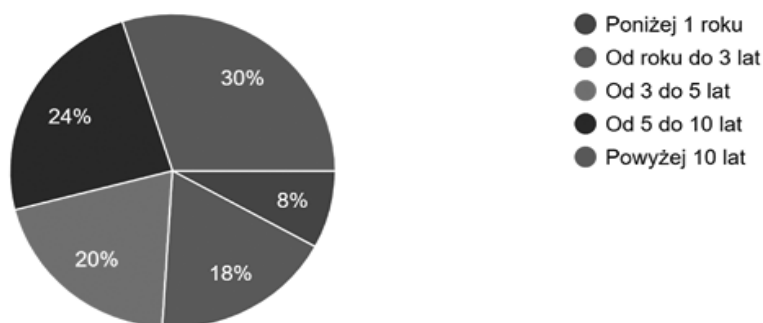
Rys. 1. Rodzaj dominującej działalności przedsiębiorstwa



Źródło: Opracowanie własne.

Sześćdziesiąt dwa procent badanych wskazało na działalność usługową jako rodzaj dominującej działalności przedsiębiorstwa. Zdecydowanie mniej, bo 22% ankietowanych, podało działalność handlową, a 16% produkcyjną. Część przedsiębiorców mogła i zapewne prowadziła działalność w mieszanej formie, np. produkcyjno-usługowej lub produkcyjno-usługowo-handlowej.

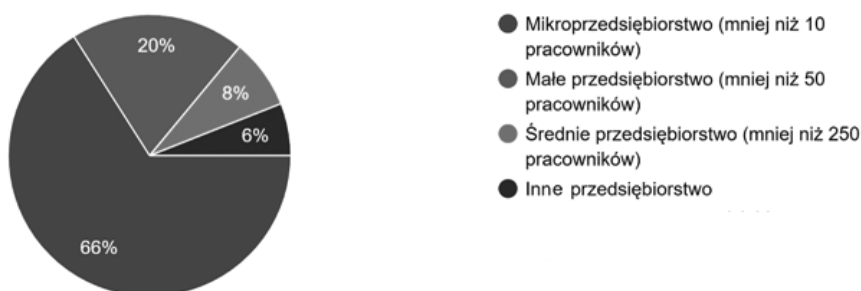
Rys. 2. Okres działalności przedsiębiorstwa



Źródło: Opracowanie własne.

Respondentom zadano pytanie, jak długo prowadzą swoje przedsiębiorstwo. Mieli do wyboru pięć wariantów odpowiedzi. Prawie 1/3 firm prowadzi swoją działalność dłużej niż 10 lat, czyli były to przedsiębiorstwa ze sporym doświadczeniem. Ponad połowę (54%) stanowiły firmy, które funkcjonują co najmniej pięć lat. Siedemdziesiąt cztery procent stanowiły firmy z doświadczeniem nie mniejszym niż trzy lata. Dwadzieścia cztery procent firm stanowiły te z doświadczeniem krótszym niż trzy lata, z czego 8% z krótszym niż rok.

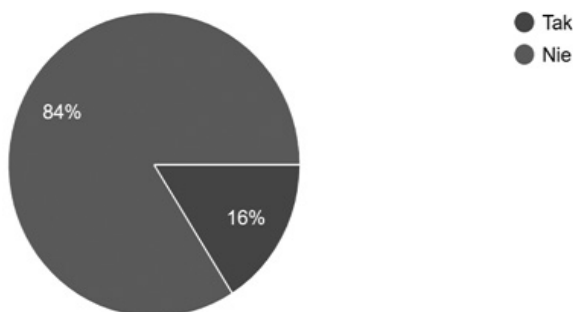
Rys. 3. Wielkość przedsiębiorstwa



Źródło: Opracowanie własne.

Dwie trzecie ankietowanych firm stanowili mikroprzedsiębiorcy. Prawie 30% stanowiły małe i średnie przedsiębiorstwa. Analizując trzy pierwsze pytania, można wskazać profil przeważającego ankietera: mikroprzedsiębiorca z branży usługowej, z kilkuletnim doświadczeniem.

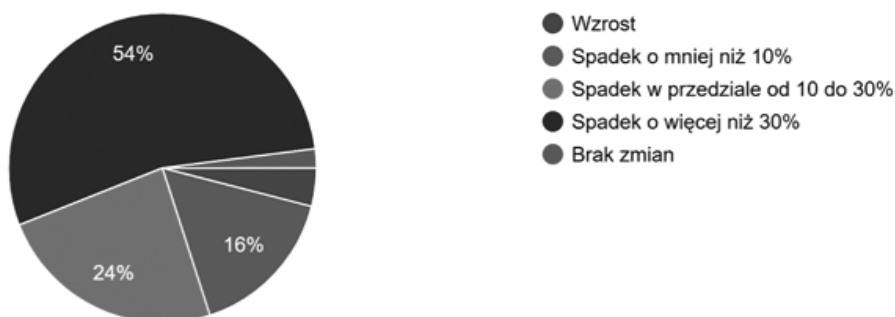
Rys. 4. Planowana w najbliższym czasie redukcja etatów



Źródło: Opracowanie własne.

Respondentom zadano pytanie: „Czy w najbliższych miesiącach Państwa firma zamierza zredukować liczbę pracowników?”. Mieli do wyboru dwa warianty odpowiedzi. Zdecydowana większość przedsiębiorców (84%) nie planowała w najbliższym czasie redukcji liczby pracowników. Pozostałe 16% wskazało, iż planuje redukcję etatów. Należy zwrócić uwagę, że po pierwsze ankietę przeprowadzono w kwietniu–maju 2020 r., a więc w okresie ogromnej niepewności, a po drugie 2/3 ankietowanych to mikroprzedsiębiorcy. W takich firmach niekiedy nie ma kogo zwalniać.

Rys. 5. Prognozowana zmiana przychodów w 2020 r. pod wpływem kryzysu

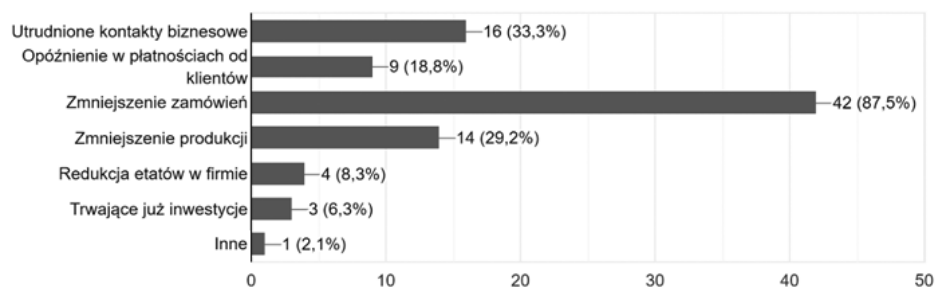


Źródło: Opracowanie własne.

Większość badanych (54%) prognozowała w 2020 r. spadek przychodów przedsiębiorstwa o więcej niż 30%. Natomiast spadek przychodów w przedziale 10–30% zadeklarowało 24% badanych, spadek o mniej niż 10% planowało 16% badanych. Dwa procent przewidywało stagnację w zakresie przychodów przedsiębiorstwa pod wpływem kryzysu.

Cztery procent ankietowanych firm uznało, że w wyniku pandemii osiągną wzrost przychodów w 2020 r., zaś 94% przedsiębiorców obawiało się o swoje finanse, prognozując w tym okresie spadki przychodów.

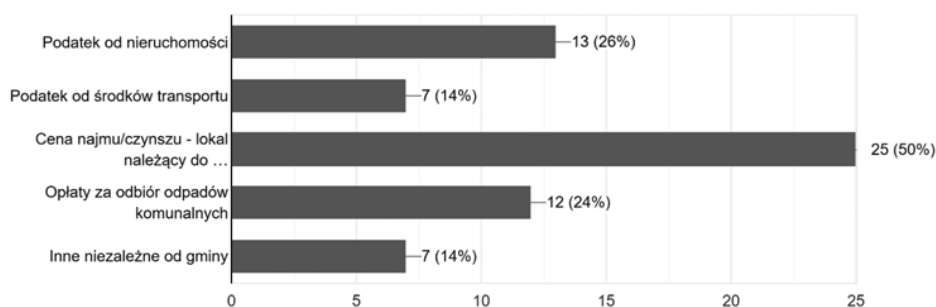
Rys. 6. Największe zagrożenie dla firmy w obecnej sytuacji



Źródło: Opracowanie własne.

Firmom zadano pytanie, co w obecnej sytuacji stanowi dla nich największe zagrożenie. Z zestawu ośmiu odpowiedzi respondenci mogli wybrać nie więcej niż trzy. Na to pytanie odpowiedzi udzieliło 48 firm. Zdecydowana większość – prawie 90% badanych – uważa za największe zagrożenie to zmniejszenie zamówień. Jedna trzecia respondentów wskazała na utrudnione kontakty biznesowe oraz zmniejszenie produkcji (29,2%). Prawie 19% wskazało na opóźnienie w płatnościach od klientów. Około 8% badanych podało redukcję etatów, zaś ok. 6% trwające inwestycje.

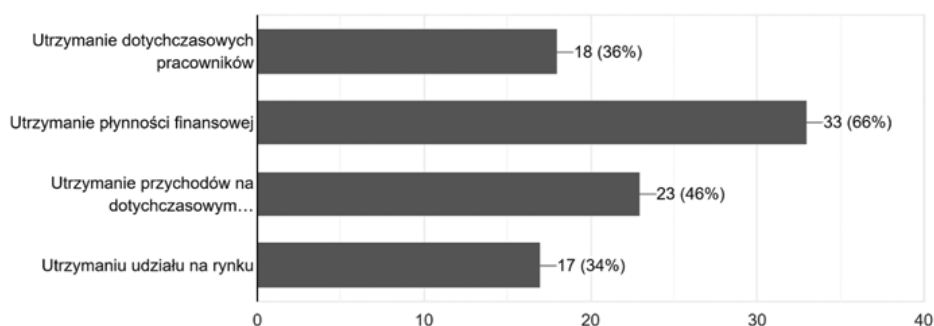
Rys. 7. Opłaty na rzecz JST stanowiące obecnie największe obciążenie



Źródło: Opracowanie własne.

Badanym zadano pytanie: „Jakie opłaty na rzecz jednostek samorządu terytorialnego są w tej chwili dla Państwa firmy największym obciążeniem?”. Było to pytanie wielokrotnego wyboru (50 firm). Połowa (50%) respondentów wskazuje, że największym obciążeniem dla firmy są opłaty związane z ceną najmu/czynszu lokalu należącego do gminy. Podatek od nieruchomości jest dla 26% badanych najuciążliwszy, 24% wskazało na opłaty za odbiór odpadów komunalnych. Odpowiedzi: „Podatek od środków transportu” i „inne niezależne od gminy” zostały wybrane przez 12% ankietowanych. Konkludując, cena najmu/czynszu za lokal należący do gminy jest rodzajem opłaty wskazywanym przez badanych jako najbardziej uciążliwy. Rodzi się jednocześnie pytanie, czy wskazując na opłatę czynszową, przedsiębiorcy mieli na myśli również opłaty na rzecz firm/osób niezwiązanych z JST? Przy ewentualnych kolejnych badaniach należy w tym zakresie dokonać wyraźnego podziału.

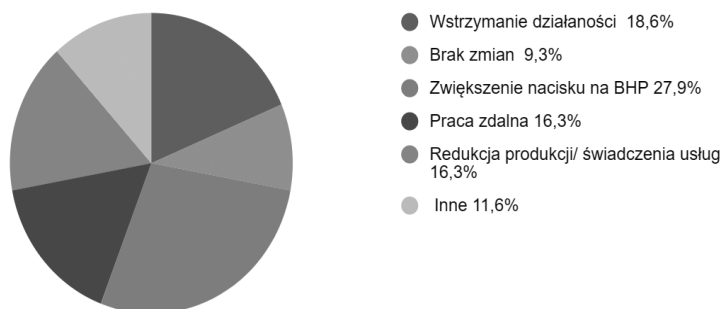
Rys. 8. Obecne priorytety dla przedsiębiorstwa



Źródło: Opracowanie własne.

Na pytanie wielokrotnego wyboru o treści: „Co w obecnej sytuacji jest najważniejsze dla Państwa przedsiębiorstwa?” 66% respondentów wskazało utrzymanie płynności finansowej, 46% – przychodów na dotychczasowym poziomie, a 36% – utrzymanie dotychczasowych pracowników. Nieco mniej odpowiedzi – 34% – dotyczyło utrzymania udziału na rynku. Należy podkreślić, że utrzymanie płynności finansowej ma wpływ na pozostałe aspekty (odpowiedzi).

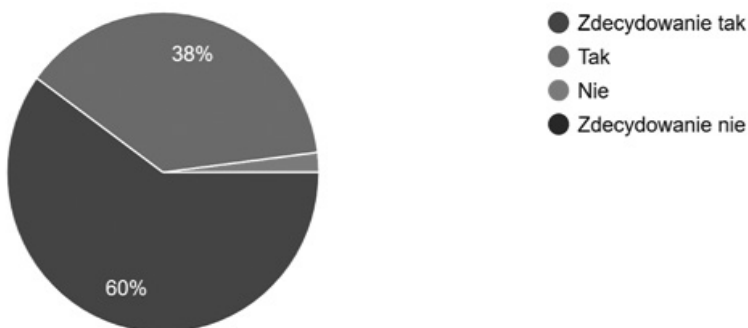
Rys. 9. Zmiany wprowadzone w funkcjonowaniu przedsiębiorstwa



Źródło: Opracowanie własne.

Zmiany wprowadzane w firmach podczas panowania pandemii były zróżnicowane. Z perspektywy przedsiębiorców najważniejsze zmiany zaszły w zakresie BHP (27,9%). Z jednej strony wynikało to z wymogów prawnych, z drugiej przedsiębiorcy zapewne dostrzegli, że zwiększenie nacisku na bezpieczeństwo i higienę pracy jest również w ich interesie. Niestety spora część odpowiedzi dotyczyła wstrzymania działalności. Przejście na pracę zdalną oraz redukcja produkcji lub świadczenia usług były na tym samym poziomie – 16,3%. Należy podkreślić, że wstrzymanie działalności oraz praca zdalna mają zbliżone wartości. Są jednak rozwiązaniami z dwóch odmiennych biegunów. Tam, gdzie nie dało się stosować pracy zdalnej, przedsiębiorcy ograniczali działalność lub ją zawieszali.

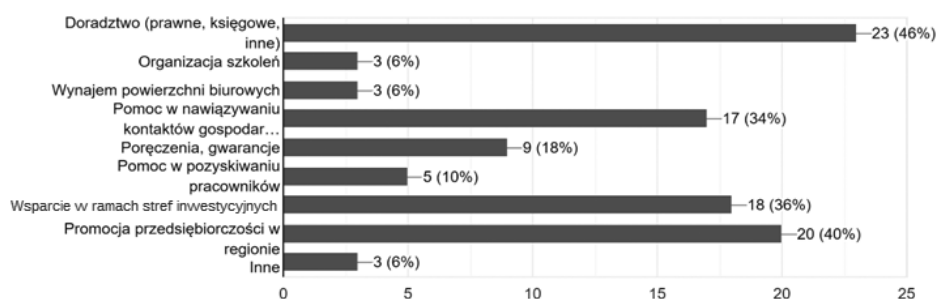
Rys. 10. Respektowanie zmian w przedsiębiorstwie przez pracowników



Źródło: Opracowanie własne.

W odpowiedzi na pytanie: „Czy pracownicy respektują zmiany wprowadzone w Państwa przedsiębiorstwie?” 98% wskazało odpowiedź twierdzącą. Tylko 2% firm udzieliło odpowiedzi negatywnych.

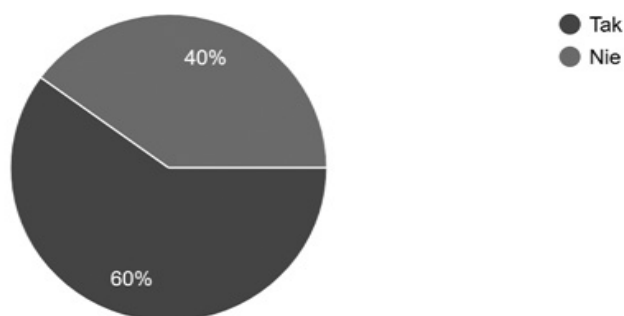
Rys. 11. Rodzaj wsparcia, którego przedsiębiorcy oczekują od JST



Źródło: Opracowanie własne.

Badanie wykazało, że na pytanie (wielokrotnego wyboru) dotyczące wsparcia oczekiwanego od JST najczęściej respondentów (46%) wskazała na doradztwo (prawne, księgowe, inne). Kolejnymi formami pomocy oczekiwanymi przez firmy są promocja przedsiębiorczości w regionie (40%) doradztwo i wsparcie w ramach stref inwestycyjnych (odpowiedzi na poziomie 36%). Pomocy w nawiązywaniu kontaktów gospodarczych oczekuje 34% badanych. Dziesięć procent przedsiębiorców liczy na pomoc w pozyskiwaniu pracowników. Typy wsparcia, na które oczekuje 18% badanych, to poręczenia, gwarancje. Sześć procent spośród ankietowanych chciałoby uzyskać wsparcie w organizacji szkoleń, taka sama ilość odpowiedzi przypada na wynajem powierzchni biurowych oraz odpowiedź „inne”. Reasumując, pomoc w zakresie doradztwa okazała się najbardziej oczekiwanym wsparciem przez przedsiębiorców.

Rys. 12. Korzystanie przez firmę z rozwiązań z „Tarczy Antykryzysowej”



Źródło: Opracowanie własne.

Większość respondentów (60%) postanowiła lub planowała skorzystać z rozwiązań proponowanych przez rządową Tarczę Antykryzysową. Może to wynikać z faktu, że 2/3 badanych stanowili mikroprzedsiębiorcy. Wśród najczęściej wpisywanych rozwiązań możemy wymienić: możliwość trzykrotnej wypłaty świadczenia postojowego, zwolnienia z zapłaty ZUS czy wsparcia finansowego w ramach tzw. Tarczy Finansowej. Niektóre firmy skorzystały również z „Pożyczki dla mikroprzedsiębiorców”, która umożliwiła im pokrycie bieżących kosztów prowadzenia działalności gospodarczej (np. podatków, składek czy kosztów wynajmu lokalu).

Ustawa przewiduje również możliwość skorzystania z dofinansowania części kosztów prowadzenia działalności gospodarczej w przypadku obniżenia obrotów w wyniku pandemii koronawirusa. Dofinansowania są wypłacane w okresach miesięcznych po złożeniu przez przedsiębiorcę oświadczenia o prowadzeniu działalności w danym miesiącu, za który dofinansowanie jest wypłacane. Wsparcie może być przyznane na okres nie dłuższy niż trzy miesiące. Również zwolnienia ze składek ZUS obejmują trzy miesiące (marzec, kwiecień, maj), co oznacza, że składki nie będą płacone od kwietnia do czerwca 2020 r. Zwolnienie od opłacania składek będzie realizowane w formie ich umorzenia²¹. Pośród firm wypełniających ankietę znalazły się również przedsiębiorstwa (40%), które nie skorzystały z Tarczy Antykryzysowej z powodu niespełnienia wymagań.

²¹ <https://www.gov.pl/web/rodzina/tarcza-antykryzysowa-przewodnik-po-rozwiazaniach-dla-przedsiębiorców-i-pracowników> (dostęp: 16.05.2020).

Podsumowanie

Epidemia COVID-19 przyniosła wiele zmian w zakresie organizacji przedsiębiorstw. Wyniki przeprowadzonego badania potwierdzają, że pandemia wpłynęła na bezpieczeństwo ekonomiczne firm, głównie na prognozowane przychody. Jednocześnie perspektywa czasowa badań skłania autorów pracy do weryfikacji tychże prognoz. Jednym z najważniejszych problemów dla pracodawców jest utrzymanie płynności finansowej oraz poziomu zatrudnienia. Odpowiedzi respondentów potwierdzają nasze obserwacje związane z koniecznością wprowadzenia zmian w przedsiębiorstwach. Wyniki badania wskazują, że przejście na pracę zdalną okazało się najczęstszym rozwiązaniem wybieranym przez przedsiębiorstwa. Wiązało się to z inwestowaniem środków w odpowiednie rozwiązania technologiczne.

Odpowiedzi respondentów wskazują, iż wielu z nich (60%) postanowiło skorzystać z Tarczy Antykryzysowej, która pozwalała na przetrwanie ich biznesu w czasie pandemii. Największym wsparciem okazał się ratunek finansowy. Wiele osób preferowało pożyczki bądź zwolnienia ze składek ZUS, co w dużym stopniu usprawniło ich organizację. Inne przedsiębiorstwa przetrwały ten czas poprzez zwalnianie pracowników, co równało się ze zmniejszeniem kosztów lub sprawniejszym przejściem na tryb pracy zdalnej. Przejście na taki tryb pracy łączy się z wprowadzeniem określonych zmian do regulaminów pracy. Przedsiębiorcy kładą większy nacisk na procedury BHP, aby w pełni dbać o bezpieczeństwo swoje, pracowników oraz klientów.

Ryzykiem są między innymi opóźnienia i przerwy w dostawach produktów, drastyczne zmiany popytu ze strony konsumentów, znacznie zwiększone koszty, jak i opóźnione zamówienia. Nie lada wyzwanie stanowią również w czasie pandemii kwestie logistyczne.

W celu reagowania na nowo powstające problemy firmy powinny tworzyć odpowiedzialne za to zespoły. Ponadto powinny opracować cele i plan awaryjny. Dzięki temu możliwe będzie jak najtrafniejsze podejmowanie decyzji w różnych sytuacjach. Umiejętności zawodowe członków wspomnianych zespołów powinny być oceniane przez kierownictwo firmy. W momencie, kiedy firma sama nie poradzi sobie z zaistniałą sytuacją, powinna zatrudnić odpowiednich specjalistów, których kompetencje pozwolą znaleźć inne rozwiązania powstałych problemów i poprawić działanie firmy.

W przypadku braku planu należy od razu dokonać konkretnej oceny wszystkich obszarów ryzyka. Obejmuje to zakres pracowników, outsourcingu, łańcucha dostaw oraz działań związanych z komunikacją. Firma jest zobowiązana podjąć odpowiednie działania dotyczące miejsca pracy, planów produkcji, zaopatrzenia, dostaw, logistyki, bezpieczeństwa personelu oraz kapitału finansowego. Powinna opracować skuteczne rozwiązania planów awaryjnych i odpowiedni podział pracy.

Zdecydowana większość analizowanych firm (ponad 90%) wprowadziła zmiany w swoim funkcjonowaniu. Wśród „pozytywnych” zmian znalazło się podniesienie poziomu BHP oraz przejście na pracę zdalną (tam gdzie było to możliwe). Wśród „negatywnych” wskazano na redukcję produkcji/świadczenia usług oraz wstrzymanie działalności firmy. Budującym jest fakt, że prawie wszyscy pracownicy (98%) respektowali wprowadzone zmiany.

Bibliografia

- Baturo W., *Katastrofy i zagrożenia we współczesnym świecie*, Wydawnictwo Naukowe PWN, Warszawa 2008.
- Bralewski A., *Zagrożenie bezpieczeństwa ekonomicznego Polski*, „Zeszyty Naukowe SGSP” 2018, nr 68/4, Warszawa 2018.
- Chepik O., Mishanova E., Kalinina G., Gracheva A., *Economic Security of Economic Entities in Crises*, w: Gimbatov Sh., Abdulaeva Z., Bashirova A., Denevizuk D., *Proceedings of the VIII International Scientific and Practical Conference “Current problems of social and labour relations” (ISPC-CPSLR 2020)*, „Advances in Social Science, Education and Humanities Research” 2021, vol. 527.
- Duława J., *Vademecum medycyny wewnętrznej*, PZWL Wydawnictwo Lekarskie, Warszawa 2015.
- Michałowska M., Stankiewicz D., Danielak W., *Zarządzanie sytuacją kryzysową w przedsiębiorstwie*, „Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze” 2015, nr 2, Zielona Góra 2015.
- Wawrzusiszyn A., *Pojęcie i istota bezpieczeństwa*, w: Stawnicka J., Wiśniewski B., Socha R. (red.), *Zarządzanie kryzysowe. Teoria, praktyka, konteksty, badania*, Wydawnictwo Wyższej Szkoły w Szczytnie, Szczytno 2011.

Wróblewski D. (red.), *Zagadnienia ogólne z zakresu zarządzania ryzykiem i zarządzania kryzysowego analiza wybranych przepisów*, Centrum Naukowo-Badawcze Ochrony Przeciwpowodzi, Józefów 2014.

<https://rcb.gov.pl/zarzadzanie-kryzysowe/> (dostęp: 30.06.2021).

<http://www.gov.pl/web/zdrowie/pierwszy-przypadek-koronawirusa-w-polsce> (dostęp: 30.06.2021).

<http://gov.pl/web/mswia/rzadowy-zespol-zarzadzania-kryzysowego-podjal-decyzje-o-odwolaniu-impres-masowych> (dostęp: 30.06.2021).

<http://www.hellozdrowie.pl/koronawirus-w-polsce-stwierdzono-pierwszy-smiertelny-przypadek-zakazenia-wirusem-sars-cov-2/> (dostęp: 30.06.2021).

Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. 2020 poz. 1842).

Ustawa dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst ujednolicony: Dz.U. 2007 nr 89 poz. 590, z późn. zm.).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2020 r. w sprawie przywrócenia tymczasowo kontroli granicznej osób przekraczających granicę państwową stanowiącą granicę wewnętrzną (Dz.U. 2020 poz. 434).

Rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz.U. 2020 poz. 491).

Rozporządzenie Ministra Zdrowia z dnia 24 marca 2020 r. zmieniające rozporządzenie w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz.U. 2020 poz. 522).

Rozporządzenie Rady Ministrów z dnia 31 marca 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz.U. 2020 poz. 566).

Economic security and crisis management of entrepreneurs in the voivodeship Pomeranian Voivodeship, in the beginning of the coronavirus pandemic

Abstract: The aim of the study is to present the economic situation of entrepreneurs from the Pomeranian Voivodeship in the initial period of the coronavirus pandemic. A survey tool was used in the publication to implement this assumption. They were filled in by entrepreneurs representing mainly service activities. The survey results indicate that entrepreneurs were not properly prepared for the limitations related to the epidemiological situation. Entrepreneurs had to react quickly to keep in business. Some of them benefited from state aid.

The study attempts to diagnose threats to economic security of entrepreneurs at the time of sudden changes in the economy. Companies were forced to make changes in crisis situations. It is important that entrepreneurs, mainly those who start running a business, systematically focus on the risk area. The publication draws attention to aspects which, if omitted, may lead to the loss of stability of the company in crisis situations.

Key words: COVID-19, economic security, entrepreneur, lockdown in Poland

dr Mariola Bartusek

Śląski Uniwersytet Medyczny w Katowicach
Wydział Nauk o Zdrowiu, Katedra Pielęgniarstwa
Zakład Pielęgniarstwa i Społecznych Problemów Medycznych
e-mail: mbartusek@sum.edu.pl
ORCID: 0000-0002-8833-8657

Rozdział 4

Bezpieczeństwo i higiena pracy pielęgniarek w czasie trwania pandemii

Streszczenie: Wśród czynników szkodliwych na stanowisku pracy pielęgniarki czynniki biologiczne odgrywają znaczącą rolę. Dzięki wprowadzonym przed laty zmianom, usankcjonowanym prawnie, wykształceniu personelu oraz zastosowaniu wielu specjalistycznych procedur zminimalizowano ryzyko występowania wielu chorób personelu powodowanych tymi czynnikami. Mimo tego pandemia wywołała duże poruszenie w świecie medyków.

Dzięki znajomości procedur postępowania, środkom ochrony indywidualnej oraz działaniu specjalistycznych zespołów dokumentujących zagrożenia i tym razem można było szybko wprowadzić zmiany zapewniające bezpieczeństwo. Jednakże kolejne odsłony pandemii koronawirusa, zachorowania personelu, a często także ich śmierć, zmuszają do podjęcia dyskusji nad dalszym bezpieczeństwem personelu medycznego oraz wyciągnięciem wniosków w kierunku zastosowania innych skutecznych metod.

Słowa kluczowe: ochrona zdrowia pielęgniarek, czynniki szkodliwe, pandemia COVID-19

Wprowadzenie

Pielęgniarki stanowią najliczniejszą grupę zawodową wśród personelu medycznego. Podczas wykonywania zawodu zobowiązane są do ustawicznego kształcenia, wysokiej odpowiedzialności zawodowej, której niedopełnienie skutkować może pozbawieniem prawa wykonywania zawodu.

Bezpieczeństwo i higiena pracy odgrywają bardzo dużą rolę w opiece zdrowotnej, warunkują bowiem nie tylko zdrowie pracownika, ale i pacjentów. Praca pielęgniarek oparta jest na wykonywaniu czynności, które stanowią składową procedurę medycznej, którą wykonują w całości, a także jako zadania w trakcie wykonywania procedury przez innych pracowników medycznych. Przygotowują narzędzia, sprzęt i miejsce do wykonania procedury przez innego pracownika medycznego. Tym samym zapewnienie przez pracodawcę bezpiecznego miejsca pracownikowi pozwala na prowadzenie procedury bez zbędnych utrudnień. Postępowanie takie przyczynia się również do poprawy stanu zdrowia pacjenta, jego ratowania lub umożliwienia powrotu do zdrowia.

Dzięki wprowadzonym przed laty w Polsce zmianom w polityce zdrowotnej, usankcjonowanym prawnie, wysokiemu wykształceniu personelu medycznego oraz zastosowaniu wielu specjalistycznych procedur zminimalizowano ryzyko występowania wielu zagrożeń zdrowotnych w czasie trwania pandemii. Mimo znajomości procedur postępowania, środków ochrony indywidualnej oraz działania specjalistycznych zespołów dokumentujących zagrożenia medykom trudno było odnaleźć się w tak trudnej sytuacji. Ryzyko zakażenia na stanowisku pracy powodowane COVID-19 doprowadziło wielu pracowników medycznych do choroby, nawet do śmierci.

Dotychczasowe zabezpieczenia i ochrona pracownika w czasie poprzedzającym pandemię okazały się niewystarczające po jej nastaniu. Zmusiło to przedstawicieli sektora ochrony zdrowia do wprowadzenia wielu nowych procedur i standardów postępowania. Zmianie uległo wiele przepisów prawnych ważnych nie tylko dla personelu medycznego, ale całego społeczeństwa. Dla pracowników podmiotów działalności leczniczej, zarówno kadry kierowniczej, jak i personelu, który sprawuje bezpośrednią opiekę nad pacjentem czy administruje, wprowadzone zmiany przełożyły się na bezpośrednią pracę. Wymagała ona odtąd bieżącej weryfikacji szybko zmieniających się przepisów, wytycznych i zaleceń, większej koncentracji ze względu na szczegółowe wytyczne oraz

większego nakładu pracy i sił, powodowanych zmniejszającą się w szybkim tempie liczbą personelu.

Celem niniejszego artykułu jest omówienie warunków pracy pielęgniarek z próbą zdefiniowania podstawowych czynników wpływających w negatywny sposób na ich stan zdrowia. Identyfikacja tych czynników przed pandemią, a następnie w czasie jej trwania pozwala na zwrócenie uwagi na prawidłowe, bezpieczne i higieniczne warunki pracy pielęgniarek. Warunki pracy personelu medycznego w czasie pandemii są bowiem odmienne od tych, jakie występowały przed nią. W kolejnej części pracy zwrócono zatem uwagę na szczególny charakter ochrony pielęgniarek w czasie trwania pandemii. Ze względu na liczne problemy występujące od lat w sektorze ochrony zdrowia zabezpieczenie to w minionym okresie było niewystarczające. Negatywnym skutkiem były liczne zachorowania i śmierć personelu medycznego spowodowane zakażeniem koronawirusem.

Ochrona pracowników medycznych w czasie ich pracy zawodowej jest jednym z obowiązków pracodawcy, a co za tym idzie przedstawicieli sektora. To w gestii dysponentów środków finansowych leży podjęcie kolejnych decyzji zabezpieczających personel. Mimo iż prezentowana publikacja obejmuje zakres wykonywania zawodu przez pielęgniarki, przekłada się również na bezpieczeństwo całego personelu medycznego. Biorąc pod uwagę odpowiedzialność medyków za zdrowie i życie społeczeństwa, warto podjąć starania, by ochrona personelu była jak największa.

Poniższa analiza opiera się na obowiązujących wymogach prawnych, standardach i procedurach oraz zasadach postępowania.

Czynniki szkodliwe na stanowisku pracy pielęgniarki

Efektywność pracy pielęgniarek warunkowana jest wieloma czynnikami. Wśród nich wyróżnia się m.in. sprzęt i aparaturę medyczną, przedmiot i podmiot opieki oraz współpracowników. Optymalizacja współdziałania tych czynników sprzyja racjonalnej pracy, a bezpieczne warunki i środowisko pracy, w tym współpraca między zespołami, przyczyniają się jej efektywności¹. Praca

¹ G. Gawęł *Obciążenie na pielęgniarskich stanowiskach wynikających z narażenia na czynniki środowiska pracy*, w: Zarządzanie w pielęgniarstwie. Podręcznik dla studentów studiów magisterskich Wydziałów Pielęgniarstwa oraz Wydziałów Nauk o Zdrowiu. Pod red. A. Ksykiewicz-Doroty. Wydawnictwo PZWL Warszawa 2013, s. 439.

na stanowisku pielęgniarki obciążona jest licznymi czynnikami, które mają szkodliwy wpływ na stan zdrowia. W efekcie działanie czynników mających negatywny wpływ na stan zdrowia pielęgniarek doprowadzić może do obniżenia ich efektywności poprzez przyczynianie się do uciążliwości wykonywanej pracy. Wynikiem takich sytuacji może być wywołanie jednej z chorób uznanych za zawodową². Wśród czynników, jakie pojawiają się na stanowisku pracy pielęgniarek, a których oddziaływanie ma wpływ na stan zdrowia pielęgniarek, pojawiają się także te uznawane za niebezpieczne oraz uciążliwe. Za czynnik niebezpieczny uznaje się czynnik doprowadzający u pielęgniarki np. do urazu lub zatrucia. Czynnik uciążliwy natomiast prowadzi do wielu objawów niemierzalnych, np. zmęczenia, przeciążenia czy choroby³.

Definiując obciążenie pracą jako stopień zaangażowania pracownika w wykonywanie zadań, można dokonać klasyfikacji czynników obciążających pielęgniarkę na stanowisku pracy, dzieląc je na: materialne warunki pracy, rodzaj pracy, jaka jest wykonywana, specyfika wykonywanych zadań związanych z pełnieniem przez pielęgniarkę określonej roli, relacje interpersonalne, kultura organizacyjna oraz ścieżka kariery zawodowej pielęgniarek i położnych. Czynniki biologiczne wraz z czynnikami chemicznymi, fizycznymi oraz społecznym środowiskiem pracy należą do pierwszej grupy, tj. materialnego środowiska pracy⁴. Czynniki biologiczne, do których zalicza się drobnoustroje komórkowe, pasożyty, organizmy bezkomórkowe zdolne do przenoszenia materiału genetycznego, w tym też te, które zostały zmodyfikowane genetycznie, doprowadzają często do zakażeń, stanów alergicznych oraz zatrucia. Mikroorganizmy i makroorganizmy oraz substancje przez nie wytwarzane są bardzo często powodem występowania jednostek chorobowych, u podłoża których leżą alergie, czynnik toksyczny lub nawet nowotworowy. Przyczyną chorób występujących u pielęgniarek mogą być jednak tak naprawdę wszystkie czynniki chorobotwórcze, jako że kontakt z nimi pracownicy mają nieograniczony. Do niedawna zakażenie wirusem zapalenia wątroby typu B i C oraz wirusem HIV

² E. Kuriata i in., *Rozpoznawanie przez pielęgniarki szkodliwych czynników chemicznych i fizycznych na stanowiskach pracy w szpitalu*, „Family Medicine & Primary Care Review” 2012, vol. 14/1, s. 29–36.

³ G. Gaweł, *Obciążenie...*, dz. cyt., s. 439.

⁴ G. Gaweł *Obciążenia na pielęgniarskich stanowiskach pracy*, w: Podstawy organizacji pracy pielęgniarskiej. Podręcznik dla studentów studiów licencjackich Wydziałów Pielęgniarstwa oraz Wydziałów Nauk o Zdrowiu, pod red. A. Ksykiewicz-Doroty, Wydawnictwo Czelej, Lublin 2004, s. 110–111.

były wiodącymi wśród chorób występujących u pielęgniarek na skutek działania czynników biologicznych na stanowisku pracy⁵.

Ze względu na wagę uszkodzeń, jakie wywołują czynniki biologiczne, warunki pracy regulowane są postanowieniem „Dyrektywy 2000/54/WE Parlamentu Europejskiego i Rady z dnia 18.09.2000 w sprawie w sprawie ochrony pracowników przed ryzykiem związanym z narażeniem na działanie czynników biologicznych w miejscu pracy (siódma dyrektywa szczegółowa w rozumieniu art. 16 ust. 1 dyrektywy 89/391/EWG) (Dz. Urz. WE L 262 z 17.10.2000, str. 21; Dz. Urz. UE Polskie wydanie specjalne rozdz. 5, t. 4, str. 48)”⁶. Podstawę w Polsce stanowi Ustawa Kodeks Pracy⁷ oraz akt wykonawczy w postaci Rozporządzenia Ministra Zdrowia z dnia 22.04.2005 w sprawie szkodliwych czynników biologicznych dla zdrowia w środowisku pracy oraz ochrony zdrowia pracowników zawodowo narażonych na te czynniki, ogłoszone 11.05.2005 r.⁸

Od 29 grudnia 2020 r. obowiązują nowe zapisy zmieniające dotychczasowe wytyczne⁹. Rozporządzenie prezentuje wykaz biologicznych czynników szkodliwych, prace, podczas wykonywania których dojść może do zakażenia, określa szczegółowo zakres ochrony pracowniczej oraz podaje środki celem zapewnienia odpowiedniej ochrony osób narażonych na ich działanie. Ponadto ustala wykonanie i prowadzenie przez pracodawcę rejestru prac, w których występuje narażenie na działanie czynników biologicznych, oraz pracowników na to zakażenie narażonych wraz ze sposobem ich ochrony¹⁰. Załącznik nr 1 Rozporządzenia dokonuje klasyfikacji szkodliwych czynników biologicznych. Grupa pierwsza obejmuje czynniki, które w małym stopniu zagrażają ludziom, do grupy drugiej należą czynniki, które mogą wywołać zakażenie u ludzi, jednak rozprzestrzenienie się zakażenia w populacji jest mało prawdopodobne. Grupa trzecia czynników zagrożenia obejmuje takie, które mogą doprowadzić

⁵ A. Frąckowiak, *Zagrożenia w pracy pielęgniarki środowiskowej*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach” 2010, nr 1(6), s. 56.

⁶ *Rozporządzenie Ministra Zdrowia z dnia 22.04.2005 w sprawie szkodliwych czynników biologicznych dla zdrowia w środowisku pracy oraz ochrony zdrowia pracowników zawodowo narażonych na te czynniki* (Dz.U. z 2005 nr 81, poz. 716 z późn. zm.). Źródło: <http://www.przepisy.gofin.pl/przepisy,4,18,39,335,,20201229,rozporzadzenie-ministra-zdrowia-z-dnia-22042005-r-w-sprawie.html> (dostęp: 29.05.2021).

⁷ Kodeks Pracy Art. 222¹ § 3 ustawy z dnia 26 czerwca 1974 r. (Dz.U. z 1998 r. nr 21, poz. 94, z późn. zm.).

⁸ *Rozporządzenie Ministra Zdrowia...*, dz. cyt.

⁹ Tamże.

¹⁰ Tamże.

do ciężkich chorób u ludzi i jednocześnie mogą rozprzestrzeniać się w populacji. Natomiast grupa czwarta to czynniki o najcięższych skutkach dla ludzi, bowiem nie tylko może dojść do ciężkich chorób i rozprzestrzeniania się w populacji, ale niestety z reguły nie ma przeciw nim skutecznych środków profilaktycznych¹¹.

W obliczu trwającej pandemii bardzo istotne stało się określenie ryzyka zakażenia koronawirusem, ustalając, iż będzie czynnikiem zakażenia grupy trzeciej, określanym zespołem ostrej niewydolności oddechowej¹². Tym samym zagrożenie koronawirusem uznane zostało jako czynnik zawodowy szkodliwy na stanowisku pracy. Grupa pracowników medycznych, w tym również pielęgniarki, narażona na czynniki biologiczne, uznana została za tę, która na stanowisku pracy ma dodatkowy czynnik szkodliwy dla zdrowia. To bardzo ważne dla przyszłości zdrowia personelu medycznego, któremu z tego tytułu przysługiwać będzie dodatkowa ochrona i rekompensata finansowa za trud warunków pracy.

Bezpieczeństwo i higiena pracy pielęgniarek

Bezpieczeństwo pracy pielęgniarki, bez względu na to, gdzie usytuowane jest jej stanowisko, odzwierciedla obowiązujące wymogi prawne. Ponadto Państwowa Inspekcja Pracy w karcie „Bezpiecznej Pracy w zawodzie pielęgniarki” zebrała i uporządkowała najważniejsze wytyczne. Przekazując informacje o warunkach bezpiecznej pracy, możliwościach jego zorganizowania oraz organizacji pracy, daje pracodawcom i pracownikom podstawy warunkujące stabilizację pracowników w zakresie bezpieczeństwa pracy¹³. Praca pielęgniarki po wielokroć nosi znamiona pracy umysłowej i fizycznej. Podczas wykonywania zadań pielęgniarka wykazać się musi ogromną wiedzą, samodyscypliną i koncentracją. Bardzo często dochodzi też do wysiłku fizycznego powodowanego np. zmianą pozycji chorego, jego przemieszczaniem czy obracaniem. Wykonując wiele

¹¹ Tamże.

¹² *Szkodliwe czynniki biologiczne – zmiany dla pracodawców*, 22.01.2021, <https://www.ca-staff.eu/publikacje/szkodliwe-czynniki-biologiczne-zmiany-dla-pracodawcow> (dostęp: 29.05.2021).

¹³ P. Rozowski, *Bezpieczna praca w zawodzie pielęgniarki*, PIP, Wyd. 1/2019, s. 1–3, pip.gov.pl/pl/f/v/228249/bezpieczna%20praca%20w%20zawodzie%20pielęgniarki.pdf (dostęp: 28.05.2021).

zadań, pielęgniarka obciąża w szczególności układ kostno-stawowy, a ponadto jest bezpośrednio narażona na inne czynniki, m.in. biologiczne¹⁴.

Na stanowisku pracy pielęgniarki rozpoznawanych jest wiele czynników szkodliwych, których skutki wpływają negatywnie na ich stan zdrowia. Zdarza się, iż na początku ich występowania i oddziaływania na człowieka doprowadzają do występowania niespecyficznych objawów, np. obniżonej satysfakcji osobistej, objawów ze strony układu pokarmowego czy krążenia¹⁵. Ze względu na bezpośredni kontakt z chorym, a przez to z materiałem zakaźnym, pielęgniarki są bardzo narażone na zakażenia i ich skutki. Do zakażenia dochodzi podczas wykonywania zadań, procedur medycznych bądź przy ich przygotowywaniu lub porządkowaniu po wykonaniu. Do zakażenia dochodzi wówczas przez kontakt z przedmiotami lub narzędziami, które były wykorzystywane w pracy z chorym¹⁶.

Zgodnie z definicją ryzyka zawodowego, które rozumiane jest jako „prawdopodobieństwo wystąpienia niepożądanych zdarzeń związanych z wykonywaną pracą powodujących straty, w szczególności wystąpienia u pracowników niekorzystnych skutków zdrowotnych w wyniku zagrożeń zawodowych występujących w środowisku pracy lub sposobu wykonywania pracy (Polska Norma PN-N-18002)”¹⁷, mocą Rozporządzenia Ministra Zdrowia z dnia 14 grudnia 2020 r. pracodawcy zobligowani zostali do aktualizacji oceny ryzyka zawodowego, na jakie może być narażony pracownik, albo które potencjalnie może mu grozić, przy wykorzystaniu klasyfikacji i wykazu czynników szkodliwych zawartych w załącznikach Rozporządzenia. Tym samym w czasie 30 dni od wejścia w życie wspomnianego dokumentu miano dokonać wprowadzenia zmian w zakresie uwzględnienia koronawirusa zespołu ostrej niewydolności oddechowej 2 (SARS-CoV-2). Zapis ten pozwolił m.in. na zastosowanie większej ochrony pracownika będącego w stanie narażenia zdrowia i życia na wirus¹⁸. Również w pozostałych przypadkach, kiedy do zachorowania do-

¹⁴ K. Kulczycka, M. Grenda, E. Stychno, *Trudności w wykonywaniu pracy na stanowisku pielęgniarki pediatrycznej*, „Journal of Education, Health and Sport” 2016, vol. 6(10), s. 90–108.

¹⁵ K. Kowalczyk i in., *Zagrożenia zawodowe pielęgniarek, położnych i lekarzy w środowisku pracy*, „Problemy Higieny i Epidemiologii” 2008, nr 89(2), s. 211–215.

¹⁶ P. Rozowski, *Bezpieczna praca...*, dz. cyt.

¹⁷ *O ocenie ryzyka zawodowego. Informacja wprowadzająca*, <https://www.pip.gov.pl/pl/bhp/ocena-ryzyka-zawodowego/o-ocenie-ryzyka-zawodowego/6256,o-ocenie-ryzyka-zawodowego-informacja-wprowadzajaca.html> (dostęp: 28.05.2021).

¹⁸ *Rozporządzenie Ministra Zdrowia...*, dz. cyt.

chodzi na skutek zakażenia czynnikiem biologicznym, szczególnie ważna jest profilaktyka. Skuteczną ochronę pracowników przed zakażeniami stanowią szczepienia. Są one podstawowym ogniwem łańcucha epidemiologicznego w zapobieganiu szerzenia się zakażeń. Istotne jest, że ich regularne stosowanie na populacji doprowadza do zahamowania powstawania nowych zakażeń. To m.in. poprzez wprowadzenie obowiązku szczepień ochronnych zmniejszono bądź wykluczono występowanie niektórych chorób, np. błonicy czy krztuśca. Światowa Organizacja Zdrowia sygnalizuje, że wielomilionowa populacja ludzi została uratowana dzięki zwiększeniu odporności nabytej dzięki szczepieniom. Niezwykle istotne jest wykorzystanie tej wiedzy w kontekście ochrony pracowników narażonych na szkodliwe działanie czynników biologicznych¹⁹.

Zdaniem Konsultanta Krajowego w dziedzinie pielęgniarstwa epidemiologicznego w roku 2017 istota szerokiego wpływu szczepień na populację ma znaczenie niejako z dwóch powodów. Dr n. med. Beata Ochocka wskazywała: „pomimo że żyjemy w czasach, w których dokonał się wielki postęp medycyny, obserwujemy zjawisko powrotu tzw. starych chorób zakaźnych, jak i pojawienie się jednostek nowych, często bardziej niebezpiecznych”²⁰.

Oprócz szczepień personel medyczny zobowiązany jest do przestrzegania procedur ogólnych, stanowiących niejako bazę do bezpiecznej platformy wykonywania zadań. Wśród nich na uwagę zasługuje komputerowy system zarządzania, w tym zarządzania materiałami sterylnymi, współpraca centralnej sterylizatorni z poszczególnymi oddziałami i blokiem operacyjnym, przestrzeganie zasad podczas mycia i dezynfekcji sprzętu, narzędzi czy też właściwe postępowanie z materiałem przed i po sterylizacji²¹.

Jak w każdym zakładzie pracy, pielęgniarkę obowiązuje szereg badań, m.in. przed przyjęciem do pracy, badania okresowe czy badania po dłuższej nieobecności w pracy. Tym samym zobligowana jest do dbania o własne zdrowie, które stanowi istotny czynnik również w walce o zdrowie i życie pacjenta. Niezwykle ważne jest, że pielęgniarki są zobligowane do postępowania zgodnego z zasadami etyki zawodowej, co w połączeniu z ogromną samodyscypliną i odpowiedzialnością zawodową nie pozwala na ukrywanie choroby. W takim przypadku

¹⁹ J. Walusiak-Skorupa, *Profilaktyka chorób zakaźnych – kierunek dla zbudowania zdrowego miejsca pracy*, „Pielęgniarka Epidemiologiczna” 2017, nr 4(71), s. 29.

²⁰ B. Ochocka, *Z doświadczenia praktyków*, „Pielęgniarka Epidemiologiczna” 2017, nr 4(71), s. 30.

²¹ B. Próchnicka, *Współpraca bloku operacyjnego i centralnej sterylizatorni a nadzór nad zakażeniami szpitalnymi*, „Pielęgniarka Epidemiologiczna” 2017, nr 4(71), s. 22.

bowiem choroba pielęgniarki mogłaby przyczynić się do pogorszenia stanu zdrowia pacjenta. W czasie pandemii personel medyczny jest szczególnie uwrażliwiany na występowanie takich objawów jak bóle głowy, gardła, bóle mięśniowe, kaszel, katar, gorączka, zmęczenie czy biegunki, które każdorazowo są weryfikowane pod kątem możliwości zakażenia się koronawirusem²². Niektóre z objawów pojawiają się nagle, inne w łagodny, nie niepokojący sposób. Dlatego wartość etycznego postępowania pielęgniarek, wzmacniana zapisami Kodeksu etyki zawodowej, nie pozwala pielęgniarce na bagatelizowanie objawów²³.

Kiedy w grę wchodzi życie ludzkie, wszyscy muszą dołożyć starań, by je chronić. W placówkach opieki medycznej od wielu lat jest ogromny deficyt personelu. Braki pielęgniarek sygnalizowane od dawna wymagają dobrze przygotowanej strategii uzupełnienia niedoborów. W przeciwnym razie już niebawem dojdzie do utrudnień w funkcjonowaniu podmiotów działalności leczniczej.

Bezpieczeństwo pielęgniarek w czasie pandemii

Karta „Bezpiecznej pracy w zawodzie pielęgniarki” wskazuje ponadto sposoby przeciwdziałania zakażeniom wirusami, bakteriami i drobnoustrojami chorobotwórczymi. Przed wykonywaniem jakichkolwiek zadań pielęgniarka zobowiązana jest umyć ręce ciepłą wodą z mydłem. Następnie do wykonania zadania należy założyć rękawiczki. Pomiędzy zabiegami dobrze po umyciu rąk stosować kremy ochronne, a w przypadku jakiegokolwiek skałeczenia ranę zdezynfekować, a miejsce zranione zabezpieczyć przed zabrudzeniem. Wszystkie zranienia, uszkodzenia i przerwania ciągłości skóry należy zgłosić wskazanej w zakładzie osobie odpowiedzialnej za bezpieczeństwo i higienę pracy w zakładzie²⁴. Zgodnie z procedurami przysyłać należy do sterylizacji wszystkie narzędzia wymienione w procedurach. Igły i strzykawki powinny być wyłącznie jednorazowego użytku. Po wykorzystaniu należy umieszczać je w pojemnikach do tego odpowiednio przygotowanych, zamykanych oraz oznakowanych. Wykonując zadania w środowisku narażonym na czynniki biologiczne rozprzestrzeniające się drogą powietrzną, pielęgniarki zobligowane

²² M. Tomaszewska-Kowalska, A. Balas, *Koronawirus – bądź odpowiedzialny*, „Pielęgniarka Epidemiologiczna” 2020, nr 2(80), s. 8.

²³ *Kodeks Etyki Zawodowej Pielęgniarki i Położnej Rzeczypospolitej Polskiej*, źródło: <https://nipip.pl/prawo/samorzadowe/krajowy-zjazd-pielęgniarek-i-polozonych/kodeks-etyki-zawodowej-pielęgniarki-i-polozonej-rzeczypospolitej-polskiej>.

²⁴ P. Rozowski, *Bezpieczna praca...*, dz. cyt.

są do stosowania maseczek ochronnych, półmasek lub masek filtrujących. Ciało pielęgniarki powinno zostać ponadto osłonięte odzieżą ochronną, najlepiej jednorazowymi kombinezonami. W normalnym trybie podczas pracy np. na blokach operacyjnych, oddziałach OIOM, hemodializ, oddziałach zakaźnych czy pulmonologicznych itp. odzież ochronna jednorazowa po wykonaniu procedury wyrzucana jest do odpowiednich, oznakowanych pojemników. Pozostała odzież pracownicza przechowywana jest oddzielnie od odzieży prywatnej.

W uzasadnionych przepisami przypadkach pracownik może zostać poddany szczepieniom ochronnym²⁵. Pomimo dużej skuteczności szczepień, procedur skoordynowanych i kompleksowych, nie można jednak bagatelizować mycia i dezynfekcji rąk, od których wszystko się zaczyna. Zakażenia wirusem SARS-CoV-2 przyczyniły się w dużej mierze do zwiększenia aktywności pracowników w tym zakresie, dodatkowo zwracając uwagę na konieczność zmiany preparatów do dezynfekcji. Ponadto zalecenia Światowej Organizacji Zdrowia i wytyczne Departamentu Zdrowia zwracają uwagę, iż mycie nie tylko usuwa mechanicznie istniejące zabrudzenia, ale w połączeniu ze skuteczną dezynfekcją wpływa na obniżenie prognozy przenoszonych zakażeń²⁶.

Dezynfekcja jest procesem, który eliminuje drobnoustroje w 99,99%. Skuteczność ta wynika z prawidłowo przeprowadzonej dezynfekcji, a mianowicie polegającej na minimum 30-sekundowej dezynfekcji rąk, preparatem w ilości 3 ml, przy czym zawartość alkoholu etylowego lub izopropylowego nie może być mniejsza niż 60% i nie większa niż 75%. Pozytywne efekty dezynfekcji widać m.in. w spadku zachorowań na grypę oraz WZW typu A, zwanego chorobą brudnych rąk²⁷. Ze względu na transmisję wirusa duże znaczenie ma również dezynfekcja powierzchni, na której np. przygotowywane zostają narzędzia, leki itp. Pozwala to na stwierdzenie, iż odpowiednie zabezpieczenie powierzchni skutecznie chroni pielęgniarkę przed zakażeniem. Z międzynarodowych badań wynika, że trwałość koronawirusa na różnych powierzchniach wynosi od dwóch godzin do dziewięciu dni, co staje się jednym z najmniejbezpieczniejszych czynników dla personelu medycznego²⁸.

²⁵ Tamże.

²⁶ P. Żbikowski, *Dezynfekcja rąk i powierzchni oraz antyseptyka błon śluzowych w dobie pandemii COVID-19*, „Pielęgniarka Epidemiologiczna” 2021, nr 1(83), s. 12–13.

²⁷ W. Ferschke, *Skuteczna dezynfekcja tarczą ochronną przeciw koronawirusowi*, „Pielęgniarka Epidemiologiczna” 2021, nr 1(83), s. 11.

²⁸ P. Żbikowski, *Dezynfekcja rąk...*, dz. cyt., s. 15–16.

W czasie trwania pandemii w placówkach opieki zdrowotnej wprowadzone zostały szczególne zasady postępowania. Wśród nich na uwagę zasługują „Zasady i organizacja bezpiecznej pracy w przypadku rozprzestrzeniania się infekcji COVID-19”. Zgodnie z wytycznymi podane zostały kolejne kroki postępowania personelu medycznego. Ich przestrzeganie daje pielęgniarkom szansę na bezpieczną pracę. Podane wskazania do postępowania rozpoczynają się od dezynfekcji rąk każdorazowo przed wejściem do holu szpitalnego. Pielęgniarka ponadto musi zmierzyć temperaturę, ocenić swój stan zdrowia pod kątem zagrożenia infekcją COVID-19 i przy jakichkolwiek wątpliwościach zgłosić je przełożonemu. W dalszej kolejności następuje założenie odzieży ochronnej, używanej tylko w zakładzie pracy. Odzież ta winna być codziennie zmieniana, a w przypadku gdy nie jest to możliwe, powinno się stosować odzież jednorazową. Używana odzież nie może być zabierana do domu. Jedną z ważnych zasad pracy pielęgniarek jest tzw. zasada „nic poniżej łokci”. Oznacza to pracę bez biżuterii i bez używania jakichkolwiek preparatów ozdobnych, np. w postaci lakieru do paznokci. Dezynfekcja rąk następuje według znanego pielęgniarkom schematu Światowej Organizacji Zdrowia. W czasie pracy pielęgniarkom zaleca się niedotykanie ust, oczu, jeśli nie zachodzi ku temu ważna potrzeba. Z pacjentem kontakt winien być bezpieczny, aczkolwiek nie bliski. Pielęgniarka przeprowadza z pacjentami wiele rozmów, jednakże w wyniku istniejącego zagrożenia powinny być one skracane, pacjentów należy zachęcać, by przebywali w sali, skracali czas spacerów po korytarzu i ograniczali kontakt ze współpracownikami. Jeśli w toku wykonywanej pracy jest to możliwe, należy zachować odstęp dwóch metrów. Dodatkowo pielęgniarki obowiązują zasady dodatkowe, np. w pomieszczeniach socjalnych, gdzie zaleca się maksymalnie dwie osoby na pokój, szatnię, dyżurkę itp. Pielęgniarka podejmując pracę, powinna zorganizować też bezpieczne miejsce pracy, tak by sama sobie nie zagrażała zakażeniem. W toku pracy należy bowiem dezynfekować klawiaturę komputera i myszkę, telefon używany też przez inne osoby, stojak do kroplówek czy inne przedmioty. W przypadku sprzętu wykorzystywanego do wykonywania procedur medycznych, tam gdzie to możliwe, należy stosować sprzęt jednorazowy, a wszelkie odpady traktować jak zakaźne. Przy wykonywaniu procedur specjalistycznych z zakładaniem np. dostępu naczyniowego, wykonywaniu EKG, zmianie opatrunku czy toalecie chorego zawsze należy używać masek jednorazowych, przyłbic, rękawic, dokonując weryfikacji, jakich środków należy używać. Jeśli mowa o масечkach, bezwzględnie należy przestrzegać zakrywania nosa, ust,

podbródka. Maseczki nie wolno nosić zawieszanej na szyi czy w jakikolwiek sposób inny niż jest zalecony. Jeśli pielęgniarka obejmuje opieką pacjenta podejrzanego o zakażenie koronawirusem, postępowanie jej musi być zgodne z procedurami izolacji, planem higieny, postępowaniem z bielizną i odpadami²⁹. Zalecenia dla pracowników medycznych objęte są procedurami koniecznymi do stosowania w podmiotach działalności leczniczej. Ich stosowanie przez personel medyczny jest obowiązkowe. Wytyczne dotyczące postępowania z odpadami wytwarzanymi w czasie występowania zakażeń koronawirusem SARS-CoV-2 opracowane przez Głównego Inspektora Sanitarnego obejmują oprócz zaleceń dla placówek podmiotów działalności leczniczej również inne osoby i podmioty wytwarzające odpady w czasie trwania kwarantanny i izolacji. Ich przestrzeganie przyczynia się do obniżenia ryzyka przenoszenia zakażenia w społeczeństwie³⁰.

Podsumowanie

Pandemia koronawirusa COVID-19, która rozpoczęła się w 2020 r., spowodowała wiele niekorzystnych zmian, m.in. gospodarczych, społecznych czy kulturowych. Jej negatywne skutki dotknęły niemalże każdej z dziedzin gospodarki całego świata. Społeczny wymiar strat tak naprawdę jeszcze dziś, w czasie jej trwania, jest nie do oszacowania. Podobnie w sferze kulturowej efekty zweryfikują następne pokolenia. Niestety najbardziej dotkliwa okazała się sytuacja w sektorze ochrony zdrowia.

Dotychczasowe trudności w zakresie organizowania i funkcjonowania opieki zdrowotnej uwypukliły trudności organizacyjne i braki kadrowe. To, co dotychczas działało, zmieniło się pod wpływem nieprzewidywalnych zmian zdrowotnych społeczeństwa. Również stosowane procedury i standardy postępowania wymagały uaktualnienia i dostosowania do niecodziennych warunków. Zmieniły się też priorytety finansowe. Tym razem należało ponieść koszty nie tylko na potęgowanie i ratowanie zdrowia przez wyasygnowanie środków na pokrycie kosztów procedur medycznych, ale i na bezpieczeństwo społeczne.

²⁹ M. Tomaszewska-Kowalska, A. Balas, *Koronawirus – bądź odpowiedzialny*, „Pielęgniarka Epidemiologiczna” 2020, nr 2(80), s. 5–11.

³⁰ Wytyczne w sprawie postępowania z odpadami wytwarzanymi w czasie występowania zakażeń koronawirusem SARS-CoV-2 i zachorowań na wywołaną przez niego chorobę COVID-19 (w czasie trwania pandemii/epidemii nie dotyczy podmiotów udzielających świadczeń zdrowotnych), „Pielęgniarka Epidemiologiczna” 2020, nr 2(80), s. 16–20.

W tym zakresie duże nakłady zostały poniesione na odzież ochronną medyków, bez której tak naprawdę nie powinni oni przystępować do pracy. Z narażeniem swojego życia, które wielu z nich straciło, odbywały się przyjęcia chorych, ich diagnostyka, leczenie i pielęgnacja. Z kolei korzystne okazały się zmiany systemowe dotyczące wprowadzenia usług elektronicznych, skracających znacząco czas zarówno personelu medycznego, jak i pacjentów.

Przed nami ważne decyzje związane z koniecznością wymiany starego sprzętu komputerowego w podmiotach działalności leczniczej, wprowadzenia nowego oprogramowania i aplikacji oraz wzorów dokumentacji medycznej. Pielęgniarska dokumentacja elektroniczna jest już gotowa, przeszła badania naukowe potwierdzające jej efektywność i korzyść zastosowania, zarówno dla pielęgniarek, jak i pacjentów. Teraz czas jej wdrożenia, który musi być unormowany prawnie. Czasu jest mało, jako że przed jesienią winny zostać podjęte najważniejsze decyzje i działania, by wejść w jesień, która może nas powitać następną falą pandemii. Kolejne odsłony pandemii, zachorowania personelu, a często także jego śmierć, zmuszają do podjęcia dyskusji nad dalszym bezpieczeństwem personelu oraz wyciągnięciem wniosków w kierunku zastosowania innych skutecznych metod. Warto podkreślić, że zdrowie społeczeństwa to zdrowie każdego człowieka, razem i osobno. To codzienny trud personelu medycznego, ale i społeczna ochrona zdrowia ludzi.

Pielęgniarki, mimo iż stanowią najliczniejszą grupę zawodową wśród medyków, w rzeczywistości są tylko jednym z wielu ogniw bezpieczeństwa zdrowotnego całego społeczeństwa. Dbając o swoje zdrowie, przyczyniają się do dbania o zdrowie społeczne. Społeczeństwo szanując zdrowie swoje i innych, wzmacnia zdrowie pielęgniarek. Nich więc ta krótka dysertacja będzie początkiem wspólnych działań na rzecz zdrowia społeczeństwa po pandemii.

Bibliografia

- Ferschke W., *Skuteczna dezynfekcja tarczą ochronną przeciw koronawirusowi*, „Pielęgniarka Epidemiologiczna” 2021, nr 1(83).
- Frąckowiak A., *Zagrożenia w pracy pielęgniarki środowiskowej*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach” 2010, nr 1(6).
- Gawel G., *Obciążenie na pielęgniarskich stanowiskach wynikające z narażenia na czynniki środowiska pracy*, w: *Zarządzanie w pielęgniarstwie*. Podręcznik

- dla studentów studiów magisterskich Wydziałów Pielęgniarstwa oraz Wydziałów Nauk o Zdrowiu, A. Ksykiewicz-Dorota (red.), Wydawnictwo PZWL, Warszawa 2013.
- Gaweł G., *Obciążenia na pielęgniarskich stanowiskach pracy*, w: Podstawy organizacji pracy pielęgniarskiej. Podręcznik dla studentów studiów licencjackich Wydziałów Pielęgniarstwa oraz Wydziałów Nauk o Zdrowiu, A. Ksykiewicz-Dorota (red.), Wydawnictwo Czelej, Lublin 2004.
- Kodeks Etyki Zawodowej Pielęgniarki i Położnej Rzeczypospolitej Polskiej*, <https://nipip.pl/prawo/samorzadowe/krajowy-zjazd-pielegniarek-i-polozonych/kodeks-etyki-zawodowej-pielegniarki-i-polozonej-rzeczypospolitej-polskiej/> (dostęp: 27.05.2021).
- Kodeks Pracy, Art. 222¹ § 3 ustawy z dnia 26 czerwca 1974 r. (Dz. U. z 1998 r. nr 21, poz. 94, z późn. zm.).
- Kowalczyk K. i in., *Zagrożenia zawodowe pielęgniarek, położnych i lekarzy w środowisku pracy*, „Problemy Higieny i Epidemiologii” 2008, nr 89(2).
- Kulczycka K., Grenda M., Stychno E., *Trudności w wykonywaniu pracy na stanowisku pielęgniarki pediatrycznej*, „Journal of Education, Health and Sport” 2016, vol. 6(10).
- Kuriata E. i in., *Rozpoznawanie przez pielęgniarki szkodliwych czynników chemicznych i fizycznych na stanowiskach pracy w szpitalu*, „Family Medicine & Primary Care Review” 2012, vol. 14/1.
- Ochocka B., *Z doświadczenia praktyków*, „Pielęgniarka Epidemiologiczna” 2017, nr 4(71).
- Próchnicka B., *Współpraca bloku operacyjnego i centralnej sterylizatorni a nadzór nad zakażeniami szpitalnymi*, „Pielęgniarka Epidemiologiczna” 2017, nr 4(71).
- Rozowski P., *Bezpieczna praca w zawodzie pielęgniarki*, PIP, Wyd. 1/2019, s. 1–3, pip.gov.pl/pl/f/v/228249/bezpieczna%20praca%20w%20zawodzie%20pielegniarki.pdf (dostęp: 28.05.2021).
- Rozporządzenie Ministra Zdrowia z dnia 22.04.2005 w sprawie szkodliwych czynników biologicznych dla zdrowia w środowisku pracy oraz ochrony zdrowia pracowników zawodowo narażonych na te czynniki z późn. zmianami, stan od 29.12.2020.

Szkodliwe czynniki biologiczne – zmiany dla pracodawców, 22.01.2021, <https://www.ca-staff.eu/publikacje/szkodliwe-czynniki-biologiczne-zmiany-dla-pracodawcow> (dostęp: 29.05.2021).

Tomaszewska-Kowalska M., Balas A., *Koronawirus – bądź odpowiedzialny*, „Pielęgniarka Epidemiologiczna” 2020, nr 2(80).

Walusiak-Skorupa J., *Profilaktyka chorób zakaźnych – kierunek dla zbudowania zdrowego miejsca pracy*, „Pielęgniarka Epidemiologiczna” 2017, nr 4(71).

Żbikowski P., *Dezynfekcja rąk i powierzchni oraz antyseptyka błon śluzowych w dobie pandemii COVID-19*, „Pielęgniarka Epidemiologiczna” 2021, nr 1(83).

Occupational health and safety among nurses in the pandemic times

Abstract: Among the harmful factors in the work of a nurse, biological factors play a significant role. Thanks to the legally sanctioned changes introduced years ago, staff education and the use of many specialized procedures, the risk of many diseases caused by these factors has been minimized. Nevertheless, the pandemic caused great stir among medics. Thanks to the knowledge of procedures, personal protective equipment and the operation of specialized teams documenting threats, it was possible also in these conditions to quickly introduce changes that ensure safety. However, the subsequent phases of the pandemic, reported occurrences of the illness among staff, and often their deaths, force further discussion on ensuring safety of the staff and drawing conclusions aimed at the use of other effective methods.

Key words: protection of nurses' health, harmful factors, pandemic COVID-19

dr inż. Rafał Parczewski

Wojskowa Akademia Techniczna

e-mail: borys174@wp.pl

ORCID: 0000-0002-2603-0596

mgr Arkadiusz Chomacki

funkcjonariusz SG

Komenda Główna Straży Granicznej

e-mail: semtuk@interia.pl

Rozdział 5

Bezzałogowe statki powietrzne w procesie zapewnienia bezpieczeństwa w Polsce

Streszczenie: Rola bezzałogowych statków powietrznych w procesie bezpieczeństwa z roku na rok staje się bardziej widoczna. Służby typu Straż Graniczna, Policja czy wojsko używają tych latających obiektów do różnych zadań, zarówno w czasie pokoju, kryzysu, jak i działaniach wojennych (ćwiczenia, misje). Bezzałogowe statki powietrzne, zwane potocznie dronami, biorą aktywny udział w akcjach poszukiwawczo-ratowniczych, co tylko świadczy o ich wielozadaniowości. Opracowanie opisuje rolę dronów w zachowaniu bezpieczeństwa państwa. Zaangażowanie bezzałogowych statków powietrznych jest również aktywne w dobie pandemii COVID-19. Monitoring, prewencja czy świadczenie usług transportowych to funkcjonalności, które pomagają minimalizować skutki pandemii. Kluczowym celem rozdziału jest przedstawienie roli bezzałogowych statków powietrznych w procesie bezpieczeństwa państwa (ochrony granicy RP).

Słowa kluczowe: bezzałogowe statki powietrzne, ochrona granicy państwowej, bezpieczeństwo, zarządzanie kryzysowe

Wprowadzenie

Bezzałogowe statki powietrzne stały się już nieodzownym elementem i skutecznym rozwiązaniem dla wielu instytucji i jednostek państwowych. Cywilna i wojskowa sfera lotnictwa załogowego z roku na rok się unowocześnia. Zmiany przepisów prawnych i nowe technologie zwiększające funkcjonalność bezzałogowych statków powietrznych pozwalają na realizację zadań praktycznie z każdego obszaru.

Współczesne bezzałogowe statki powietrzne wyposażone są w kamery dzieńne i termowizyjne oraz posiadają wiele przydatnych funkcji, które można wykorzystać w czasie pokoju czy nawet działań wojennych. Straż Graniczna oraz wojsko wykorzystują bezzałogowe statki powietrzne głównie w zakresie monitoringu, rozpoznania i obserwacji.

Wysoki stopień niezawodności bezzałogowych platform latających sprawił, że również grupy przestępcze zaczęły stosować system bezzałogowy do różnego rodzaju procederów przestępczych. Straż Graniczna używa bezzałogowych systemów powietrznych głównie do ochrony granicy państwowej. Jest to doskonały i ekonomiczny sposób na właściwe rozdysponowanie sił i środków w trakcie pełnienia służby.

Zwiększenie wydajności czynnika ludzkiego i zastosowanie bezzałogowych statków powietrznych do niektórych zadań powoduje z pewnością zwiększenie bezpieczeństwa. Obecnie możliwości platform bezzałogowych pozwalają na ich uczestnictwo w akcjach kryzysowych, akcjach poszukiwawczo-ratowniczych czy innych działaniach priorytetowych z punktu widzenia państwa. Powodzie, pożary i inne katastrofy to zdarzenia, w przypadku których powinniśmy cały czas być czujni i skutecznie minimalizować negatywne skutki danego kataklizmu, skupiając się na ratowaniu życia ludzkiego.

Ze względu na specjalistyczny układ konstrukcyjny bezzałogowych statków powietrznych możemy je skutecznie wykorzystywać w różnych warunkach terenowych (tereny zamknięte, tereny otwarte, tereny morskie czy góryste). Jak można zauważyć, bezzałogowe systemy powietrzne odnoszą liczne sukcesy na arenie narodowej i międzynarodowej.

Bezpośredni udział w akcjach kryzysowych czy w zwalczaniu pandemii COVID-19 świadczy tylko o niezawodności bezzałogowych statków powietrznych. Rozwój i wdrażanie nowych pomysłów technologicznych pozwala na ciągły rozwój bezzałogowych statków powietrznych.

Należy dodać, że zauważana jest tendencja wspomagania lotnictwa załogowego w niektórych czynnościach przez bezzałogowe statki powietrzne. Proces szkolenia pilotów bezzałogowych statków powietrznych nie jest tak bardzo skomplikowany, a przy tym jest znacznie tańszy niż szkolenie pilota w lotnictwie załogowym. Efektywne użycie bezzałogowych statków powietrznych powoduje ich wielozadaniowość. Wykorzystanie potencjału dronów w geodezji, kartografii czy przemyśle farmaceutycznym jest dużym osiągnięciem naukowo-badawczym.

W obliczu ciągłego rozwoju technologicznego państwa muszą stale dostosowywać się do nowych wyzwań i zagrożeń. Ataki terrorystyczne, pandemie, nielegalna migracja czy przemyt towarów akcyzowych powodują ciągłe zmiany w tzw. tarczy ochronnej każdego państwa.

Ciągła zmiana działania grup przestępczych jest niebezpieczna dla każdego kraju. Nowy sprzęt, technologie i uzbrojenie powodują, że jesteśmy bezpieczniejsi, ale zarazem musimy być bardziej czujni. Liczne przypadki użycia dronów do przemytu nielegalnych towarów akcyzowych czy nielegalne przekroczenie granicy państwowej drogą powietrzną świadczy o skali zagrożenia.

Bezpieczeństwo całego społeczeństwa jest rzeczą ważną, dlatego jeśli pojawi się już jakieś niebezpieczeństwo, trzeba je jak najszybciej zminimalizować. Dzięki dronom można skuteczniej egzekwować prawo i prowadzić działania zmierzające do poprawy szeroko pojętego bezpieczeństwa państwa.

Bezzałogowe statki powietrzne w Straży Granicznej

Bezzałogowe statki powietrzne to po angielsku *Unmanned (Uninhabited) Aerial Vehicle* w skrócie UAV. Termin „bezzałogowe statki powietrzne” można zdefiniować jako sterowany w sposób zdalny, automatyczny lub metodą będącą kombinacją tych sposobów statek powietrzny. Powyższa definicja obejmuje różne rodzaje statków powietrznych, wyróżnia natomiast sposoby kontrolowania lotu: autonomiczny, zdalnie sterowany i mieszany¹.

Początkowo platformy bezzałogowe nie były zróżnicowane pod względem ich możliwości. W chwili obecnej istnieje wiele kryteriów, według których

¹ M. Adamski, J. Rajchel, *Bezzałogowe statki powietrzne. Część I. Charakterystyka i wykorzystanie*, Wyższa Szkoła Oficerska Sił Powietrznych, Dęblin 2013, s. 349.

można sklasyfikować bezzałogowe statki powietrzne, m.in. parametry lotu, charakter wykonywanej misji, układ konstrukcyjny czy udźwig².

Bezzałogowy statek powietrzny to platforma bezzałogowa operująca w atmosferze oraz poza nią, wraz z towarzyszącymi urządzeniami i elementami zapewniającymi kontrolowanie lotu³.

Błyskawiczny postęp w dziedzinie nowoczesnych technologii wpłynął na rozwój bezzałogowych statków powietrznych, które w chwili obecnej wykorzystywane są do celów cywilnych i wojskowych. Nie ma żadnych ograniczeń technicznych dotyczących rozmiaru bezzałogowych statków powietrznych⁴.

Ustawa prawo lotnicze z dnia 3 lipca 2002 r. określa możliwości wykonywania lotów w polskiej przestrzeni powietrznej przez bezzałogowe statki powietrzne. Według wskazanej ustawy bezzałogowy statek powietrzny (UAV) musi być wyposażony w takie same urządzenia umożliwiające lot, nawigację i łączność jak załogowy statek powietrzny wykonujący lot z widocznością (VFR) lub według wskazań przyrządów (IFR) w określonej klasie przestrzeni powietrznej. Odstępstwa mające zastosowanie w tym zakresie dla załogowych statków powietrznych stosuje się jednakowo do bezzałogowych statków powietrznych (UAV)⁵.

Także lotnictwo bezzałogowe musi być w odpowiedni sposób nadzorowane i traktowane na równi z lotnictwem załogowym.

Nowe przepisy określające loty cywilnych statków powietrznych zostały zawarte w Rozporządzeniu Wykonawczym Komisji (UE) 2019/947 z dnia 24.05.2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (BSP). Dokument określa bezzałogowe statki powietrzne jako niezależne od ich masy, mogące być eksploatowane w obrębie jednolitej europejskiej przestrzeni powietrznej obok załogowych statków powietrznych, zarówno samolotów, jak i śmigłowców⁶.

Przepisy dotyczące wykonywania lotów cywilnych bezzałogowymi statkami powietrznymi różnicują platformy latające ze względu na wagę i rodzaj wykonywanego lotu.

² Tamże, s. 49.

³ L. Cwojdzinski, *Bezzałogowe systemy walki*, Wojskowa Akademia Techniczna, Warszawa 2014, s. 15.

⁴ A. Konert, *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym*, C.H. BECK, Warszawa 2020, s. 31.

⁵ Ustawa z dnia 3 lipca 2002 r. *Prawo lotnicze*, Dz.U. z 2020 r. poz. 1970, z późn. zm.

⁶ Rozporządzenie Wykonawcze Komisji (UE) 2019/947 z dnia 24.05.2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych, L 152/45.

W chwili obecnej można latać dronami w całej Europie przy dokonaniu odpowiednich formalności, przepisy zostały ujednolicone dla wszystkich posiadaczy i użytkowników wskazanego sprzętu.

Straż Graniczna używa już od dłuższego czasu bezzałogowych platform latających, dzięki którym jeszcze skuteczniej realizuje zadania w ochronie granicy państwowej. Doskonałe właściwości bezzałogowych statków powietrznych pozwalają na częstą identyfikację różnego rodzaju przestępstw granicznych.

Z posiadanych informacji internetowych można wywnioskować, że zauważalne są przypadki przemytu papierosów bez polskich znaków akcyzy na wschodnich granicach Polski. Bliskość Ukrainy i Białorusi powoduje, że przemycany towar w postaci papierosów staje się atrakcyjną formą zarobkową wśród grup przestępczych. Przemycane papierosy mogą być rozprowadzone po terytorium naszego kraju, lecz również mogą trafić na rynek zachodni.

Użycie bezzałogowych statków powietrznych do monitoringu granicy państwowej na odcinku lądowym czy wodnym jest bardzo istotne ze względu na szybką identyfikację danego zdarzenia, określenie współrzędnych i przekazanie informacji do właściwego stanowiska dowodzenia. Samo przekazanie informacji jest na tyle istotne, że kierujący działaniami może we właściwy punkt skierować patrol mobilny. Przekazanie obrazu czy wykonanie zdjęć przez bezzałogowy statek powietrzny może służyć jako dowód w sprawie i być bardzo istotnym elementem w dalszym postępowaniu karno-skarbowym.

Drony w lotnictwie cywilnym są również wykorzystywane do kontroli zanieczyszczeń powietrza i różnego rodzaju pomiarów w wielu dziedzinach przemysłu. Drony wykorzystywane są w ratownictwie medycznym i w sektorze budowlanym, świadczą usługi logistyczne oraz transportowe.

Bezzałogowe statki powietrzne mogą wspierać jednostki samorządu terytorialnego, jak również być narzędziem czysto komercyjnym. Skala użycia cywilnych dronów jest ogromna i ciągle jest zapotrzebowanie na ich usługi.

W bezzałogowym lotnictwie wojskowym drony wykorzystywane są do celów rozpoznawczych, wywiadowczych, szkoleniowych i treningowych. Stosuje się je w trakcie realizacji misji zagranicznych. Drony mają również możliwość integracji ze sprzętem wojskowym. Specjalistycznie wyposażone drony mogą skutecznie naprowadzić na cel i są w pełni automatyczne.

Nowoczesna technologia bezzałogowych statków powietrznych pozwala na długotrwały lot o dużym zasięgu i pułapie. W chwili obecnej drony wykorzystywane przez polską armię są włączane do systemu zarządzania kryzysowego, gdzie dosko-

nale się sprawdzają. Wczesne wykrycie danego niebezpieczeństwa i odpowiednia reakcja mogą zapobiec nieszczęściu. Zadania realizowane przez opisywane maszyny są na ogromną skalę powszechne i tak naprawdę nie zostały do końca określone.

Bezpieczeństwo w ochronie granicy państwowej

Przestrzeń powietrzna jako ośrodek służący przemieszczaniu się oraz komunikowaniu stał się w ostatnich kilkunastu latach polem starć różnorodnych sił usiłujących zdobyć przewagę technologiczną w tej domenie, a tym samym uzyskać rynkową dominację. Efektem tych działań była komercyjna implementacja niszowych do tej pory rozwiązań, jakimi są bezzałogowe aparaty latające. Niski koszt wytwarzania, szerokie kanały dystrybucji oraz łatwość obsługi spowodowały gwałtowny wzrost wykorzystania dronów zarówno przez instytucje państwowe, jak i podmioty prywatne.

Nasylenie przestrzeni powietrznej niewielkimi obiektami latającymi spowodowało pojawienie się nowych zagrożeń. Możliwość nieuprawnionej ingerencji w życie prywatne obywateli, wykorzystanie BSP jako narzędzia czynów kryminalnych, czy ostatecznie środek zamachów terrorystycznych, w świetle braku kompleksowych rozwiązań prawnych regulujących dostęp to tego typu urządzeń oraz konieczności posiadania odpowiednich kwalifikacji operatorskich stały się palącym dylematem bezpieczeństwa.

Na gruncie administracji państwowej, dostrzegając potencjał oraz szerokie możliwości zastosowania BSP w domenie bezpieczeństwa oraz zarządzania kryzysowego, szereg służb oraz instytucji administracji publicznej wprowadziło do użytku przedmiotowe rozwiązania. Jedną z pierwszych formacji, która wdrożyła operacyjnie drony do działalności służbowej, była Straż Graniczna.

Jako jednolicie umundurowana i uzbrojona formacja przeznaczona do ochrony granicy państwowej na lądzie i na morzu oraz kontroli ruchu granicznego realizuje ustawowe zadania m.in. poprzez rozpoznawanie, zapobieganie i wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców w zakresie swojej działalności⁷. Odpowiada także za bezpieczeństwo w komunikacji międzynarodowej i porządek publiczny zarówno w zasięgu terytorialnym przejścia granicznego, jak i w strefie nadgranicznej.

⁷ Ustawa o Straży Granicznej z 12 października 1990 r. Dz.U. z 2011 r. nr 116, poz. 675.

Obecnie występująca reorientacja założeń funkcjonowania formacji określiła rolę Straży Granicznej jako organ administracji państwowej posiadający szerokie uprawnienia do działania na terytorium całego kraju, nie tylko w sferze ścigania przestępstw kryminalnych, lecz również uprawnionego do kontroli legalności zatrudnienia cudzoziemców, warunków pracy, zakwaterowania, wynagrodzenia, kontroli firm zatrudniających obcokrajowców oraz wszelkich związanych z tym dokumentów⁸.

Wdrażanie wieloletnich koncepcji funkcjonowania Straży Granicznej spowodowało, że formacja ta stała się nowoczesną służbą graniczo-migracyjną o charakterze policyjnym. Straż Graniczna jest odpowiedzialna za dokonywanie odpraw granicznych, jak również ochronę lądowej, morskiej i powietrznej granicy zewnętrznej UE/Schengen, realizując zadania w zakresie przeciwdziałania i zwalczania nielegalnej migracji, zwalczania przestępczości transgranicznej oraz przestępczości uwzględniającej udział cudzoziemców. W sytuacjach zagrożeń na terenie kraju siły i środki Straży Granicznej mogą być używane w stanach wyjątkowych, stanach klęski żywiołowej, ataków terrorystycznych, jak również akcjach poszukiwawczo-ratowniczych itp.⁹

Szerokie uprawnienia funkcjonariuszy Straży Granicznej, wyszkolenie, znajomość topografii terenu, struktury społecznej funkcjonującej w terytorialnym zasięgu działania danej jednostki organizacyjnej określa Straż Graniczną jako jedną z istotnych służb krajowego systemu bezpieczeństwa. Posiadanie komponentów logistycznych (pojazdy terenowe, łodzie patrolowe, statki powietrzne, pojazdy specjalistyczne, sprzęt pirotechniczny) umożliwiają realizację zadań w działaniach podejmowanych podczas wystąpienia sytuacji kryzysowych.

Powietrznym komponentem wykorzystywanym przez Straż Graniczną – prócz załogowych statków powietrznych – są bezzałogowe aparaty latające, znajdujące się na wyposażeniu oddziałów Straży Granicznej odpowiedzialnych za ochronę zewnętrznej granicy UE/Schengen. Obecnie są to głównie modele płatowców FlyEye oraz wielowirnikowce różnych typów, wykorzystywane głównie do rozpoznawania rejonów oraz miejsc narażonych na przestępczość graniczną, dozoru obiektów bądź rejonów, działań operacyjnych zmierza-

⁸ D. Magierek, *Rola Straży Granicznej w zapewnieniu bezpieczeństwa Polski (1990–2004)*, Toruń 2011, s. 269–279.

⁹ P. Górski, *Aspekty niemilitarne systemu obronnego państwa*, w: R. Kulczycki, B. Wiśniewski (red.), *Zaspokajanie potrzeb wojennych resortu spraw wewnętrznych i administracji*, Warszawa 2005, s. 19–21.

jących do ujęcia sprawców przekroczenia granicy państwowej oraz przemytu, ale też działań poszukiwawczych.

Obecnie jednym z największych zagrożeń w ochronie granicy państwowej jest przemyt wyrobów akcyzowych z wykorzystaniem dronów. Mając na uwadze widoczny trend wzrostowy zdarzeń związanych z przekroczeniem granicy państwowej wbrew przepisom BSP, istotną kwestią w świetle ustawowych zadań Straży Granicznej pozostaje pozyskanie odpowiednich środków technicznych oraz wypracowanie skutecznych metod przeciwdziałania ww. zagrożeniom.

Udział w różnego rodzaju targach branżowych, konferencjach i testach systemów komercyjnych antydronowych w znacznym stopniu przyczynia się do wypracowania świadomości sytuacyjnej w zakresie istniejącego potencjału technicznego, jak również trwającego progresu badawczego w tej materii. Pozwala też zdefiniować potrzeby operacyjne innych formacji/służb współdziałających ze Strażą Graniczną biorących udział w procesie identyfikacji możliwych zagrożeń, które na wielu płaszczyznach zadaniowych bywają zbieżne.

Przegląd zdolności operacyjnych dostępnych obecnie rozwiązań technicznych w zakresie przeciwdziałania zagrożeniom ze strony BSP wykazał dwa aspekty, które mają kluczowe znaczenie przy ocenie skuteczności poszczególnych systemów antydostępowych, a obecnie, wydawać by się mogło, stanowią odrębne moduły badawczo-rozwojowe poszczególnych podmiotów działu bezpieczeństwa. Prawidłowa detekcja oraz efektywna neutralizacja BSP powinny stanowić w miarę możliwości zunifikowany i mobilny system przeciwdziałający zagrożeniom ze strony BSP. Przeprowadzane analizy na obecnym etapie poszukiwania skutecznych systemów pozwoliły na identyfikację istniejących mankamentów konfiguracyjnych poszczególnych komponentów systemów, co samo w sobie stanowi dużą wartość dodaną i może być punktem odniesienia oraz przedmiotem dalszej oceny i weryfikacji w procesie poszukiwania skutecznych rozwiązań antydronowych. Obecnie jednak ich poziom nie stanowi skutecznego środka przeciwdziałającego zagrożeniom ze strony BSP.

Aktualnie prezentowane systemy mogą znaleźć zastosowanie w monitoringu oraz stacjonarnej ochronie terenów zamkniętych bądź obiektów infrastruktury krytycznej. Natomiast mając na względzie manewrowy i selektywny charakter ochrony granicy państwowej, ilość autonomicznych komponentów wchodzących w skład poszczególnych systemów, ich zasięg oraz zdolności neutralizacyjne znacznie ogranicza możliwości ich wykorzystania w realizacji zadań służbowych SG.

Wykorzystanie BSP stanowi zatem – prócz niezwykle pozytywnego wymiaru praktycznego – również poważne techniczne wyzwanie, wymagające znalezienia skutecznych środków zaradczych, których obecnie prezentowany poziom jest daleki od pożądanego.

Zakończenie

W instytucjach państwowych typu Straż Graniczna, Wojsko Polskie czy Policja drony są już wykorzystywane i sprawdzone w różnego rodzaju sytuacjach.

Policja wykorzystuje drony do wykrywania wykroczeń w ruchu drogowym, przestępstw, monitoringu czy patrolowania. Straż Graniczna w realizacji czynności służbowych z zakresie ochrony granicy państwowej. Wojska Obrony Terytorialnej, artyleria i jednostki specjalne w armii używają już od dłuższego czasu systemu bezzałogowych statków powietrznych do różnego rodzaju zadań w kraju i za granicą.

Powyższe może tylko świadczyć o fachowości i zaufaniu do opisywanego systemu. Najważniejsze dla każdego państwa jest zachowanie właściwego poziomu bezpieczeństwa, które określane jest jako „[...] stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Jedną z podstawowych potrzeb człowieka jest sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych [...]”¹⁰.

Bezpieczeństwo to także możliwość przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukovanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów¹¹.

Analizując przytoczone definicje, pojęcie bezpieczeństwa należy zawsze postrzegać kompleksowo oraz wielowymiarowo z uwzględnieniem istniejącego kontekstu sytuacyjnego. Niezależnie od przyjętego zakresu definicyjnego bezpieczeństwo powinno być pochodną ujęcia systemowego, którego Straż Graniczna – obok innych służb i instytucji – jest istotnym jego elementem.

¹⁰ Bezpieczeństwo w: *Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2009.

¹¹ S. Koziej, *Wstęp do teorii i historii bezpieczeństwa*, skrypt internetowy, Warszawa/Ursynów, 2010, s. 2.

Powyższe rozważania z pewnością nie wyczerpują całości problemu. Niezbędne jest prowadzenie badań w kierunku zwiększenia efektywności bezzałogowych systemów latających.

Działalność grup przestępczych, sytuacje kryzysowe czy ataki terrorystyczne wymagają stosowania odpowiednich narzędzi dających poczucie bezpieczeństwa. Drony świetnie sprawdzają się przy monitorowaniu i obrazowaniu terenu, dzięki czemu są doskonałym środkiem, który może w odpowiednim czasie rozpoznać zagrożenie.

Bezzałogowe statki powietrzne zarówno w lotnictwie cywilnym, jak i wojskowym dzięki swoim właściwościom wykorzystywane są do różnych celów, w zależności od ustawowych zadań danego organu czy instytucji.

Dzisiejsze bezzałogowe statki powietrzne są w stanie ratować ludzkie życie i zdrowie, dlatego dostosowanie ich funkcjonalności do panujących zagrożeń jest głównym zadaniem badaczy i inżynierów tej dziedziny.

Szybka i skuteczna wymiana informacji pozwala na podjęcie odpowiednich działań zapobiegawczych¹². Powyższe jest istotne z punktu widzenia każdej akcji poszukiwawczej, ratowniczej, kryzysowej itp.

Wymagane są analizy i badania dotyczące działalności grup przestępczych, które do swojej działalności wykorzystują bezzałogowe statki powietrzne.

Bibliografia

- Adamski M., Rajchel J., *Bezzałogowe statki powietrzne. Część I. Charakterystyka i wykorzystanie*, Wyższa Szkoła Oficerska Sił Powietrznych, Dęblin 2014.
- Cwojdzinski L., *Bezzałogowe systemy walki. Charakterystyka, wybrane problemy użycia i eksploatacji*, Wydawnictwo Wojskowa Akademia Techniczna 2014.
- Górski P., *Aspekty niemilitarne systemu obronnego państwa*, w: R. Kulczycki, B. Wiśniewski (red.), *Zaspokajanie potrzeb wojennych resortu spraw wewnętrznych i administracji*, Warszawa 2005.
- Konert A., *Bezzałogowe statki powietrzne. Nowa era w prawie lotniczym*, C.H. BECK, Warszawa 2020.

¹² R. Parczewski, *Ochrona praw dziecka w kontekście bezpieczeństwa w Strefie Schengen*, w: Scientific Bulletin of Chełm. Section of Pedagogy, Państwowa Wyższa Szkoła Zawodowa, Chełm 2020, s. 165, <https://drive.google.com/file/d/16RVGSsI2JKjqwKp4Ab0Ls7Ei1p-sDcbD/view>.

Bezzałogowe statki powietrzne w procesie zapewnienia bezpieczeństwa...

- Koziej S., *Wstęp do teorii i historii bezpieczeństwa*, skrypt internetowy, Warszawa/Ursynów, 2010.
- Magierek D., *Rola Straży Granicznej w zapewnieniu bezpieczeństwa Polski (1990–2004)*, Toruń 2011.
- Parczewski R., *Ochrona praw dziecka w kontekście bezpieczeństwa w Strefie Schengen*, w: *Scientific Bulletin of Chełm. Section of Pedagogy*, Państwowa Wyższa Szkoła Zawodowa, Chełm 2020.
- Słownik terminów z zakresu bezpieczeństwa narodowego*, Warszawa 2009.
- Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze* (Dz.U. z 2020 r. poz. 1970, z późn. zm.).
- Ustawa o Straży Granicznej z 12 października 1990 r.* (Dz.U. z 2011 r. nr 116, poz. 675).
- Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 26 marca 2013 r. w sprawie wyłączenia zastosowania niektórych przepisów ustawy – Prawo lotnicze do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków* (Dz.U. 2013 poz. 440).
- Rozporządzenie Wykonawcze Komisji (UE) 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych* (L 152/45).

Unmanned aerial vehicles in the process of ensuring safety in Poland

Abstract: The role of unmanned aerial vehicles in the safety process becomes more visible every year. Services such as: Border Guard, police or military use these flying objects for various tasks, both in times of peace, crisis, and warfare (exercises, missions). Unmanned aerial vehicles, commonly known as drones, take an active part in search and rescue operations, which only proves their multi-tasking nature. The article describes the role of “drones” in maintaining state security. The involvement of unmanned aerial vehicles is also active in the time of the COVID-19 pandemic. Monitoring, prevention, or the provision of transport services are those functionalities that help minimize the effects of a pandemic. The key objective of the article is to present the role of unmanned aerial vehicles in the process of state security (protection of the Polish border).

Key words: unmanned aerial vehicles, state border protection, security, crisis management

CZĘŚĆ II

WYBRANE KWESTIE PSYCHOSPOŁECZNE W ZWIĄZKU Z PANDEMIĄ COVID-19

mgr inż. Joanna Grzegorzczak

Politechnika Poznańska, Wydział Inżynierii Zarządzania

e-mail: joanna.g.grzegorzczak@doctorate.put.poznan.pl

ORCID: 0000-0002-9137-7086

Rozdział 6

Działania CSR w obliczu pandemii COVID-19

Streszczenie: Globalizacja, rozwój koncepcji zrównoważonego rozwoju, wzrastająca presja różnych środowisk, wzrost świadomości społecznej oraz rosnące oczekiwania konsumentów mają istotny wpływ na funkcjonowanie współczesnych podmiotów gospodarczych. Odpowiedzią na nowe trendy i zmieniające się otoczenie biznesowe stała się koncepcja społecznej odpowiedzialności biznesu (w skrócie CSR). Od początku XXI w. CSR zintensyfikował się do jednej z najważniejszych strategii zarządzania – zarówno wśród teoretyków, jak i praktyków biznesu. Jednakże niespodziewana pandemia koronawirusa SARS-CoV-2 wymusiła zmianę dotychczasowego podejścia do społecznej odpowiedzialności biznesu. W artykule podjęto próbę weryfikacji, czy sytuacja spowodowana pandemią COVID-19 skłoniła organizacje biznesowe do podjęcia nowych działań CSR. Pierwszą część opracowania stanowi prezentacja istoty społecznej odpowiedzialności biznesu oraz kluczowych obszarów zaangażowania przedsiębiorstw. Następnie autorka dokonała analizy kierunków ewolucji koncepcji CSR w obliczu pandemii nowego koronawirusa. W ostatniej części rozdziału zaprezentowano praktyki, jakie w czasie pandemii COVID-19 wdrożyła firma IKEA Retail Polska.

Słowa kluczowe: społeczna odpowiedzialność biznesu, CSR, kryzys, pandemia COVID-19

Wprowadzenie

Współcześnie podmioty gospodarcze przestają być traktowane wyłącznie jako „instrumenty do osiągnięcia celów ekonomicznych”¹. Zanieczyszczenie środowiska naturalnego, wzrost świadomości ekologicznej społeczeństw, zwiększenie oczekiwań względem organizacji, a także zmiana podejścia inwestorów sprawiają, że przedsiębiorstwa coraz częściej podlegają ocenie w kategoriach moralnych i społecznych. Nie ulega wątpliwości, że obecnie organizacje biznesowe działają w ramach szeroko pojmowanego systemu społecznego i ponoszą współodpowiedzialność za jego rozwój. Powoduje to, że coraz większa liczba przedsiębiorstw dostrzega konieczność przewartościowania modelu biznesowego na bardziej odpowiedzialny. Menedżerowie zarządzający organizacjami biznesowymi zaczynają wyrażać większą troskę o dobro pracowników, społeczeństwa, jak i środowiska naturalnego. W Polsce trend ten rozwija się od kilkunastu lat, ale to 2020 r. przyspieszył wdrażanie idei społecznej odpowiedzialności biznesu. Kryzys spowodowany pandemią koronawirusa SARS-CoV-2 wywołał zmiany w podejściu organizacji do społecznej odpowiedzialności – przedsiębiorstwa na nowo zdefiniowały kluczowe grupy interesariuszy, a dotychczas prowadzone działania zostały zastąpione nowymi inicjatywami. Celem niniejszego opracowania jest wskazanie, jakie działania z zakresu CSR prowadziły w czasie pandemii COVID-19 polskie przedsiębiorstwa. Z powodu braku opracowań dotyczących społecznej odpowiedzialności biznesu w warunkach COVID-19 autorka dokonała analizy dwóch raportów prezentujących działania wybranych firm w 2020 r., a także przeanalizowała inicjatywy podjęte przez firmę IKEA Retail Polska.

Istota społecznej odpowiedzialności biznesu

Społeczna odpowiedzialność biznesu, czyli CSR, jest koncepcją wielowymiarową, co znacznie utrudnia znalezienie jednej, ogólnie obowiązującej definicji. Na przestrzeni kilkudziesięciu lat w literaturze przedmiotu pojawiło się

¹ A. Paliwoda-Matiolańska, *Odpowiedzialność społeczna w procesie zarządzania przedsiębiorstwem*, Warszawa 2009, s. 21.

przynajmniej kilkaset różnych wyjaśnień terminu „społeczna odpowiedzialność biznesu”. Problem z przejrzystym zdefiniowaniem CSR wynika m.in. z²:

- niejednoznacznej terminologii – poza najpopularniejszą społeczną odpowiedzialnością biznesu w języku polskim funkcjonują inne, bliskoznaczne terminy, jak: społeczna odpowiedzialność przedsiębiorstw, społeczna odpowiedzialność korporacji, przedsiębiorstwo obywatelskie, społeczne zaangażowanie biznesu, odpowiedzialność korporacyjna czy marketing społeczny. Podobne problemy związane z terminologiczną niejednoznacznością występują też w wielu innych językach;
- interdyscyplinarności koncepcji – społeczna odpowiedzialność biznesu czerpie z różnych dziedzin nauki. Zróżnicowanie ujęć pochodzących z dorobku ekonomii, zarządzania, prawa, filozofii czy socjologii powoduje możliwość różnego definiowania CSR, akcentującego wyłącznie wybrane elementy koncepcji;
- zakresu stosowania – na sposób pojmowania społecznej odpowiedzialności biznesu wpływają też takie czynniki, jak: kontekst kulturowy, regulacje prawne, oczekiwania społeczne w danym kraju, a także wielkość firmy, branża czy etap życia organizacji. Wszechstronne zastosowanie koncepcji sprawia, że istnieje możliwość formułowania różnych definicji, dopasowanych do indywidualnych oczekiwań;
- ciągły rozwój idei – jak podkreśla B. Rok, „inaczej określano CSR w latach 30. ubiegłego wieku, a inaczej w latach 90.”³. Koncepcja społecznej odpowiedzialności biznesu nieustannie ewoluuje, poszerzając się o kolejne obszary. W pierwotnym ujęciu, zaproponowanym pod koniec XIX w. przez A. Carnegiego, CSR oznaczał dobroczynne działania na rzecz osób ubogich oraz czynienie z prywatnych majątków użytku dla całego społeczeństwa⁴.

Współcześnie społeczna odpowiedzialność biznesu ma o wiele szersze znaczenie. Dziś CSR można zinterpretować jako dobrowolne uwzględnienie w działalności gospodarczej interesów społecznych, ochrony środowiska

² B. Rok, *Podstawy odpowiedzialności społecznej w zarządzaniu*, Warszawa 2013, s. 73–81.

³ B. Rok, dz. cyt., s. 76.

⁴ M. Rybak, *Etyka menedżera – społeczna odpowiedzialność przedsiębiorstwa*. Warszawa 2004, s. 15.

przyrodniczego oraz relacji z szeroko rozumianymi interesariuszami⁵. Według W. Leońskiego istotą CSR jest poczucie odpowiedzialności za efekty społeczne i środowiskowe prowadzonej działalności gospodarczej. Dla społecznie odpowiedzialnych organizacji istotne jest także utrzymywanie pozytywnych i długotrwałych relacji z różnymi członkami życia społeczno-gospodarczego⁶. Zgodnie z inną definicją społeczna odpowiedzialność biznesu oznacza strategiczne i holistyczne podejście do zarządzania organizacją, zakładające dobrowolne przestrzeganie zasad etyki biznesu, eliminowanie negatywnego oddziaływania na otoczenie, maksymalizowanie pozytywnego wpływu na społeczeństwo i środowisko oraz prowadzenie dialogu z różnymi grupami interesariuszy⁷. Z kolei B. Rok określa CSR jako podejście strategiczne i długofalowe, oparte na trwałych i przejrzystych relacjach z otoczeniem, mające na celu wypracowanie rozwiązań korzystnych dla samej organizacji, jak i jej interesariuszy⁸. Inną aktualną definicję społecznej odpowiedzialności biznesu prezentuje norma PN-ISO 26 000, według której CSR to „odpowiedzialność organizacji za wpływ jej decyzji i działań na społeczeństwo i środowisko zapewniana przez przejrzyste i etyczne postępowanie, które:

- przyczynia się do zrównoważonego rozwoju, w tym dobrobytu i zdrowia społeczeństwa;
- uwzględnia oczekiwania interesariuszy;
- jest zgodne z obowiązującym prawem i spójne z międzynarodowymi normami postępowania;
- jest zintegrowane z działaniami organizacji i praktykowane w jej relacjach”⁹.

Definicję społecznej odpowiedzialności biznesu zawiera także „Odnowiona strategia Unii Europejskiej na lata 2011–2014 dotycząca społecznej odpowiedzialności przedsiębiorstw”, przyjęta przez Komisję Europejską w 2011 r. W do-

⁵ K. Zadros, *Jak uciec od społecznej odpowiedzialności i pozostać społecznie odpowiedzialną firmą*, „Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska” 2017, nr 108, s. 452.

⁶ W. Leoński, *Społeczna odpowiedzialność i nieodpowiedzialność biznesu*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania” 2015, nr 39, s. 69.

⁷ B. Buczkowski, T. Dorożyński, A. Kuna-Marszałek, T. Serwach, J. Wieloch, *Społeczna odpowiedzialność biznesu. Studia przypadków firm międzynarodowych*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016, s. 16.

⁸ B. Rok, *Odpowiedzialny biznes w nieodpowiedzialnym świecie*, Warszawa 2004, s.18

⁹ <https://odpowiedzialnybiznes.pl/hasla-encyklopedii/spoleczna-odpowiedzialnosc-biznesu-csr> (dostęp: 14.11.2021).

kumencie tym zdefiniowano CSR jako „odpowiedzialność przedsiębiorstw za ich wpływ na społeczeństwo”¹⁰.

Dokonując analizy przytoczonych definicji społecznej odpowiedzialności biznesu, można zauważyć, iż wszystkie opierają się na podobnych założeniach – dobrowolności, prospołecznej i proekologicznej postawie podmiotów gospodarczych oraz dialogu z interesariuszami. Reasumując rozważania nad definicją CSR, należy przyjąć, że społeczna odpowiedzialność biznesu to dobrowolne i trwałe podejmowanie takich decyzji biznesowych, które poza maksymalizacją zysku wywierają pozytywny wpływ na społeczeństwo i środowisko naturalne. Istotą społecznej odpowiedzialności biznesu jest zatem integracja aspektów społecznych i środowiskowych z codzienną działalnością przedsiębiorstwa.

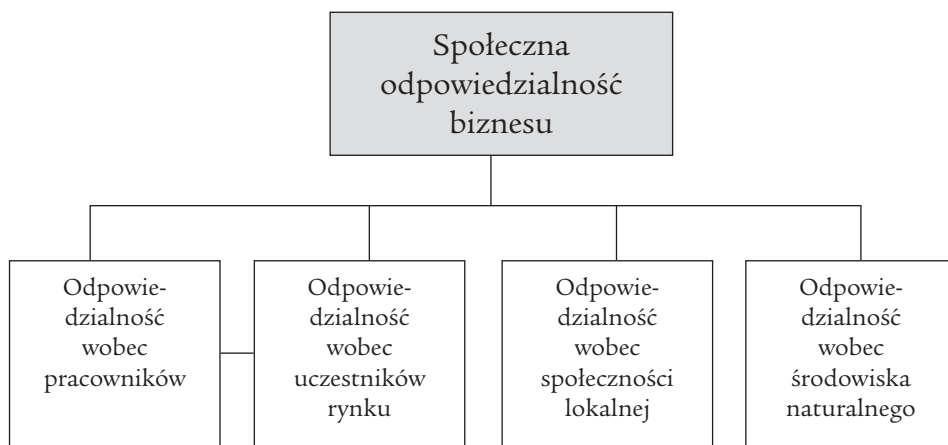
Obszary społecznej odpowiedzialności biznesu

Wszechstronność koncepcji CSR sprawia, że organizacje gospodarcze mogą angażować się w nią w różny sposób – w zależności od posiadanych kompetencji, zasobów, a także tradycji kulturowych, sytuacji społecznej i ekologicznej oraz branż, w jakich funkcjonują¹¹. W praktyce społeczna odpowiedzialność biznesu przejawia się w rozmaitych działaniach, jakich podejmują się przedsiębiorstwa. Praktyki te powinny być realizowane kompleksowo i długofalowo, najlepiej we wszystkich obszarach reprezentujących określone grupy interesariuszy. W literaturze przedmiotu uwzględnia się różne ujęcia kluczowych obszarów społecznej odpowiedzialności. Na rysunku 1 zaprezentowano jeden z najczęściej spotykanych podziałów, według którego przedsiębiorstwa powinny prowadzić politykę CSR w czterech obszarach zaangażowania.

¹⁰ Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. *Odnowiona strategia Unii Europejskiej na lata 2011–2014 dotycząca społecznej odpowiedzialności przedsiębiorstw*, Bruksela, 2011, KOM (2011) 681 wersja ostateczna, s. 7.

¹¹ M. Żemigła, *Społeczna odpowiedzialność przedsiębiorstwa budowanie zdrowej, efektywnej organizacji*, Kraków 2007, s. 101.

Rysunek 1. Obszary społecznej odpowiedzialności biznesu



Źródło: Opracowanie własne na podstawie: M. Ratajczak, *Implementacja strategii CSR w odniesieniu do środowiska naturalnego jako ważny element strategii rozwojowych współczesnych przedsiębiorstw*, „Zeszyty Naukowe SGGW w Warszawie. Problemy Rolnictwa Światowego” 2010, nr 10, s. 79.

Aktywność przedsiębiorstw w ramach przedstawionych obszarów wyraża się w takich działaniach, jak¹²:

- zapewnianie bezpiecznych i stabilnych warunków pracy, możliwości rozwoju, sprawiedliwego wynagrodzenia i dodatkowych świadczeń, budowanie przyjaznego i zadawalającego środowiska pracy – pracownicy;
- dostarczanie bezpiecznych produktów i usług, monitorowanie jakości, współpraca z lokalnymi partnerami, przeciwdziałanie korupcji czy stosowanie sprawiedliwej polityki cenowej – rynek;
- wsparcie finansowe i rzeczowe lokalnych instytucji, integracja ze społecznością lokalną, tworzenie nowych miejsc pracy i wspieranie inicjatyw sprzyjających rozwojowi regionu – społeczność lokalna;
- wdrażanie procesów produkcyjnych przyjaznych dla środowiska, efektywne wykorzystywanie zasobów naturalnych, redukcja emisji gazów cieplarnianych oraz współpraca z instytucjami ekologicznymi – środowisko naturalne.

¹² M. Ratajczak, *Implementacja strategii CSR w odniesieniu do środowiska naturalnego jako ważny element strategii rozwojowych współczesnych przedsiębiorstw*, „Zeszyty Naukowe SGGW w Warszawie. Problemy Rolnictwa Światowego” 2010, nr 10, s. 79

Realizacja kompleksowych i długofalowych praktyk w zakresie społecznej odpowiedzialności biznesu pozwala na osiągnięcie szeregu korzyści, zarówno przez samą organizację, jak i przez jej interesariuszy. Wyniki badania „Menedżerowie CSR 2020” wskazują, że do głównych korzyści wewnętrznych (ponoszonych przez przedsiębiorstwo) należy¹³:

- podniesienie poziomu zaangażowania pracowników;
- zwiększenie rozpoznawalności marki;
- podniesienie poziomu świadomości pracowników w zakresie etyki;
- poprawa relacji ze społecznościami lokalnymi;
- podniesienie poziomu zaufania konsumentów;
- wdrożenie innowacyjnych, nowatorskich rozwiązań;
- większe zaufanie wśród inwestorów;
- osiągnięcie przewagi konkurencyjnej;
- poprawa reputacji i wizerunku przedsiębiorstwa.

E. Jastrzębska oraz K. Gadomska-Lila wskazują, że implementacja koncepcji społecznej odpowiedzialności biznesu niesie też wiele korzyści w czasie kryzysu. Organizacje, które traktują CSR jako istotną część swojej strategii, potrafią lepiej zarządzać ryzykiem, a ponadto tworzą pozytywne i długofalowe relacje ze wszystkimi grupami interesariuszy. Społecznie odpowiedzialne firmy budują tzw. kapitał zaufania, dzięki czemu nawet w okresie kryzysu posiadają lokalnych klientów, mogą liczyć na poparcie pracowników oraz wyrozumiałość partnerów biznesowych¹⁴. W konsekwencji firmy działające w duchu CSR potrafią przetrwać sytuacje kryzysowe. Oczywiście przezwyciężenie kryzysu będzie możliwe wyłącznie wtedy, gdy organizacja wdroży trwałe i adekwatne do sytuacji działania¹⁵. Pandemia COVID-19 jako sytuacja bezprecedensowa wpłynęła na polskie przedsiębiorstwa i postawiła je przed wieloma nowymi wyzwaniami.

Wpływ pandemii COVID-19 na działania CSR

Globalna pandemia COVID-19, spowodowana rozprzestrzenianiem się koronawirusa SARS-CoV-2, wywarła ogromny wpływ na funkcjonowanie

¹³ <https://odpowiedzialnybiznes.pl/aktualności/jakie-sa-korzysty-z-wdrazania-odpowiedzialnego-biznesu-wyniki-badania-menedzerowie-csr-2020> (dostęp: 14.11.2021).

¹⁴ E. Jastrzębska, *CSR a kryzys*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu” 2011, nr 156, s. 111.

¹⁵ K. Gadomska-Lila, *Społeczna odpowiedzialność biznesu w obliczu kryzysu gospodarczego*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania” 2012, nr 28, s. 28.

większości przedsiębiorstw. Jednym z największych wyzwań, przed jakim stanęli menedżerowie organizacji gospodarczych, było dostosowanie strategii CSR do warunków pandemii. W celu określenia, jak sytuacja wywołana pandemią COVID-19 wpłynęła na działania CSR podejmowane przez polskie przedsiębiorstwa, autorka opracowania dokonała analizy dwóch raportów:

- „Odpowiedzialny biznes w Polsce 2020. Dobre praktyki”¹⁶ przygotowanego przez Forum Odpowiedzialnego Biznesu, będącego największą i najstarszą polską organizacją pozarządową zajmującą się kwestiami społecznej odpowiedzialności biznesu;
- „100 firm, organizacji oraz inicjatorów, którzy podjęli działania społeczne w odpowiedzi na pandemię COVID-19 w 2020 roku”¹⁷ autorstwa Tomasa Smorgowicza – eksperta w dziedzinie CSR oraz założyciela Fundacji Rozwoju Społecznej Odpowiedzialności HELISA.

Pierwsza z omawianych publikacji zawierała 1958 przykładów dobrych praktyk prowadzonych w 2020 r. przez 225 podmiotów gospodarczych. Ponad połowa z zaprezentowanych działań dotyczyła praktyk nowych, zgłoszonych do raportu po raz pierwszy – ponad 40% więcej niż w 2019 r. Wzrost nowych działań, w większości spowodowanych pandemią COVID-19, pozwala wnioskować, iż polskie przedsiębiorstwa dostosowały swoje strategie CSR do nadzwyczajnej sytuacji. Również w drugim z raportów wskazano na ogromną aktywność organizacji – ponad 80% analizowanych firm zadeklarowało swoje zaangażowanie w działania społecznie odpowiedzialne. W obydwu publikacjach wyróżniono kilka kluczowych grup odbiorców pomocy. Wedle danych zebranych w raporcie „100 firm, organizacji oraz inicjatorów, którzy podjęli działania społeczne w odpowiedzi na pandemię COVID-19 w 2020 roku” aż 86% organizacji wsparło swoimi działaniami przedstawicieli służb medycznych, policję, służby bezpieczeństwa oraz sanepid. Ponadto 65% przedsiębiorstw zaangażowało się w pomoc na rzecz konsumentów, seniorów oraz indywidualnych osób w potrzebie, a 20% firm wspomogło dzieci, rodziców oraz opiekunów dydaktycznych. Również w 19. wydaniu raportu „Odpowiedzialny biznes w Polsce” zaobserwowano wzmożone działania na rzecz społeczności lokalnej – tutaj rozumianej zbiorczo jako: służba zdrowia, nauczyciele i uczniowie, seniorzy

¹⁶ <https://odpowiedzialnybiznes.pl/publikacje/raport-2020/> (dostęp: 14.11.2021).

¹⁷ <https://odpowiedzialnybiznes.pl/aktualności/pandemia-wywrocila-dotychczasowy-porzadek/> (dostęp: 14.11.2021).

oraz inni przedstawiciele społeczeństwa. Inicjatywy skierowane do tej grupy interesariuszy obejmowały:

- dofinansowanie budowy szpitali tymczasowych;
- darowizny finansowe na zakup sprzętu medycznego i środków ochrony osobistej;
- darowizny rzeczowe obejmujące środki ochrony osobistej oraz sprzęt medyczny;
- dostosowanie linii produkcyjnych do wytwarzania płynu dezynfekującego, wydruku przyłbic czy szycia maseczek;
- dostarczanie darmowego cateringu oraz produktów spożywczych pracownikom szpitali i samotnym seniorom;
- przekazanie telefonów, tabletów oraz kart SIM oddziałom zakaźnym;
- przekazanie komputerów stacjonarnych, laptopów, drukarek i tabletów szkołom podstawowym, domom dziecka oraz potrzebującym dzieciom;
- użyczenie samochodów służbowych szpitalom i laboratoriom;
- udostępnianie miejsc do odizolowania osób przebywających na kwarantannie;
- zaangażowanie pracowników w pomoc w ramach wolontariatu pracowniczego.

Kolejną grupą odbiorców pomocy byli wewnętrzni interesariusze organizacji – ich pracownicy. Najważniejszymi działaniami w tym obszarze było utrzymanie zatrudnienia, zapewnienie bezpiecznych warunków pracy i zapobieganie rozprzestrzenianiu się koronawirusa SARS-CoV-2 wśród pracowników. W ramach poprawy bezpieczeństwa przedsiębiorstwa dostosowywały powierzchnię biurową do zasad reżimu sanitarnego, kontrolowały temperaturę ciała pracowników przed wejściem do zakładu, realizowały kampanie informacyjne, oferowały darmowe konsultacje z internistami, zaopatrywały pracowników i ich rodziny w konieczne środki ochrony osobistej, wprowadzały system pracy rotacyjnej, a w wielu przypadkach zdecydowały się na przejście w tryb pracy zdalnej. Zmiana modelu pracy niosła ze sobą kolejne wyzwania – przedsiębiorstwa musiały zapewnić zatrudnionym odpowiedni sprzęt IT, umożliwiający efektywną pracę z domu. Firmy przekazywały pracownikom niezbędny sprzęt lub dofinansowywały jego zakup. Przejście na *home office* wiązało się także z wprowadzeniem specjalnych programów szkoleniowych online oraz zdalną socjalizacją pracowników i przełożonych. Priorytetowe stało się również wsparcie psychologiczne osób zatrudnionych – jak wskazuje sondaż Centrum

Badawczo-Rozwojowego BioStat, aż 58,6% Polaków odczuło negatywny wpływ pandemii na swój stan psychiczny¹⁸. Aby wesprzeć pracowników w obliczu pandemii koronawirusa, pracodawcy organizowali sesje z psychologami, przygotowywali spotkania online poświęcone technikom relaksacyjnym, radzeniu sobie ze stresem, *work-life balance* oraz uruchamiali specjalne infolinie, gdzie pracownicy mogli skorzystać z bezpłatnych porad psychologów, prawników i doradców finansowych.

Adresatami inicjatyw z zakresu społecznej odpowiedzialności biznesu, które zaprezentowano w omawianych raportach, byli także klienci, dostawcy i partnerzy biznesowi. Wśród podejmowanych w tym obszarze działań należy wyróżnić udostępnianie darmowych usług i produktów, wydłużanie terminów płatności, stałe dokonywanie zamówień, nieoprocentowaną pomoc finansową dla franczyzobiorców, a także odbieranie niesprzedanych produktów i zwracanie środków pieniężnych. Społecznie odpowiedzialne organizacje wspierały swoich dostawców i partnerów biznesowych dzieląc się także swoim *know-how*, np. w celu szybszego przystosowania linii produkcyjnej do wytwarzania maseczek ochronnych. Sporą liczbę inicjatyw stanowiły działania edukacyjne – podmioty gospodarcze prowadziły kampanie edukacyjne i udzielały innym organizacjom porad w zakresie zarządzania kryzysowego, zmian prawnych i podatkowych, a także korzystania z pomocy w ramach Tarczy Antykryzysowej. Ważnym efektem pandemii koronawirusa SARS-CoV-2 był także wzrost działań realizowanych w ramach współpracy międzysektorowej lub wewnątrzbranżowej. Autor raportu „100 firm, organizacji oraz inicjatorów, którzy podjęli działania społeczne w odpowiedzi na pandemię COVID-19 w 2020 roku” podaje, iż ponad 40% zbadanych organizacji zjednoczyło siły dla zwiększenia skali pozytywnego wpływu na sytuację kryzysową.

Wyzwaniem spowodowanym rozprzestrzenianiem się koronawirusa jest także minimalizowanie negatywnego wpływu na środowisko przyrodnicze, o czym wspomina jeden z autorów raportu Forum Odpowiedzialnego Biznesu. W wyniku pandemii nastąpił ogromny wzrost ilości zużytych tworzyw sztucznych jednorazowego użytku, które w dużych ilościach trafiają na dno mórz i oceanów, przyczyniając się do zanieczyszczenia plastikiem całych ekosystemów. Według szacunków Światowej Organizacji Zdrowia w pierwszym półroczu 2020 r. społeczność na całym świecie zużywała miesięcznie około 89 milio-

¹⁸ https://www.biostat.com.pl/pandemia_negatywnie_wplywa_na_finanse_zycie_towarzyskie_i_stan_psychiczny_polakow.php (dostęp: 14.11.2021).

nów maseczek i 76 milionów rękawiczek, co znacznie zwiększyło konsumpcję plastiku¹⁹. W niespotykanej dotąd ilości wyrzucało się także opakowania po przesyłkach kurierskich, a w wyniku lockdownu większość restauracji i punktów gastronomicznych oferowała żywność w opakowaniach jednorazowych. Zanieczyszczenie środowiska naturalnego to palący problem, jednak mimo to w przedstawionych raportach nie zaprezentowano żadnych działań mających na celu przeciwdziałanie zatrutowaniu środowiska.

Analiza informacji zawartych w omawianych publikacjach pozwoliła na stworzenie listy najważniejszych wyzwań, jakie stoją przed społecznie odpowiedzialnymi organizacjami. Wyniki analizy zaprezentowano w tabeli 1.

Tabela 1. Inicjatywy CSR wywołane pandemią COVID-19

Obszar	Pracownicy	Rynek	Społeczność lokalna	Środowisko naturalne
Inicjatywy CSR wywołane pandemią COVID-19	1. Utrzymanie zatrudnienia 2. Zapewnienie bezpieczeństwa w miejscu pracy 3. Wsparcie organizacyjne pracy zdalnej 4. Zapewnienie pomocy psychologicznej	1. Zdolność do współpracy wewnątrzsektorowej i międzybranżowej 2. Wsparcie dostawców, odbiorców i partnerów biznesowych	1. Wsparcie służb medycznych, seniorów, ośrodków opiekuńczych, uczniów i nauczycieli 2. Wolontariat pracowniczy	Ograniczenie ilości plastiku Serwowanie żywności w opakowaniach biodegradowalnych Stosowanie ekologicznych opakowań na przesyłki kurierskie

Źródło: opracowanie własne.

¹⁹ <https://www2.deloitte.com/pl/pl/pages/press-releases/articles/nie-mozemy-zyc-bez-plastiku-pakiet-GOZ.html> (dostęp: 14.11.2021).

Działania firmy IKEA Retail Polska w czasie pandemii COVID-19

Doskonałym przykładem organizacji biznesowej, która zareagowała na sytuację epidemiczną w sposób odpowiedzialny jest firma IKEA Retail Polska. Od początku pandemii firma realizowała kompleksowe i odpowiedzialne działania na rzecz różnych grup interesariuszy, które zostały szczegółowo opisane na stronie internetowej biura prasowego przedsiębiorstwa (<http://biuroprasowe.ikea.pl>). Szczególną troską IKEA objęła swoich pracowników, zapewniając im bezpieczne warunki pracy oraz próbując odpowiedzieć na wszystkie ich bieżące potrzeby. Priorytetem dla organizacji było udostępnienie pracownikom rzetelnych i sprawdzonych informacji na temat koronawirusa, dlatego w internecie IKEA uruchomiła specjalną stronę „Koronawirus – Centrum Informacji”. Dostęp do strony posiadają wszyscy pracownicy sklepów IKEA w Polsce. Mogą na niej znaleźć informacje o aktualnych wytycznych dotyczących bezpieczeństwa i higieny pracy, zaleceniach oraz zasadach postępowania. IKEA za pośrednictwem strony internetowej swojego biura prasowego informuje też o innych działaniach skierowanych do pracowników. IKEA to wielkopowierzchniowy sklep meblowy, posiadający 11 sklepów stacjonarnych na terenie Polski. Specyfika działalności uniemożliwia całkowite przejście w tryb pracy zdalnej, dlatego przedsiębiorstwo przykłada szczególną wagę do bezpieczeństwa w codziennej pracy. Pracownicy mają stały dostęp do maseczek ochronnych i płynów do dezynfekcji, a stanowiska wymagające bezpośredniego kontaktu z klientem są odpowiednio zabezpieczone. Firma dostrzega także potrzebę wsparcia psychologicznego pracowników, dlatego każda osoba, która odczuwa obawy i lęk związane z pandemią, może skorzystać ze specjalistycznej pomocy. Organizacja wdrożyła też wiele innych rozwiązań pomocowych dla pracowników, przede wszystkim:

- elastyczne godziny pracy oraz urlopy rodzicielskie dla osób, które pozostają w domu z dziećmi;
- dofinansowanie różnicy pomiędzy zasiłkiem opiekuńczym a pełnym wynagrodzeniem dla rodziców dzieci do ósmego roku życia;
- szeroki pakiet szkoleń online;
- dofinansowanie posiłków dla wszystkich pracowników.

Pomimo pandemii i trzykrotnego zamknięcia sklepów IKEA w całej Polsce sieć utrzymała zatrudnienie, a pensje pracowników nie zostały obniżone.

IKEA Retail Polska wykazała się odpowiedzialnym podejściem także w stosunku do innych grup interesariuszy. Firma przekazała ponad 4,5 miliona złotych darowizn w formie wsparcia dla społeczności lokalnych szczególnie dotkniętych pandemią. Darowizny rzeczowe w postaci mebli, akcesoriów i innych produktów IKEA trafiły do szpitali, stacji pogotowia oraz domów opieki w całym kraju. Szczególną opieką otoczone zostały szpitale zajmujące się leczeniem psychiatrycznym i psychologicznym. Dodatkowo firma włączyła się w ogólnopolską akcję #WzywamyPosiłki, w ramach której do szpitali, pogotowia ratunkowego, laboratoriów i inspekcji sanitarnych trafiło łącznie 40 tysięcy posiłków, przygotowanych przez pracowników restauracji IKEA. Realizacja inicjatywy była możliwa dzięki wsparciu jednego z partnerów biznesowych grupy – firmy Eurocash Gastronomia, która odpowiadała za dostarczenie żywności do odpowiednich punktów. Firma dostrzegła także problem osób w kryzysie bezdomności, które często przebywają w lokalach o obniżonych warunkach sanitarnych. W związku z tym organizacja wyposażyła schroniska i punkty pomocy w największych polskich miastach w takie produkty, jak: materace, koce, ręczniki, dozowniki do mydła, spryskiwacze do środków dezynfekujących, termosy i pojemniki na żywność. Dzięki pomocy IKEA warunki w schroniskach uległy poprawie, a tym samym zmalało ryzyko rozprzestrzeniania choroby COVID-19.

Grupa IKEA zadeklarowała też społecznie odpowiedzialne działania w obszarze rynku. Zgodnie z wewnętrznym zarządzeniem firma nie pobierała od najemców opłat za wynajem powierzchni w okresie zamknięcia galerii handlowych. Jednocześnie firma nie informuje o nowych działaniach prośrodowiskowych prowadzonych w czasie pandemii. Należy jednak podkreślić, że od początku 2020 r. z asortymentu IKEA oraz restauracji sieci zniknęły plastikowe słomki, jednorazowe opakowania czy worki na śmieci.

Podsumowując, firma IKEA Retail Polska zareagowała na sytuację epidemiczną w Polsce w prawdziwie odpowiedzialny sposób. Organizacja od samego początku pandemii prowadziła szereg nowych działań mających na celu wsparcie kluczowych grup interesariuszy. Inicjatywy, w jakie zaangażowała się firma IKEA, w większości odpowiadają najważniejszym wyzwaniom, jakie zaprezentowano w tabeli 1.

Podsumowanie

Pandemia COVID-19 znacząco wpłynęła na funkcjonowanie większości przedsiębiorstw, w tym na prowadzone przez nie działania CSR. Firmy z różnych branż zaangażowały się w nowe inicjatywy mające na celu minimalizowanie skutków pandemii COVID-19. Do najważniejszych działań w zakresie społecznej odpowiedzialności biznesu należy zaliczyć wsparcie szpitali i służby zdrowia, zapewnienie bezpiecznych warunków pracy pracownikom, organizację pomocy psychologicznej oraz wsparcia technicznego w czasie pracy zdalnej. Przedsiębiorstwa społecznie odpowiedzialne wykazały się odpowiedzialnością wobec swoich klientów, dostawców i partnerów biznesowych. Wiele z nich połączyło siły, aby zwiększyć skalę pozytywnego wpływu na zaistniałą sytuację kryzysową. Zaangażowanie organizacji w działania CSR na tak wielu płaszczyznach buduje zaufanie i zwiększa wiarygodność podmiotów, a co najważniejsze – pozwala przetrwać czas kryzysu zarówno organizacjom gospodarczym, jak i całemu społeczeństwu.

Obszarem, w którym zdecydowanie brakuje działań CSR, jest troska o środowisko naturalne. Pandemia spowodowała ogromny wzrost zużycia jednorazowych tworzyw sztucznych – w skali globalnej każdego miesiąca zużywane są miliony масечек i rękawiczek ochronnych. W ciągu ostatniego roku problemy związane z globalnym ociepleniem klimatu czy nadmierną konsumpcją plastiku nie przestały istnieć. W związku z tym społecznie odpowiedzialne organizacje powinny dalej dążyć do minimalizowania negatywnego wpływu na środowisko przyrodnicze.

Bibliografia

- Buczkowski B., Dorożyński T., Kuna-Marszałek A., Serwach T., Wieloch J., *Spółeczna odpowiedzialność biznesu. Studia przypadków firm międzynarodowych*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2016.
- Gadomska-Lila K., *Spółeczna odpowiedzialność biznesu w obliczu kryzysu gospodarczego*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania” 2012, nr 28.
- Jastrzębska E., *CSR a kryzys*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu 2011, nr 156.

- Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Odnowiona strategia Unii Europejskiej na lata 2011–2014 dotycząca społecznej odpowiedzialności przedsiębiorstw, Bruksela 2011, KOM (2011) 681 wersja ostateczna.
- Leoński W., *Społeczna odpowiedzialność i nieodpowiedzialność biznesu*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania” 2015, nr 39.
- Paliwoda-Matiolańska A., *Odpowiedzialność społeczna w procesie zarządzania przedsiębiorstwem*, C.H. Beck, Warszawa 2009.
- Ratajczak M., *Implementacja strategii CSR w odniesieniu do środowiska naturalnego jako ważny element strategii rozwojowych współczesnych przedsiębiorstw*, „Zeszyty Naukowe SGGW w Warszawie. Problemy Rolnictwa Światowego” 2010, nr 10.
- Rok B., *Odpowiedzialny biznes w nieodpowiedzialnym świecie*, Akademia Rozwoju Filantropii w Polsce, Forum Odpowiedzialnego Biznesu, Warszawa 2004.
- Rok B., *Podstawy odpowiedzialności społecznej w zarządzaniu*, Wydawnictwo Poltext, Warszawa 2013.
- Rybak M., *Etyka menedżera – społeczna odpowiedzialność przedsiębiorstwa*, Wydawnictwo Naukowe PWN, Warszawa 2004.
- Zadros K., *Jak uciec od społecznej odpowiedzialności i pozostać społecznie odpowiedzialną firmą*, „Zeszyty Naukowe. Organizacja i Zarządzanie/ Politechnika Śląska” 2017, nr 108.
- Żemigła M., *Społeczna odpowiedzialność przedsiębiorstwa budowanie zdrowej, efektywnej organizacji*, Oficyna Wydawnicza Wolters Kluwer Business, Kraków 2007.

Źródła internetowe

- https://www.biostat.com.pl/pandemia_negatywnie_wplywa_na_finanse_zycie_towarzyskie_i_stan_psychiczny_polakow.php (dostęp: 14.11.2021).
- <https://www2.deloitte.com/pl/pl/pages/press-releases/articles/nie-mozemy-zyc-bez-plastiku-pakiet-GOZ.html> (dostęp: 14.11.2021).
- <https://odpowiedzialnybiznes.pl/hasla-encyklopedii/spoleczna-odpowiedzialnosc-biznesu-csr/> (dostęp: 14.11.2021).

<https://odpowiedzialnybiznes.pl/aktualności/jakie-sa-korzysci-z-wdrazania-odpowiedzialnego-biznesu-wyniki-badania-menedzerowie-csr-2020/> (dostęp: 14.11.2021).

<https://odpowiedzialnybiznes.pl/aktualności/pandemia-wywrocila-dotychczasowy-porzadek/> (dostęp: 14.11.2021).

<https://odpowiedzialnybiznes.pl/publikacje/raport-2020/> (dostęp: 14.11.2021).

CSR activities in the face of the COVID-19 pandemic

Summary: Globalization, the development of the concept of sustainable development, increasing pressure from various environments, increasing social awareness and growing consumer expectations have a significant impact on the functioning of modern business entities. The concept of corporate social responsibility (CSR for short) has become a response to new trends and changing business environment. Since the beginning of the 21st century, CSR has intensified into one of the most important management strategies—both among theoreticians and business practitioners. However, the unexpected SARS-CoV-2 coronavirus pandemic forced a change in the current approach to corporate social responsibility. The article attempts to verify whether the situation caused by the COVID-19 pandemic prompted business organizations to undertake new CSR activities. The first part of the study presents the essence of corporate social responsibility and key areas of corporate involvement. Then, the author analyzed the directions of the evolution of the CSR concept in the face of the new coronavirus pandemic. The last part of the article presents the practices that were implemented by IKEA Retail Polska during the COVID-19 pandemic.

Key words: corporate social responsibility, CSR, crisis, COVID-19 pandemic

mgr Patryk Toczyński

Szkoła Doktorska Akademii Pomorskiej w Słupsku

email: patoczyn@wp.pl

ORCID: 0000-0003-0797-5655

Rozdział 7

E-obywatel a bezpieczny obywatel – stosowanie rozwiązań technologicznych w okresie pandemii COVID-19

Streszczenie: Okres pandemii COVID-19 przyspieszył oraz jednocześnie zwiększył zakres stosowania kanałów elektronicznych do załatwiania najróżniejszych spraw urzędowych. Specjalnie w tym celu przygotowano szereg najróżniejszych aplikacji rządowych. Zwiększył się również zakres wykorzystania bankowości elektronicznej – płatności kartami płatniczymi oraz dokonywanie zakupów online. Wszystkie wspomniane systemy mają za zadanie ułatwiać i przyspieszać obywatelom załatwianie najróżniejszych spraw. Jednakże mogą zostać one wykorzystane do kradzieży danych osobowych i innych informacji dotyczących obywateli, do inżynierii społecznej lub, co gorsza, do kontroli nad obywatelami. Powyższe systemy działające niezależnie i bezpiecznie nie są groźne dla obywatela, jednakże po połączeniu np. systemu e-pacjent z jednoczesną kontrolą finansową systemów bankowych oraz aplikacją śledzącą na telefonie może spełnić się scenariusz permanentnej kontroli rodem z książki *Rok 1984* autorstwa Georga Orwella.

Słowa kluczowe: e-obywatel, cyberbezpieczeństwo, COVID-19, aplikacje, systemy informatyczne

Wprowadzenie

Rozwój technologii, zwłaszcza w dziedzinach telekomunikacji oraz cybernetyki, pozwolił na rozwiązywanie wielu spraw obywatelskich poprzez kanały komunikacji cyfrowej. Obywatele polscy aktualnie mogą załatwić sprawy urzędowe poprzez e-mail, system ePUAP, obywatel.gov.pl czy też e-deklaracje. Do tego dochodzi szereg aplikacji na smartfon, np. mObywatel i wprowadzona w czasie pandemii COVID-19 aplikacja Kwarantanna Domowa, mających ułatwiać oraz przyspieszać komunikację pomiędzy obywatelem a organami administracji państwowej. Warto zadać pytanie, czy tak szerokie wykorzystanie różnorodnych systemów elektronicznych zapewnia obywatelom polskim bezpieczeństwo w ujęciu ochrony danych osobowych, prywatności oraz czy nie stanowi zagrożenia nieuprawnionego wykorzystania prywatnych informacji. W 2020 i 2021 r., w okresie pandemii COVID-19 przyspieszył oraz jednocześnie zwiększył się zakres stosowania kanałów elektronicznych do załatwiania najróżniejszych spraw urzędowych. Specjalnie w tym celu są również przygotowywane w szybkim tempie najróżniejsze aplikacje rządowe. Zwiększył się też zakres wykorzystania bankowości elektronicznej – płatności kartami płatniczymi oraz dokonywanie zakupów online. Wszystkie wspomniane systemy mają za zadanie umożliwić w bezpieczny dla zdrowia sposób załatwianie obywatelom najróżniejszych spraw administracyjnych czy też komercyjnych. W okresie pandemii obywatel chcący załatwić sprawę komfortowo lub w zadowalającym terminie musi skontaktować się z jednostkami administracji rządowej oraz samorządowej telefonicznie (w tym poprzez SMS), internetowo (e-mail, odpowiednie platformy) bądź poprzez specjalne aplikacje smartfonowe. Sposoby tej komunikacji w okresie pandemii mają w wielu sprawach taki sam status jak osobista wizyta petenta w urzędzie. Jednakże mogą zostać one wykorzystane do kradzieży danych osobowych i innych informacji dotyczących obywateli, do inżynierii społecznej lub, co gorsza, do kontroli nad obywatelami. Innym zagrożeniem wynikającym z tak szerokiego zastosowania rozwiązań technologicznych w administracji jest ryzyko wykluczenia społecznego osób nieradzących sobie z najnowszymi technologiami lub osób niemogących z nich korzystać z braku dostępu do sieci internetowej lub ubóstwa.

W pracy zastosowano metodologię badawczą opartą o metody teoretyczne, takie jak analiza literatury przedmiotu czy danych publicznych dotyczących aplikacji oraz rozwiązań internetowych stosowanych w okresie pandemii

COVID-19. Dużą część analizowanego materiału stanowią materiały cyfrowe. Z zakresu badań empirycznych przeprowadzono obserwację istniejących rozwiązań technologicznych oraz metodę eksperymentu polegającą na sprawdzeniu funkcjonowania wspomnianych systemów internetowych oraz aplikacji telefonicznych w praktyce. Pozwoliło to na synergiczne przedstawienie problemu oraz na wyprowadzenie wniosków.

E-obywatel

Rok 2020 oraz 2021 to okres dynamicznego rozwoju e-obywatela w Polsce. Rozwój pandemii COVID-19 na świecie, ryzyko zachorowania oraz wprowadzane obostrzenia wymusiły zmianę w codziennym życiu milionów Polaków. Znacznym utrudnieniem w owym czasie stało się ograniczanie pracy urzędów oraz skierowanie całej rzeszy urzędników do pracy zdalnej lub też za zamkniętymi drzwiami urzędów. Sytuację dodatkowo skomplikowała konieczność odbywania kwarantanny zarówno przez pracowników urzędów, jak i petentów lub sprawowanie opieki nad dziećmi, które nie poszły do szkół z powodu ich zamknięcia (wprowadzenia edukacji zdalnej). W takiej sytuacji Polakom nie pozostało nic innego jak załatwiać sprawy administracyjne na odległość: telefonicznie, korespondencyjnie, e-mailowo. Jednakże wymienione kanały komunikacji również zaczęły stanowić swoistą barierę w kontakcie z urzędem, bowiem telefonicznie można uzyskać jedynie informacje w podstawowym zakresie oraz poradę, ponieważ urzędnik nie ma możliwości zweryfikowania obywatela poprzez rozmowę głosową. Korespondencja listowa, mimo że możliwa do wysłania w czasie pandemii, również posiadała swoje ograniczenia związane z obostrzeniami w placówkach pocztowych, wydłużonych kolejkach, brakiem możliwości skorzystania z poczty w przypadku nałożonej kwarantanny czy też częstym zjawiskiem kwarantanny korespondencji spływającej do urzędu (co wydłużało proces załatwienia sprawy o kilka dni). E-mail pozwala na przysyłanie pism czy skanów dokumentów i rzeczywiście można tą drogą rozwiązać wiele spraw, ale nie stanowi on jednak oficjalnej drogi komunikacji na linii urząd–petent. Drogą tą obywatel prócz informacji urzędowej raczej nie otrzyma oficjalnych pism urzędowych, często też jest skazany na interpretację urzędnika, czy daną sprawę można załatwić e-mailowo czy nie.

W tak przedstawionej sytuacji najskuteczniejszym oraz najszybszym sposobem rozwiązania spraw administracyjnych stało się wykorzystanie przez

Polaków specjalnych systemów oraz aplikacji pozwalających na załatwienie niemal wszystkich spraw urzędowych.

Dowodem na taki stan rzeczy są dane statystyczne przedstawione przez Kancelarię Rady Prezesa Ministrów¹:

- w 2020 r. 4 174 206 Polaków założyło profil zaufany, co stanowi 47% wszystkich aktywnych profili zaufanych (8 816 654);
- w stosunku do 2019 r. (okresu sprzed pandemii) w 2020 r. założono ponad dwa miliony więcej kont w systemie;
- najwięcej kont (602 739) zostało założonych w kwietniu 2020 r., czyli w okresie obowiązywania największych obostrzeń w Polsce, włącznie z zakazem wstępu do lasów. Był to również pierwszy miesiąc całkowitej edukacji zdalnej;
- poprzez system ePUAP Polacy w 2020 r. wysłali do urzędów przeszło 1 432 770 pism elektronicznych. Dziennie było to średnio 3914 pism;
- w stosunku do roku 2019 liczba e-pism w 2020 r. zwiększyła się o 900 000, co stanowi wzrost o około 63%;
- Polacy poprzez e-usługi załatwiali również sprawy cywilne. W samym 2020 r. zwiększyło się aż niemal czterokrotnie uzyskiwanie cyfrowo odpisów aktów stanu cywilnego. Skorzystano z tej formy otrzymania dokumentu 197 967 razy;
- W 2020 r. w sposób elektroniczny 146 989 razy zgłoszono urodzenie dziecka (ponaddwukrotny wzrost w stosunku do 2019 r.);
- W 2020 r. (w stosunku do roku poprzedniego) stwierdzono również prawie trzykrotnie więcej e-wnioseków meldunkowych i ponaddwukrotnie więcej e-wnioseków dotyczących wyrobienia nowego dowodu osobistego;
- W samym 2020 r. zgłoszono w sposób elektroniczny 601 297 wniosków dotyczących zbycia/nabycia pojazdów.

Przedstawiona statystyka stanowi ewidentny dowód zwiększenia wykorzystania e-usług rządowych w celu rozwiązania spraw administracyjnych w okresie pandemii. Jednakże w zdecydowanej większości impulsem do skorzystania z tej formy komunikacji z urzędem była konieczność wynikająca z ograniczenia innych form kontaktu. E-usługi dokonały internetowej stabilizacji zaspokojenia urzędowych potrzeb obywateli w najbardziej newralgicznym momencie pande-

¹ *E-usługowe podsumowanie 2020 r.*, <https://www.gov.pl/web/cyfryzacja/e-uslugowe-podsumowanie-2020-r> (dostęp: 29.05.2021).

mii w Polsce². Zastanawiającym jest, czy trend wzrostu wykorzystania e-usług w administracji utrzyma się w 2021 r. oraz w latach kolejnych.

Z jakich systemów oraz aplikacji mogą korzystać Polacy?

Profil zaufany³ jest elektronicznym środkiem identyfikacji obywatela. Stanowi swoiste połączenie podpisu elektronicznego z dowodem osobistym. Jest on wymagany w celu załatwienia spraw urzędowych. Profil Zaufany można uzyskać poprzez system bankowy lub założyć go w czasie wizyty w urzędzie. W systemie znajdują dane osobowe, numer PESEL, miejsce i data urodzenia oraz adres zamieszkania.

ePUAP⁴ jest platformą internetową służącą do komunikacji z urzędami. Na stronie po zalogowaniu znajdują się gotowe e-formularze w celu rozwiązania spraw obywatelskich, np. takich jak zgłoszenie zbycia/nabycia pojazdu, zameldowania/wymeldowania czy też wysłanie pisma ogólnego do urzędu. Platforma pozwala na załączanie wniosków (dokumentów, zdjęć). Po wypełnieniu formularza obywatel przekierowywany jest do profilu zaufanego w celu podpisania dokumentu. W ten sposób może oficjalnie komunikować się z urzędami bądź sądami. Korespondencja posiada status tradycyjnego podpisanego dokumentu, takiego jak składany osobiście w urzędzie lub wysłany pocztą. Na platformie znajdują się e-skrzynka obywatela, na którą urzędy przesyłają odpowiedź lub zgłoszenie przyjęcia pisma. Administracja państwowa jest zobligowana do odpowiedzi bądź rozpatrzenia pisma w trybie urzędowym (postępowania administracyjnego).

Platforma Obywatel.gov.pl wraz z aplikacją na smartfony mObywatel stanowi swoistą skarbnicę wiedzy o obywatelu. W systemie znajdują się takie dane, jak⁵:

- adres zameldowania;
- dane aktów cywilnych (rodzice, małżeństwo);
- dane kontaktowe;

² Tamże.

³ Tamże.

⁴ *Załatw sprawy urzędowe przez internet na ePUAP*, <https://www.gov.pl/web/gov/załatwiasprawy-urzedowe-przez-internet-na-epuap> (dostęp: 29.05.2021).

⁵ Ministerstwo Cyfryzacji, <https://obywatel.gov.pl> (dostęp: 29.05.2021).

- dane wszystkich dotychczas wyrobionych dowodów osobistych;
- dane dotyczące prawa jazdy wraz z wglądem do systemu punktów karnych;
- dane dotyczące posiadanych pojazdów;

System pozwala również na uzyskanie zaświadczenia o zameldowaniu oraz załatwienie spraw urzędowych poprzez przekierowanie na odpowiednią stronę. Istotnym jest fakt, że jeżeli obywatel chce skorzystać ze wspomnianego systemu, wystarczy, że zaloguje się poprzez Profil Zaufany. Wszystkie dane o obywatelu, o których wie administracja państwowa, wprowadzane są automatycznie, nawet wbrew wiedzy czy zgody osób zainteresowanych.

Kolejnym systemem są e-Deklaracje⁶. Jest to platforma internetowa dla obywateli w celu załatwienia spraw skarbowo-podatkowych. Poprzez system można złożyć elektroniczne deklaracje podatkowe takie jak rozliczenie roczne PIT. W systemie znajdują dane osobowe obywateli, złożone deklaracje oraz informacje o zarobkach i odprowadzonych składkach podatkowych. Do systemu można zalogować się poprzez Profil Zaufany bądź poprzez podanie danych podatkowych.

Obywatel może skorzystać również z platformy Pacjent.gov.pl⁷. Jest to internetowe konto pacjenta, na którym znajdują się dane o zdrowiu obywateli, informacje dotyczące zwolnień lekarskich, wystawionych skierowań czy recept. W okresie pandemii poprzez system można zarejestrować się na szczepienie przeciw COVID-19. System pozwala również na umawianie wizyt lekarskich i zabiegów medycznych. Do systemu można zalogować się, używając Profilu Zaufanego, dowodu osobistego z warstwą elektroniczną lub poprzez specjalną aplikację na smartfony mojeIKP.

Przedstawione systemy magazynują oraz przetwarzają ogromne ilości danych o obywatelach polskich. Dane osobowe oraz wrażliwe, które w niepowołanych rękach mogą stanowić zagrożenie dla bezpieczeństwa obywateli. Zaskakującym jest, iż w zasadzie do każdego systemu wystarczy zalogować się za pomocą Profilu Zaufanego. W wyniku wycieku bądź utraty danych logujących wraz z hasłem (np. w przypadku zgubienia telefonu) obywatel może stać się ofiarą przestępstwa lub oszustwa z bardzo nieprzyjemnymi skutkami.

⁶ E-deklaracje, <https://www.podatki.gov.pl/e-deklaracje> (dostęp: 29.05.2021).

⁷ Ministerstwo Zdrowia i Narodowy Fundusz Zdrowia, <https://pacjent.gov.pl>, (dostęp: 29.05.2021).

E-obywatel a bezpieczny obywatel – stosowanie rozwiązań technologicznych...

Nieuprawniony dostęp do systemów przez osoby trzecie może posłużyć do wyłudzeń finansowych, do kradzieży tożsamości czy też dokonywania przestępstw.

Do powyżej przedstawionych systemów e-usług można dołączyć również aplikacje smartfonowe specjalnie przygotowane dla obywateli polskich w czasie trwania pandemii, takie jak:

Kwarantanna Domowa⁸, będąca aplikacją weryfikującą odbywanie nałożonej przez sanepid kwarantanny. Aplikacja z wykorzystaniem automatu dzwoni do obywatela, po czym informuje go, że ma wykonać zdjęcie w miejscu odbywania kwarantanny wraz z przesłaniem danych geolokalizacyjnych (GPS). Dane te ze zdjęciem są zapisywane na rządowych serwerach. Jednocześnie podawana jest informacja, iż po zakończeniu kwarantanny wszelkie dane z bazy danych zostaną usunięte. Zainstalowanie oraz korzystanie z aplikacji w czasie nałożonej kwarantanny jest obowiązkowe⁹. Osoby, które nie posiadają odpowiedniego sprzętu bądź połączenia z internetem, są zobowiązane do złożenia stosownego oświadczenia pod rygorem odpowiedzialności karnej. Oświadczenie takie zgodnie z ustawą musi być złożone do Policji bądź właściwego miejscowo Państwowego Powiatowego Inspektora Sanitarnego¹⁰.

STOP COVID – ProteGo Safe¹¹ – to dobrowolna aplikacja na telefon. Jej zadaniem jest ograniczanie transmisji wirusa SARS-CoV-2. Poprzez technologię Bluetooth aplikacja rejestruje każde spotkanie z innym użytkownikiem, które trwało powyżej 15 minut i odbyło się w odległości do 2 metrów. Jeżeli któryś z użytkowników zachoruje w ciągu 14 dni, pozostali zostaną poinformowani o tym fakcie. Aplikacja zapisuje miejsce i czas przebywania użytkowników oraz to, z kim spotykali się w tym czasie. Na szczęście nie jest ona obowiązkowa. Jednakże wyciek wspomnianych danych mógłby służyć do kontroli nad obywatelami.

Domowa Opieka Medyczna wraz z aplikacją PulsoCare¹² – to obowiązkowe aplikacje medyczne dla osób skierowanych przez lekarza podstawowej opieki

⁸ Aplikacja Kwarantanna Domowa, <https://www.gov.pl/web/koronawirus/kwarantanna-domowa> (dostęp: 29.05.2021).

⁹ Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020 r., poz. 374, z późn. zm.

¹⁰ Tamże.

¹¹ STOP COVID, <https://www.gov.pl/web/protegosafe> (dostęp: 29.05.2021).

¹² Domowa Opieka Medyczna, <https://www.gov.pl/web/domowaopiekamedyczna> (dostęp: 29.05.2021).

zdrowotnej do programu Domowa Opieka Medyczna. Aplikacja wraz z przekazanym pacjentowi pulsoksymetrem stanowi zdalny system opieki zdrowotnej. Poprzez aplikację wysyłane są do systemu Ministerstwa Zdrowia takie parametry zdrowotne jak saturacja, tętno, temperatura ciała czy też występujące objawy chorobowe. Wgląd do danych posiadają lekarze, którzy na podstawie odczytów mogą zdalnie skierować pacjenta na teleporadę, wezwać pogotowie czy skierować na dalsze leczenie.

W okresie pandemii Polacy coraz chętniej korzystają również z elektronicznych kanałów bankowości. Badania sektora bankowego wskazują, iż jesienią 2020 r. zwiększyła się o ponad 50% ta forma korzystania z usług bankowych w stosunku do sytuacji sprzed pandemii¹³. Stanowi to ryzyko zwiększania się zjawisk takich jak próby wyłudzenia czy kradzieży danych w celu włamań do internetowej bankowości. Zwiększona sprzedaż poprzez internet może nasilić także tzw. oszustwa internetowe polegające na fikcyjnej sprzedaży towarów. Kolejnym zagrożeniem jest potencjalna awaria systemów bankowych, która odcięłaby klientom dostęp do posiadanych zasobów finansowych. W okresie pandemii COVID-19 niektóre osoby zostały zmuszone do takiej formy bankowości poprzez nałożoną kwarantannę, zamknięcie stacjonarnych sklepów specjalistycznych (meblowe, sportowe) czy też oddolnymi restrykcjami w niektórych punktach handlowych odmawiających przyjmowania gotówki.

Inną formą obowiązkowej przemiany w e-obywatela w trakcie COVID-19 stało się nauczanie zdalne. Wymagające z dnia na dzień od rodziców, dzieci oraz nauczycieli biegłej obsługi sprzętu multimedialnego, posiadania odpowiedniego sprzętu (komputera, kamerki, mikrofonu) i stabilnego podłączenia do sieci teleinformatycznej. Dodatkowo sprawy uczniów zaczęły być intensywnie załatwiane poprzez e-dzienniki. W celu realizacji materiału nauczania zaistniała konieczność założenia dzieciom internetowych kont na platformach szkoleniowych takich jak MS Teams czy Google ZOOM. W czasie zajęć dzieci musiały udostępniać swój wizerunek oraz głos. Realizacja sprawdzianów i rozliczenie z przedmiotu często były realizowane przez odesłanie nauczycielowi wypełnionego oraz zeskanowanego materiału. Taka sytuacja spowodowała masowe przetwarzanie danych osobowych dzieci z wykorzystaniem sieci internetowej.

¹³ A. Marciniak, *Badania Mastercard: W pandemii Polacy częściej korzystają z cyfrowej bankowości*, <https://newsroom.mastercard.com/eu/pl/news-briefs/badanie-mastercard-w-pandemii-polacy-czesciej-korzystaja-z-cyfrowej-bankowosci> (dostęp: 29.05.2021).

Osobliwą kwestią funkcjonowania Polaków w świecie cyfrowym są e-Biura Obsługi Klienta. Zasadniczo każdy liczący się współcześnie usługodawca posiada taką formę kontaktu z klientem. Są to banki, elektrownie, gazociągi, wodociągi, dostawcy usług teleinformatycznych i e-sklepy. W każdym z tych miejsc są przetwarzane dane osobowe obywateli, często w powiązaniu z danymi finansowymi.

Bezpieczny obywatel?

Przy tak intensywnym wykorzystaniu w Polsce e-usług o charakterze rządowym i komercyjnym rodzi się pytanie, czy obywatele są bezpieczni? Wykorzystanie nowych technologii w celu usprawnienia życia społecznego wymaga od administracji państwowej oraz komercyjnego sektora usług technologicznych odpowiedzialności i właściwego zabezpieczenia danych¹⁴. Możliwości, jakie oferują usługi informatyczne w postaci ogromnej bazy danych oraz zmagazynowanej cyfrowo wiedzy o obywatelach, stanowią również bardzo atrakcyjny materiał dla grup przestępczych oraz organizacji terrorystycznych¹⁵. Coraz szersze zastosowanie technologii cyfrowej w postaci przetwarzania nieskończonej ilości danych dotyczących obywateli wpływa na rozwój takich zjawisk, jak:

- cyberprzestępczość: kradzieże, oszustwa, wyłudzenia za pomocą wykorzystania urządzeń elektronicznych;
- cyberterroryzm: ataki hakerskie o charakterze kryminalnym bądź terrorystycznym;
- wykorzystanie danych w celu zastosowania socjotechniki (manipulacja, wpływ);
- próby kontroli nad obywatelami;
- niekontrolowany wyciek danych.

W zakresie bezpieczeństwa e-obywatela przy tak ogromnej ilości przetwarzanych danych należy rozważyć również tą problematykę w ujęciu socjotechniki. Socjotechnika jest zbiorem technik oraz wiedzy na temat procesów przyczynowo-skutkowych w celu oddziaływania na postawy oraz zachowania ludzi¹⁶. Socjotechnika jest sposobem sprawowania władzy przez polityków poprzez

¹⁴ H.M. Karwan, *Nowe technologie a bezpieczeństwo kulturowe państwa*, w: Marek H., Szulca M. (red.), *Edukacja dla bezpieczeństwa. Edukacja dla bezpieczeństwa kulturowego*, Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2018, s. 33–49.

¹⁵ Tamże.

¹⁶ Ł. Scheffs, *Socjotechnika władzy*, „Przegląd Polityczny” 2016, nr 1, s. 35–45.

stosowanie odpowiedniej manipulacji wraz z wykorzystaniem danych w celu osiągnięcia pożądaných celów¹⁷. Z socjotechniką powiązana jest inżynieria społeczna, która jest nauką dobierania odpowiednich środków socjotechnicznych w celu osiągnięcia zakładanych korzyści¹⁸. Należy tu jeszcze przytoczyć zjawisko o nazwie Big Data. Jest ono trudne do jednoznacznego zdefiniowania i składa się z kilku procesów zachodzących obecnie na świecie w związku z masowym i globalnym wykorzystaniem nowoczesnych technologii¹⁹. Procesy te wiążą się z:

- bardzo dynamicznym wzrostem ilości przetwarzanych danych;
- powstaniem nowych technologii w celu przetwarzania danych;
- koniecznością magazynowania oraz archiwizowania coraz większej ilości danych, stale rosnącej;
- pojawianiem się nowych nieznaných dotąd źródeł danych, koniecznych do przetworzenia.

Syntezyując powyższe, Big Data jest zagadnieniem związanym z masowym przetwarzaniem danych informatycznych oraz procesami z tym związanymi. Przykładem wagi dostępu do danych związanych z inżynierią społeczną niech będzie fakt zakupu przez Grupę PKN Orlen (będącą spółką Skarbu Państwa) pod koniec 2020 r. spółki medialnej Polska Press, będącej wydawcą znacznej ilości tytułów prasowych i medialnych w Polsce. W ten sposób PKN Orlen uzyskała dostęp do ponad 17 mln użytkowników portali zarządzanych wcześniej przez Polska Press²⁰. Władze spółki wydały również w grudniu 2020 r. komunikat w tej sprawie: „Przejęliśmy spółkę Ruch, co ułatwi nam wejście na rynek nowych punktów sprzedaży i rozwój usług e-commerce. Z kolei dostęp do 17,4 milionów użytkowników portali zarządzanych przez Polska Press skutecznie wzmocni sprzedaż całej Grupy ORLEN, zoptymalizuje koszty marketingowe i umożliwi dalszą rozbudowę narzędzi Big Data. Podejmujemy działania, które wpisują się w nową strategię PKN ORLEN do 2030 r. i będą efektywnie wspierać dynamiczny rozwój sieci detalicznej”²¹. Kluczową kwestią w przedstawionym

¹⁷ Tamże.

¹⁸ Tamże.

¹⁹ R. Żulicki, *Potencjał Big Data w badaniach społecznych*, „Studia Socjologiczne” 2017, nr 3(226), s. 175–202.

²⁰ PKN Orlen przejmuje Polska Press, <https://www.orlen.pl/PL/BiuroPrasowe/Strony/PKN-ORLEN-przejmuje-Polska-Press-.aspx> (dostęp: 29.05.2021).

²¹ Tamże.

komunikacie prasowym pozostają dwa sformułowania. Pierwsze to: „dostęp do 17,4 milionów użytkowników”, drugie to: „dalsza rozbudowa narzędzi Big Data”.

Wymienione zagrożenia związane z realizacją usługi e-obywatel w Polsce w powiązaniu z przedstawionymi zagadnieniami socjotechniki, inżynierii społecznej oraz Big Data nasuwają pytanie, czy społeczeństwo polskie (oraz inne narody z uwagi na światowy trend) nie zmierza w kierunku permanentnej inwigilacji niczym w książce George Orwella *Rok 1984*, w której to przedstawiono, iż władza (Wielki Brat) wszystko widzi poprzez system połączonych teleekranów przesyłający tej władzy obraz i dźwięk z miejsc publicznych i z „zaczisza” domowego. Dodatkowo władza realizuje permanentną cenzurę mediów oraz kontroluje obywateli za wykorzystaniem Policji Myśli²².

Podsumowanie

Niewątpliwie zachodząca obecnie czwarta rewolucja przemysłowa związana z technologiami cyfrowymi stanowi wyzwanie związane z permanentną inwigilacją społeczeństw²³.

Przedstawione w artykule systemy działające niezależnie i bezpiecznie nie są groźne dla obywatela, jednakże połączenie np. systemu e-pacjent z jednoczesną kontrolą finansową systemów bankowych oraz aplikacją śledzącą na telefonie stanowi istotne zagrożenie. W ten sposób może spełnić się obywatelski scenariusz książki *Rok 1984* autorstwa Georga Orwella. Przykładem realnym może być „System Zaufania Społecznego” w wydaniu Chińskiej Republiki Ludowej, będący zasadniczo systemem kontroli społecznej sprawowanej nad obywatelami przez władze kraju. Innym przykładem jest Izrael, gdzie funkcjonuje system „zielonej” przepustki dla osób zaszczepionych na COVID-19 oraz metoda kontroli osób przybywających na kwarantannę za pomocą elektronicznej bransoletki. Unia Europejska opracowuje założenie systemu z rejestrem osób zaszczepionych, które będą mogły korzystać z większych swobód obywatelskich niż osoby niezaszczepione tzw. Paszporty Covidowe. Administracja rządowa oraz samorządowa w Polsce z wykorzystaniem coraz większego zasobu aplikacji mających pomagać w walce z pandemią COVID-19 i tworzeniu systemów

²² G. Orwell, *Rok 1984*, Wydawnictwo Agora, Warszawa 2004, s. 5–19.

²³ E. Jeliński, *Kilka uwag o konsekwencjach czwartej rewolucji przemysłowej*, w: Kamprowski R., Skarżyński M. (red.), *Wykorzystanie dronów i robotów w systemach bezpieczeństwa. Wybrane aspekty*, Poznań 2019, s. 7–13.

informatycznych e-obywatela również coraz mocniej ingeruje w wolność i bezpieczeństwo osobiste Polaków, jednocześnie wymuszając na nich konieczność stosowania najnowszych rozwiązań technologicznych. Rządowe oraz komercyjne bazy danych oparte o systemy informatyczne posiadają dane wrażliwe Polaków, co w przypadku awarii tychże systemów bądź nieuprawnionego ich użycia może doprowadzić do poważnego zagrożenia bezpieczeństwa oraz wolności obywateli polskich. Z uwagi na dynamikę zmian związanych z COVID-19 opracowanie to (stan na maj 2021 r.) w momencie opublikowania może wymagać dalszych analiz i rozważań.

Bibliografia

- Aplikacja Kwarantanna Domowa*, <https://www.gov.pl/web/koronawirus/kwarantanna-domowa> (dostęp: 29.05.2021).
- Domowa Opieka Medyczna*, <https://www.gov.pl/web/domowaopiekamedyczna> (dostęp: 29.05.2021).
- E-deklaracje*, <https://www.podatki.gov.pl/e-deklaracje> (dostęp: 29.05.2021).
- E-usługowe podsumowanie 2020 r.*, <https://www.gov.pl/web/cyfryzacja/e-uslugowe-podsumowanie-2020-r> (dostęp: 29.05.2021).
- Jeliński J., *Kilka uwag o konsekwencjach czwartej rewolucji przemysłowej*, w: Kamprowski R., Skarżyński M. (red.), *Wykorzystanie dronów i robotów w systemach bezpieczeństwa. Wybrane aspekty*, Poznań 2019.
- Kamprowski R., Skarżyński M. (red.), *Wykorzystanie dronów i robotów w systemach bezpieczeństwa. Wybrane aspekty*, Wydawnictwo Naukowe WNiPD UAM, Poznań 2019.
- Karwan H.M., *Nowe technologie a bezpieczeństwo kulturowe państwa*, w: Marek H., Szulca M. (red.), *Edukacja dla bezpieczeństwa. Edukacja dla bezpieczeństwa kulturowego*, Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2018.
- Marciniak A., *Badania Mastercard: W pandemii Polacy częściej korzystają z cyfrowej bankowości*, <https://newsroom.mastercard.com/eu/pl/news-briefs/badanie-mastercard-w-pandemii-polacy-czesciej-korzystaja-z-cyfrowej-bankowosci> (dostęp: 29.05.2021).
- Ministerstwo Cyfryzacji, <https://obywatel.gov.pl> (dostęp: 29.05.2021).
- Ministerstwo Zdrowia i Narodowy Fundusz Zdrowia, <https://pacjent.gov.pl> (dostęp: 29.05.2021).

Orwell G, *Rok 1984*, Wydawnictwo Agora, Warszawa 2004.

PKN Orlen przejmuje Polska Press, <https://www.orlen.pl/PL/BiuroPrasowe/Strony/PKN-ORLEN-przejmuje-Polska-Press-.aspx> (dostęp: 29.05.2021).

Scheffs Ł., *Socjotechnika władzy*, „Przegląd Polityczny” 2016, nr 1.

STOP COVID, <https://www.gov.pl/web/protegosafe> (dostęp: 29.05.2021).

Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020 r., poz. 374, z późn. zm.

Załatw sprawy urzędowe przez internet na ePUAP, <https://www.gov.pl/web/gov/zalatwiaj-sprawy-urzedowe-przez-internet-na-epuap> (dostęp: 29.05.2021).

Żulicki R., *Potencjał Big Data w badaniach społecznych*, „Studia Socjologiczne” 2017, nr 3 (226).

E-citizen and safe citizen—application of technological solutions during the COVID-19 pandemic

Abstract: The period of the COVID-19 pandemic accelerated and at the same time increased the use of electronic channels to handle various official matters. A number of various government applications have been prepared specifically for this purpose. The scope of the use of electronic banking has also increased – payments with payment cards and making online purchases. All the mentioned systems are designed to facilitate and speed up the way citizens deal with various matters. However, they can be used to steal citizens' personal and other information, for social engineering, or worse, for citizen control. The work uses a research methodology based on theoretical methods such as the analysis of the literature on the subject or public data on applications and Internet solutions used during the COVID-19 pandemic. In the field of empirical research, the observation of existing technological solutions was carried out, as well as the method of the experiment consisting in checking the functioning of the above-mentioned Internet systems and telephone applications in practice. This allowed for a synergistic presentation of the problem and for drawing conclusions.

Key words: e-citizen, cybersecurity, COVID-19, applications, IT systems

dr hab. Aleksandra Skrabacz, prof. AP

Akademia Pomorska w Słupsku

Instytut Bezpieczeństwa i Zarządzania, Katedra Bezpieczeństwa Narodowego

e-mail: aleksandraskrabacz@interia.pl

ORCID: 0000-0001-5958-810X

Rozdział 8

Wybrane aspekty zachowań psychospołecznych młodych Polaków w dobie pandemii koronawirusa

Streszczenie: Ze względu na nowe i masowe zjawisko, jakim jest pandemia koronawirusa oraz kryzys nią wywołany w wielu obszarach funkcjonowania państwa i społeczeństwa, w artykule przedstawiono wyniki badań empirycznych przeprowadzonych na grupie respondentów będących studentami jednej z warszawskich szkół wyższych. Celem badań była diagnoza i ocena wpływu pandemii na wybrane dziedziny życia tej grupy społecznej, ze szczególnym uwzględnieniem pracy i nauki oraz relacji z ludźmi i sposobów spędzania czasu wolnego w okresie izolacji społecznej. Wyniki badań upoważniają do przedstawienia wniosków i uogólnień, które mogą być przydatne do prowadzenia badań porównawczych w innych środowiskach społecznych.

Słowa kluczowe: pandemia, studenci, izolacja społeczna, relacje interpersonalne

Wprowadzenie

Rok 2020 i 2021 upływają na świecie, w Europie i w Polsce pod znakiem walki z pandemią koronawirusa, która z niespotykaną od prawie 100 lat siłą zaatakowała państwa i społeczeństwa w wymiarze globalnym, regionalnym i indywidualnym¹. Praktycznie każda dziedzina życia, a zwłaszcza społecznego, gospodarczego, politycznego i kulturalnego, w większym lub mniejszym stopniu – w sposób bezpośredni lub pośredni – odczuła zagrożenie śmiertelnościami wirusem. Mimo wynalezienia szczepionek i rozpoczęcia programu masowych szczepień przyszłość jawi się jako stan niepewności i nieprzewidywalności.

Pandemia, pomimo usilnych prób zapanowania nad nią, w dalszym ciągu oddziałuje na wiele obszarów funkcjonowania państwa oraz jego suwerena, wpływając na kondycję kraju i poziom życia obywateli². Powszechne i globalne zagrożenie koronawirusem doprowadziło do nieodwracalnego przekształcenia świata oraz zmian w obszarach, które dla członków tzw. społeczeństw rozwiniętych były czymś oczywistym. Nagle pozamykane zostały restauracje, puby i bary, zajęcia w szkołach i na uczelniach zawieszono, praca zawodowa w pewnych sektorach przeniosła się z biur do domów, spacer po parkach i lasach stały się niemożliwe, tak samo jak wizyty w bibliotekach, muzeach, kinach, operach czy galeriach handlowych³. Na straży wprowadzonych obostrzeń stały służby mundurowe, władne wystawiać mandaty za czynności dotychczas w pełni legalne, jak spacer po terenach zielonych lub przejażdżki rowerowe⁴. Państwo, jako instytucja obdarzona monopolem na siłę, stało się przez swoje interwencje bardziej widoczne i sprawcze w codziennym życiu, co nie zawsze spotykało się ze zrozumieniem i akceptacją obywateli⁵.

¹ Brainerd E., Siegler M., *The Economic Effects of the 1918 Influenza Epidemic*, 2003, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=394606 (dostęp: 20.10.2020).

² A. Skrabacz, *Bezpieczeństwo społeczne. Postawy teoretyczne i praktyczne*, Warszawa 2012, s. 53.

³ <https://covid19psychologiacom.files.wordpress.com/2020/04/koronawirus-raport-2-jak-polacy-stosujac8-siecca8-do-zalencnc81-w-zwiacca8zku-z-ko....pdf> (dostęp: 25.05.2020).

⁴ Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020, poz. 374, 567, 568, 695 i 875.

⁵ A. Skrabacz, *Wpływ pandemii koronawirusa na wybrane aspekty bezpieczeństwa społeczno-ekonomicznego Polaków*, „Bezpieczeństwo. Teoria i Praktyka”, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2021, artykuł w druku.

Poparciem tych tez mogą być poglądy wyrażone przez Polaków na temat oceny roku 2020 oraz samopoczucia w tym okresie. Z badań przeprowadzonych przez Fundację Centrum Badania Opinii Społecznej (CBOS) wynika, że dla prawie 40% Polaków najważniejszym wydarzeniem minionego roku była pandemia koronawirusa oraz inne zdarzenia z nią związane. „Cieniem” epidemii, wskazywanym przez dalsze 1,8% Polaków, była kwestia jej gospodarczych skutków. Badani mówili o zamrożeniu gospodarki, kłopotach gospodarczych, spadku koniunktury, wspomniano o likwidacji miejsc pracy oraz jej utracie przez wielu Polaków, bankructwach przedsiębiorców w niektórych branżach, a także wzroście zadłużenia Polski⁶.

Z kolei w innym badaniu z 2020 r.⁷ Polacy – opisując nastroje panujące w ich otoczeniu – niemal w trzech czwartych (71%) wspominają o nastrojach negatywnych, takich jak lęk przed przyszłością (44%), ogólne niezadowolenie i brak wiary w jakąkolwiek poprawę (15%), czy też apatia, rezygnacja, pogodzenie się z własnym losem (12%). Porównując te dane z wynikami z roku 2019, można zauważyć wyraźny wzrost negatywnych ocen nastrojów środowiskowych, ogółem aż o 20 punktów procentowych. Uwagę zwracają zwłaszcza częstsze deklaracje panującego w otoczeniu badanych lęku przed przyszłością – mamy tutaj do czynienia ze skokiem o 14 punktów procentowych w stosunku do poprzedniego roku. O pozytywnych emocjach w swoim otoczeniu wspominał z kolei tylko niespełna co czwarty Polak (23%), wskazując na ogólne (4%) i pewne (19%) zadowolenie oraz odprężenie⁸.

Wśród wyników przytoczonych badań na szczególną uwagę zasługują dane uzyskane od jednej z grup społecznych poddanych badaniu, a mianowicie młodzieży w przedziale wiekowym od 18. do 24. roku życia. Autorzy badania zwracają uwagę, że najmłodsi respondenci, w przeciwieństwie do roku 2019, w kolejnym roku kalendarzowym nie wykazywali przeciętnie lepszego samopoczucia od osób starszych. Wyraźnie częściej doświadczali też niektórych negatywnych emocji, zwłaszcza poczucia bezradności (44% wobec 31% wśród ogółu), depresji (32% w stosunku do 21% wśród ogółu), a także zniechęcenia i znużenia (47% wobec 36% wśród ogółu). Warto dodać, że częstość odczuwania

⁶ K. Pankowski, *Rok 2020 pod znakiem pandemii*, Centrum Badania Opinii Społecznej, komunikat z badań, nr 15/2021, ISSN 2353-5822, Warszawa 2021, s. 1.

⁷ J. Scovil, *Samopoczucie Polaków w roku 2020*, Centrum Badania Opinii Społecznej, komunikat z badań, nr 1/2021, ISSN 2353-5822, Warszawa 2021, s. 7.

⁸ Tamże.

depresji, bezradności i znużenia osiągnęła wśród najmłodszych respondentów najwyższy poziom na przestrzeni ostatnich dwóch dekad. Można to wiązać z wyjątkowym doświadczeniem domowej izolacji, zdalnego nauczania i braku kontaktu z rówieśnikami, na które ta grupa badanych nie była we wcześniejszych latach narażona⁹.

Mając do dyspozycji dane z ogólnopolskich badań opinii publicznej oraz doświadczenia własne wynikające z pracy w roli nauczyciela akademickiego, od marca 2020 r. prowadzącego zajęcia dydaktyczne w trybie zdalnym, autorka niniejszego rozdziału podjęła wysiłek badawczy mający na celu weryfikację poglądów młodych ludzi – studentów – na temat wpływu pandemii koronawirusa na życie zawodowe i naukowe oraz relacje interpersonalne z bliższym i dalszym otoczeniem społecznym. W ramach badań poszukiwano odpowiedzi na następujące problemy badawcze:

1. Jakie zmiany u badanych przyniosła pandemia COVID-19 w obszarze pracy, nauki, hobby oraz kontaktów interpersonalnych?
2. Jak respondenci oceniają zmiany wymuszone przez pandemię w badanych obszarach?
3. Jak oceniają stan izolacji społecznej i czym on się charakteryzuje?
4. Czy i w jaki sposób zmieniły się kontakty z domownikami, bliską rodziną oraz przyjaciółmi i znajomymi?
5. W jaki sposób badani spędzali czas wolny, pozostając w izolacji społecznej?

Główną tezę, wokół której koncentrowały się niniejsze rozważania, było podsumowanie zawarte w raporcie CBOS: „Szczególną uwagę zwraca najmłodsza grupa badanych, w wieku 18–24 lata, w której częstość występowania stanów depresyjnych, poczucia bezradności, a także zniechęcenia i znużenia osiągnęła najwyższe poziomy na przestrzeni ostatnich dwóch dekad”¹⁰. W trakcie realizacji procesu dydaktycznego wielokrotnie istniała możliwość wymiany poglądów na temat obecnej sytuacji pandemicznej, jak również było możliwe prowadzenie obserwacji młodych ludzi, którzy doświadczają tak skrajnych i często negatywnych przeżyć, z jakimi mają do czynienia w tym trudnym dla wszystkich czasie.

Zatem chcąc rozwiązać przyjęte problemy badawcze, w pracy zastosowano interdyscyplinarne metody badawcze, w tym intuicyjne, komparatystyczne

⁹ Tamże, s. 6.

¹⁰ Tamże, s. 10.

i obserwacyjne, przy wykorzystaniu dostępnych parametrów liczbowych. Mają one zapewnić zarówno efektywność poznawczą, jak i pragmatyczną. Wśród metod empirycznych wybrano metodę sondażu diagnostycznego techniką ankietowania, z wykorzystaniem kwestionariusza ankiety.

Badania przeprowadzone na jednej z warszawskich uczelni technicznych, wśród studentów pierwszego i drugiego stopnia nauczania, studia stacjonarne i niestacjonarne, na kierunku bezpieczeństwo narodowe, z którymi autorka niniejszego opracowania w semestrze letnim prowadziła zajęcia dydaktyczne. W badaniu, przeprowadzonym w dniach 13 i 18 kwietnia 2021 r., wzięło udział 115 respondentów, spośród których 47 osób stanowiły kobiety (41%), a mężczyźni tworzyli grupę 68-osobową (59%). Rozkład wieku przedstawiał się następująco: od 20 do 24 lat było 76 osób (66%), w przedziale 25–30 lat – 39 osób (34%). Z wykształceniem wyższym licencjackim było 39 osób, co stanowiło 34%, reszta grupy badawczej posiadała wykształcenie średnie (66%). Wszyscy ankietowani pochodzili z miast powyżej 200 000 mieszkańców.

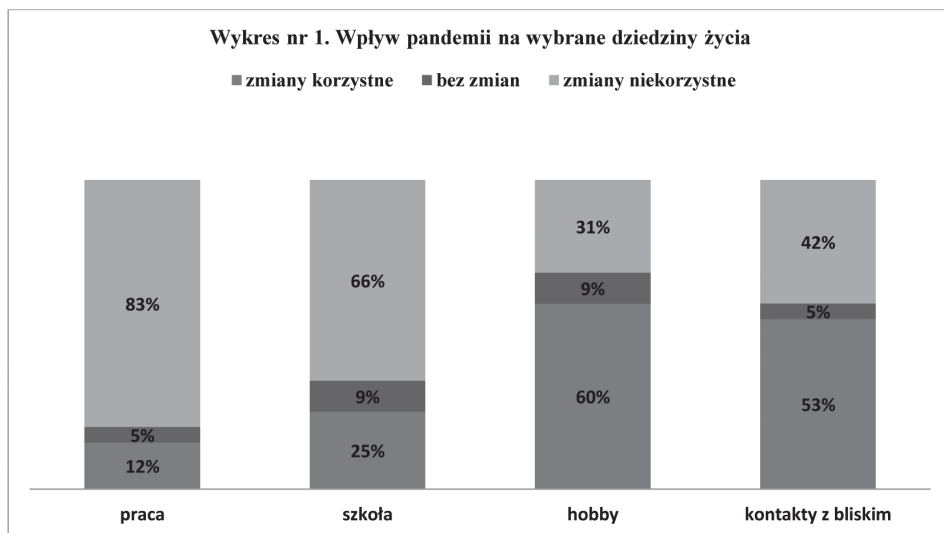
W badaniu udział brały osoby aktywne zawodowo oraz studiujące, z czego 86% ankietowanych były to osoby studiujące i pracujące zawodowo, natomiast 14% tylko studiujące. Osoby aktywne zawodowo reprezentowały: administrację publiczną – 35%, usługi – 20%, przemysł – 10%, transport – 10%, handel – 10% ochronę zdrowia – 5%, edukację – 5%, służby mundurowe – 5%.

Kwestionariusz ankiety składał się z 11 pytań zamkniętych, w tym jednego wielokrotnego wyboru. Ankieta została przygotowana oraz udostępniona online za pomocą sieci Internet.

Wyniki badań empirycznych

We wprowadzeniu skonstatowano, że rok 2020 zapisze się na kartach globalnej historii pod hasłem „COVID-19”. Pandemia, która dotknęła świat, zmieniła życie ludzi nie do poznania. Wszyscy musieli nauczyć się żyć w nowej rzeczywistości, w której dla bezpieczeństwa swojego, rodziny i bliskich oraz wszystkich innych, zmuszeni byli zostać w domu. Tylko dzięki nowoczesnej technologii, wszystkie te osoby miały możliwość dalszego realizowania się na polu zawodowym i naukowym. Stąd też pytania zadane respondentom oscylowały wokół problematyki pracy, nauki, samopoczucia, sytuacji rodzinnej, sposobu spędzania wolnego czasu podczas kwarantanny narodowej i przymusu pozostania w domu.

Istotnym problemem wymagającym diagnozy była kwestia zmian w wybranych dziedzinach życia, które były wywołane pandemią koronawirusa. Respondentów poproszono o wskazanie, czy w ich pracy, nauce, hobby lub kontaktach z bliskimi nastąpiły zmiany i jak je wartościują. Rozkład uzyskanych odpowiedzi prezentuje wykres nr 1.



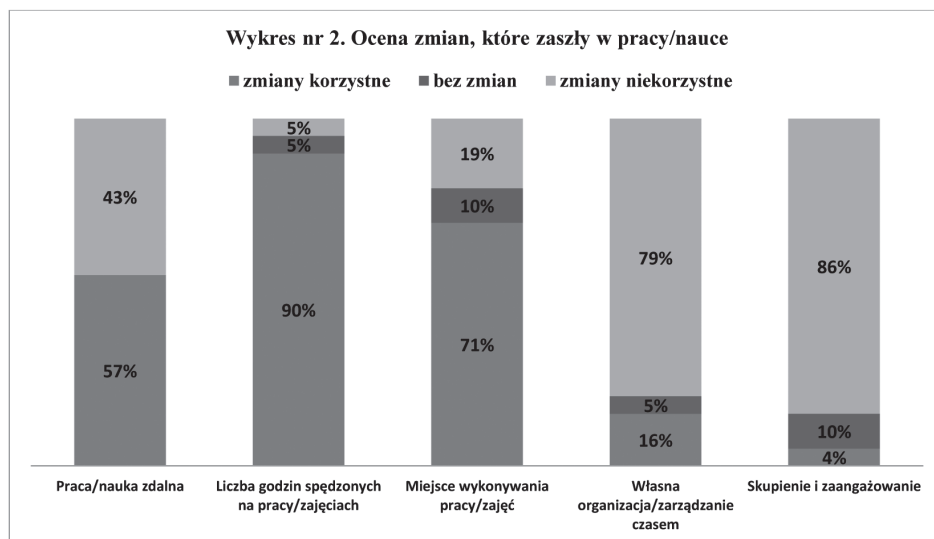
Źródło: Opracowanie własne.

Z uzyskanych odpowiedzi wynika, że największe zmiany pozytywne zaszły w realizacji hobby – 66% odpowiedzi, a także w kontaktach z bliskimi – 53% wskazań. Pozytywne zmiany w szkole wskazało 25% osób, a w pracy – tylko 12%. Jeżeli chodzi o zmiany niekorzystne, to w tej kategorii 83% badanych oceniło, że pandemia niekorzystnie wpłynęła na ich pracę, a także naukę – 66% wskazań. Ponadto 40% badanych uważa, że pogorszeniu uległy także relacje z bliskimi oraz realizacja hobby – 31% wskazań.

Wniosek: pandemia koronawirusa ze względu na swój charakter oraz rozwój sprawiła, że wiele osób obawiało się o pracę i naukę, co było pochodną zamrożenia przede wszystkim takich gałęzi gospodarki jak handel i usługi. Z kolei brak stabilnych podstaw egzystencjalnych implikował obawy o kontynuację nauki na studiach, potęgując stres wywołany globalnym zagrożeniem. Brak możliwości spędzania czasu wolnego w przestrzeni publicznej z kolei pozytywnie wpłynął

na rozwój zainteresowań i częstsze kontakty z bliskimi, w dużej mierze podyktowane też troską o ich zdrowie i życie.

Kolejną kwestią poddaną badaniu była ocena zmian, które zaszły w dwóch istotnych dla respondentów obszarach, mianowicie pracy i nauce. Wyniki zaprezentowano na wykresie nr 2.



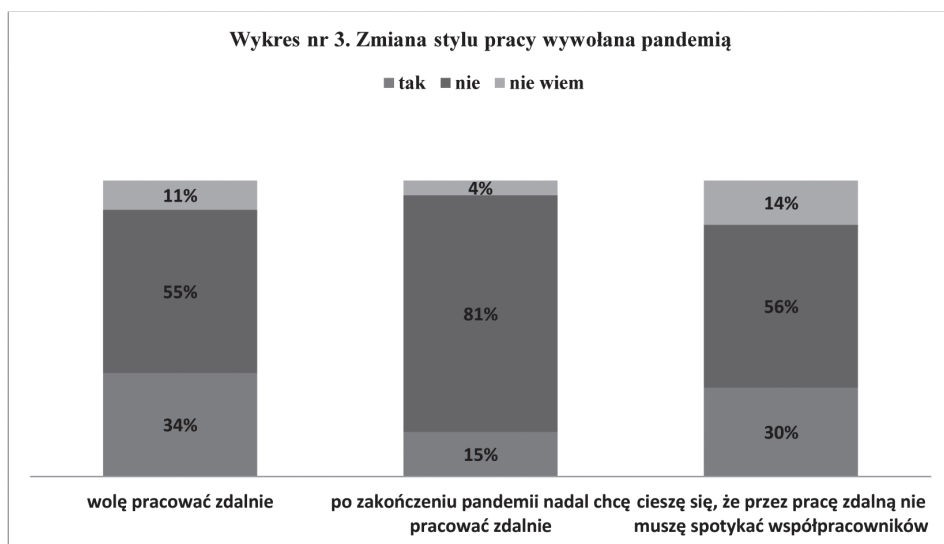
Źródło: Opracowanie własne.

Oceniając zmiany, które zaszły w zakresie pracy i nauki, warto zwrócić uwagę, że respondenci najkorzystniejsze zmiany zauważyli w liczbie godzin spędzonych na pracy lub zajęciach (90% wskazań), następnie w zakresie miejsca, w którym te czynności wykonywali (71% wskazań) oraz w ogóle w pracy i nauce zdalnej (57%). Jeżeli chodzi o zmiany niekorzystne, to najwyższe wskaźniki odnotowano w zakresie skupienia i zaangażowania w pracę i naukę (86%) oraz w zakresie własnej organizacji i zarządzania czasem (79%). Niewielka liczba osób (od 5% do 10%) uznała, że w tych obszarach nie zaszły żadne zmiany.

Wniosek: Zmiany, które zaszły w życiu studenckim i zawodowym respondentów wynikają przede wszystkim ze sposobu nauczania (tryb zdalny) oraz po części z wykonywania pracy w czasie pandemii. Zmiany te zostały w większości ocenione jako pozytywne, w tym szczególnie w zakresie ilości godzin spędzonych na wykonywaniu ww. czynności. Może się to wiązać z oszczędno-

ścią czasu, którą niesie ze sobą tryb nauki i pracy zdalnej, redukujący straty czasowe związane z dojazdem do uczelni i pracy. Korzystnie oceniono również miejsce wykonywania pracy i nauki, co wiąże się najczęściej z warunkami domowymi. Natomiast zdecydowana większość badanych, bo prawie ponad 80%, niekorzystnie oceniła swą organizację i zarządzanie czasem oraz skupienie i zaangażowanie. Jest to również w pełni zrozumiałe, gdyż warunki domowe, zwłaszcza gdy w jednym pomieszczeniu przebywa kilka osób, w tym dzieci, nie sprzyjają koncentracji na pracy i nauce, a dodatkowo pojawia się czynnik rozleniwienia, na co wskazały inne dane.

Pytanie kolejne dotyczyło zmiany stylu pracy w związku z pandemią koronawirusa. Na wykresie nr 3 zaprezentowano otrzymane wyniki.



Źródło: Opracowanie własne.

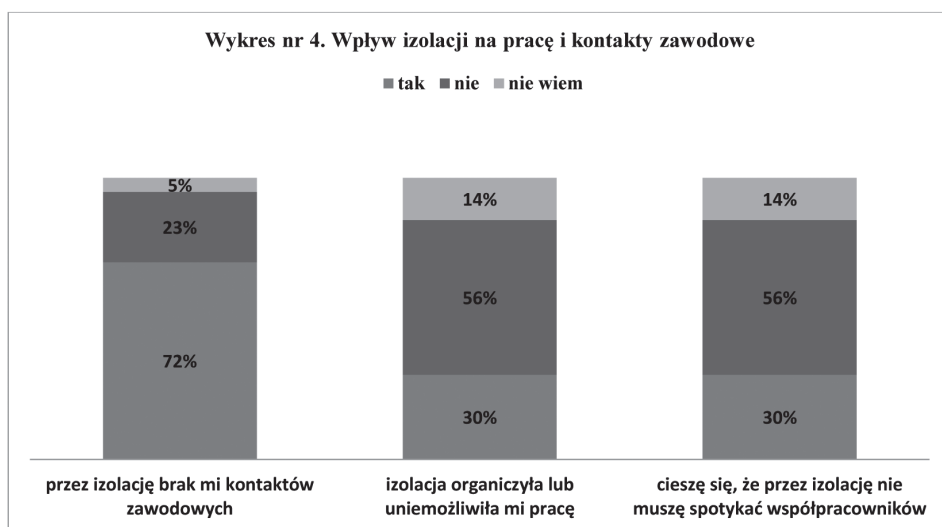
Oceniając zdalną formę wykonywania obowiązków zawodowych, 34% respondentów stwierdziło, że woli tak pracować, ale tylko 15% badanych po zakończeniu pandemii w dalszym ciągu przy takim sposobie pracy chciałoby pozostać. Ponadto 30% uczestników badania stwierdziło, że dzięki takiemu stylowi pracy nie muszą spotykać swych współpracowników, z czego się cieszą.

Odmiennego zdania była 55% grupa respondentów, którzy nie są zadowoleni ze zdalnej formy pracy, jak również z tego, że nie spotykają się z kolegami z pracy. Warto również podkreślić, że aż 80% badanych nie chce w czasie

postpandemicznym nadal pracować online. Jeżeli chodzi o procent osób, które nie miały zdania na powyższe tematy, to 10% nie wiedziało, czy woli pracować zdalnie, czy też nie, 4% nie potrafiło wskazać, czy chcą po zakończeniu pandemii dalej pracować zdalnie, a 14% nie miało zdania w sprawie spotykania się ze współpracownikami.

Wniosek: podsumowując wyniki otrzymane w kwestii pracy zdalnej, można stwierdzić, że respondenci – tak jak większość społeczeństwa – nie mieli możliwości wyboru trybu pracy, ponieważ forma zdalna była często jedynym sposobem na jej realizację. Warto podkreślić, że zdecydowana większość badanych, bo aż 80%, wyraża chęć powrotu do pracy w formie tradycyjnej, wraz z codziennymi bezpośrednimi kontaktami ze współpracownikami.

Kolejnym problemem wymagającym diagnozy, związanym z aktywnością zawodową, była kwestia wpływu izolacji na pracę i kontakty zawodowe. Rozkład odpowiedzi na to pytanie przedstawia wykres nr 4.



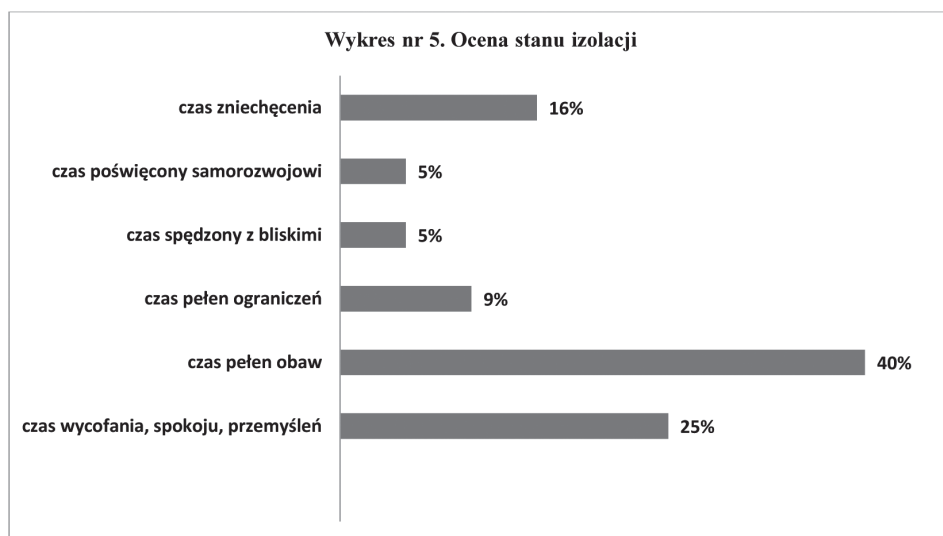
Źródło: Opracowanie własne.

Dla 30% badanych izolacja ograniczyła, a nawet uniemożliwiła wykonywanie obowiązków zawodowych, co jest szczególnie charakterystyczne dla zawodów z grupy usług handlowych czy gastronomicznych, podejmowanych najczęściej przez ludzi młodych. Dla 56% osób do takich sytuacji nie doszło, co może wskazywać na wykonywanie zdalnej pracy. Warto jednak podkreślić, że

mimo tego, że respondenci mogli pracować, to 72% badanych stwierdziło, że przez izolację brak im kontaktów zawodowych. Odmiennego zdania było 23% osób, a 5% nie miało zdania w tej sprawie. Jeżeli chodzi o kwestię spotykania się ze współpracownikami, to uzyskano taki sam rozkład odpowiedzi jak we wcześniejszym pytaniu.

Wniosek: Zamrożenie przez wiele miesięcy strategicznych dziedzin gospodarki, takich jak handel, gastronomia czy turystyka sprawiło, że zakończyła się era pracownika, na którego praca czekała, a zaczął się czas poszukiwania miejsca pracy, tak aby zapewnić podstawy egzystencji sobie i rodzinie. Problem ten jest szczególnie widoczny w środowisku młodych ludzi, często studentów, którzy dzięki pracy mogli pozwolić sobie na studiowanie. Pod koniec roku akademickiego 2020/2021 jest już widoczny odpływ studentów, którzy zostali zmuszeni do podjęcia drastycznych decyzji o rezygnacji z dalszego kształcenia się właśnie ze względu na brak pracy oraz drogie koszty życia w dużych ośrodkach akademickich.

W jednym z kolejnych pytań respondentów poproszono o ocenę stanu izolacji społecznej. Wyniki zamieszczono na wykresie nr 5.



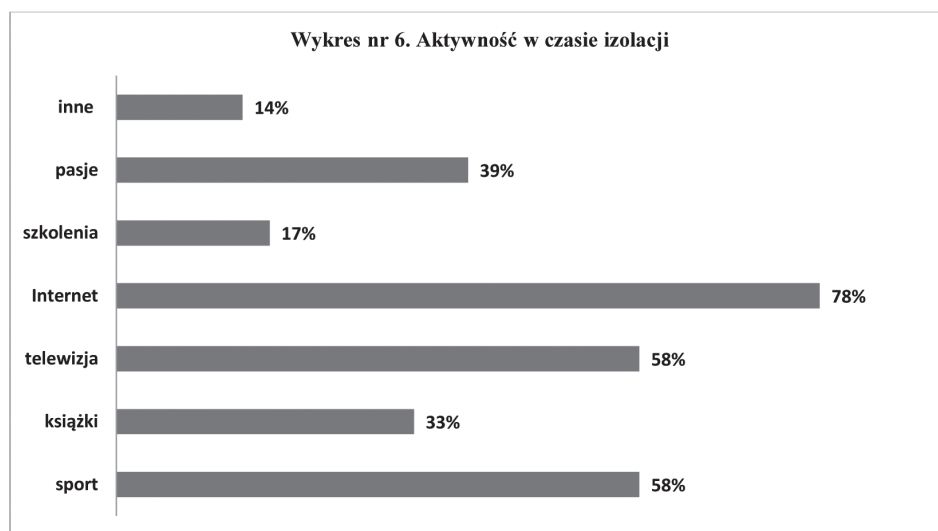
Źródło: Opracowanie własne.

Czas izolacji społecznej, trwający ponad rok, sprawił, że kondycja psychiczna wielu osób znacznie się pogorszyła. Mogą o tym świadczyć odpowiedzi re-

spodentów na pytanie o ocenę stanu izolacji. Respondenci mając do wyboru dysjunktywną kafeterię, uznali, że okres izolacji był to czas przede wszystkim pełen obaw (40% wskazań), czas wycofania, spokoju i przemyśleń (25%), czas zniechęcenia (16%) oraz czas pełen ograniczeń (9%). Zaledwie po 5% respondentów wskazało na czas spędzony z bliskimi i czas na samorozwój.

Wniosek: Długotrwały czas pandemii, której towarzyszył okres napięcia psychicznego oraz obaw o życie i zdrowie swoje i najbliższych, może stanowić problem społeczny w dłuższej perspektywie czasowej. Zagrożenie kolejnymi falami zachorowań nie tylko nie uspokaja sytuacji, ale często – podsycane niesprawdzonymi informacjami – może prowadzić do jeszcze większej traumy społecznej. Tym samym potwierdziły się wyniki badań Fundacji CBOS dotyczące stanu zniechęcenia, przygnębienia, a nawet depresji występujące wśród najmłodszej grupy respondentów.

Narodowa kwarantanna wprowadziła przez wiele miesięcy znaczne ograniczenia w korzystaniu z miejsc publicznych, dóbr kultury i wielu obiektów sportowych. Stąd też pytanie o sposób spędzania czasu wolnego w okresie ograniczeń był kolejnym obszarem, który poddano badaniu. Otrzymane dane prezentuje wykres nr 6.

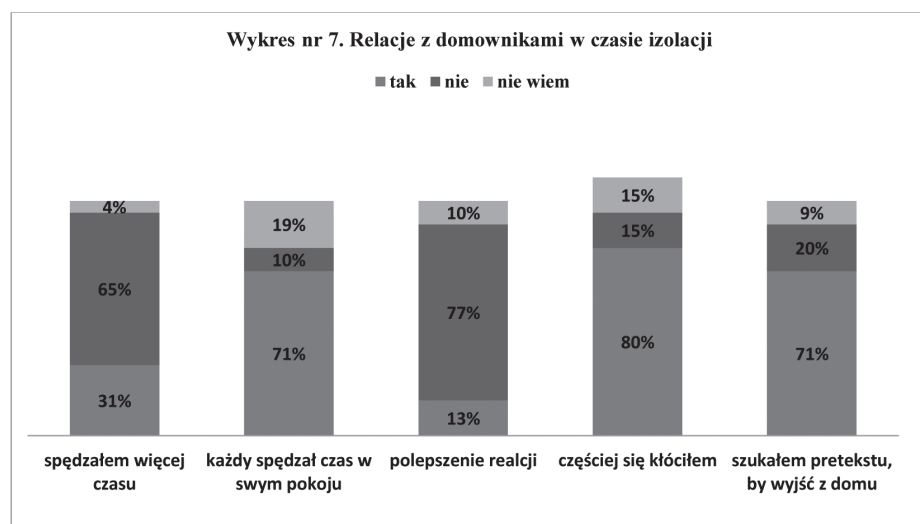


Źródło: Opracowanie własne.

Uzyskany rozkład odpowiedzi nie jest zaskoczeniem, ponieważ badania potwierdziły, że aktywność respondentów widoczna była przede wszystkim w sieci, w której czas spędzało prawie 80% badanych. Na drugiej pozycji *ex aequo* uplasowały się oglądanie telewizji oraz uprawianie sportu. Jeżeli chodzi o aktywność fizyczną, to warto dodać, że była ona wykonywana przede wszystkim na świeżym powietrzu, ponieważ większość siłowni i sal gimnastycznych była zamknięta. Stąd też wielką popularnością cieszyły się siłownie domowe, *ad hoc* budowane w domach lub garażach, w których można było choć w taki sposób dbać o kondycję fizyczną. Na trzecim miejscu uplasowała się realizacja pasji – 39%, a zaraz za nimi czytanie książek – 33%.

Wniosek: cechą społeczeństwa informacyjnego jest spędzanie czasu online, a izolacja społeczna jeszcze bardziej umocniła i utrwaliła te zachowania. Na ile ten proces jest szkodliwy dla ludzi, a szczególnie młodych pokoleń, możemy przekonać się każdego dnia, przeglądając doniesienia prasowe o cyberprzemocy i innych formach zagrożeń cyfrowych. Kilkanaście miesięcy izolacji społecznej pogłębiło nieodwracalnie proces uzależnienia od sieci, co w krótszej i dłuższej perspektywie czasowej może mieć znaczące konsekwencje w realnym życiu dla każdego z nas.

Ocena relacji zachodzących między domownikami w czasie izolacji była szczególnie istotnym elementem poddanym badaniu. Na wykresie nr 7 przedstawione dane na ten temat.

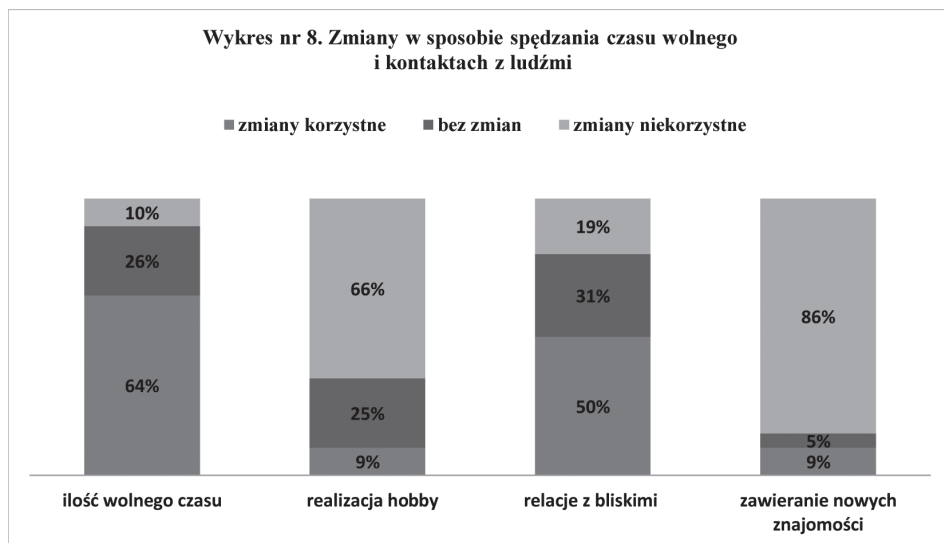


Źródło: Opracowanie własne.

Analiza uzyskanych odpowiedzi wskazuje, że zaledwie 31% badanych spędzało więcej czasu z domownikami, a dodatkowo tylko 13% osób wskazało, że ich relacje polepszyły się. W opinii 77% respondentów kontakty z innymi osobami będącymi we wspólnym gospodarstwie domowym pogorszyły się, 65% osób uważa, że nie spędzało więcej czasu z domownikami, ponieważ aż 71% respondentów spędzało czas w swoim pokoju. Z kolei 80% badanych wskazało, że częściej się kłócili, co skutkowało tym, że 71% osób szukało pretekstu, aby wyjść z domu.

Wniosek: Relacje z osobami zamieszkującymi w jednym gospodarstwie domowym stanowią jeden z najczęstszych konfliktogennych obszarów aktywności człowieka. W przypadku narzuconej odgórnie narodowej kwarantanny, problem tym bardziej się multiplikuje, gdy musimy przebywać w określonej, zamkniętej grupie ludzi przez dłuższy czas, bez możliwości oddalenia się od siebie na więcej niż kilka metrów. Szczególnego znaczenia problem ten nabiera w związkach patogennych, w których do konfliktów dochodzi nie tylko między partnerami, ale również między nimi i ich dziećmi.

Pytanie o zmiany w sposobie spędzania czasu wolnego oraz kontaktach z ludźmi stanowił kolejny problem, do którego mieli się ustosunkować badani. Otrzymane odpowiedzi prezentuje wykres nr 8.



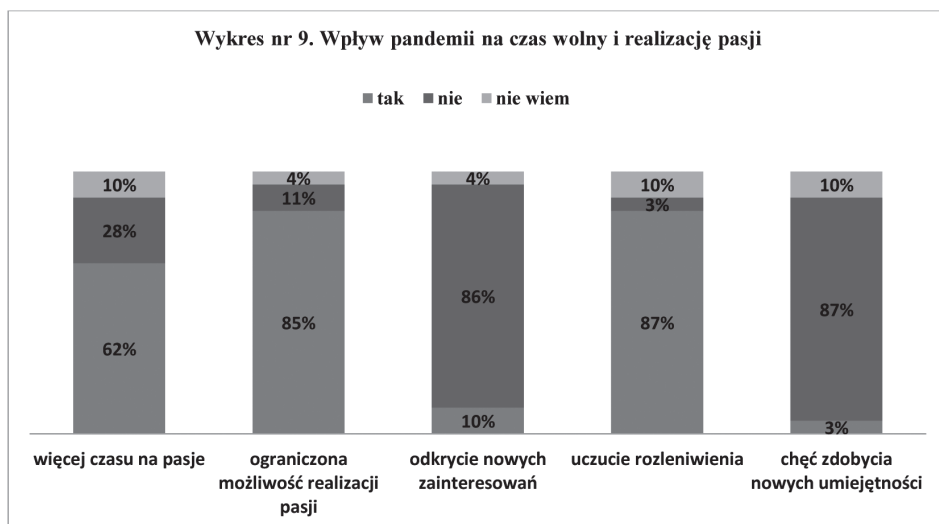
Źródło: Opracowanie własne.

Analizując kwestię ilości wolnego czasu, 64% respondentów wskazało, że zmieniło się to na korzyść, 26% uznało, że jest bez zmian, a tylko 10%, że są to zmiany niekorzystne. Kolejna kwestia dotyczyła możliwości realizacji hobby, na co 66% osób stwierdziło, że zmiany w tym zakresie są niekorzystne, a tylko 9% było odmiennego zdania. Dla 25% respondentów sytuacja pozostała bez zmian. Jeżeli chodzi o ocenę relacji z bliskimi, to dla 50% badanych polepszyły się one, dla 31% pozostały bez zmian, natomiast 19% badanych odczuło pogorszenie kontaktów z bliskimi. Dość jednoznacznie rozłożyły się odpowiedzi o ocenę możliwości zawierania nowych znajomości, ponieważ aż 86% badanych wskazało, że odczuli zmiany na gorsze, tylko 9% na lepsze, a dla 5% badanych wszystko pozostało bez zmian.

Wniosek: Można zauważyć, że choć badani w większości mieli więcej wolnego czasu, to i tak ze względu na ograniczenia pandemiczne nie mogli go wykorzystać na realizację hobby i rozwój innych zainteresowań. Natomiast relacje z bliskimi dla połowy badanych zmieniły się na korzyść, a dla innych pozostały bez zmian (30%) lub się pogorszyły (20%). Z dużą dozą prawdopodobieństwa można przypuszczać, że wpływ na taką ocenę miały warunki bytowe, w jakich przyszło spędzać izolację lub kwarantannę, które w przypadku wielu osób nie były komfortowe. Jeżeli chodzi o zawieranie nowych znajomości, to wyniki badań wskazują jednoznacznie, że był to trudny okres dla tego typu czynności i pomimo spędzania czasu wolnego przede wszystkim w internecie, a co za tym idzie możliwości zawierania znajomości online, to brak kontaktów osobistych był znacznym organicznikiem takich relacji.

Ocena wpływu pandemii na czas wolny i realizację pasji była kolejną kwestią poddaną badaniu. Wyniki zaprezentowano na wykresie nr 9.

Respondenci ustosunkowując się do tego problemu, w 62% stwierdzili, że choć mogli poświęcić więcej czasu na pasje, to jednak aż 85% uznała, że była ograniczona możliwość ich realizacji. Wynika to oczywiście z prostego faktu, że wiele obiektów użyteczności publicznej było w lockdownie, stąd też nie były dostępne lub ich działalność była znacznie ograniczona. Przeciwnego zdania było odpowiednio 28% badanych, którzy uważali, że mieli mniej czasu na pasje, a 11% uznało, że nie było ograniczeń w realizacji hobby. Warto również dodać, że zdaniem 87% osób czas pandemii nie był dobry do odkrywania nowych zainteresowań lub zdobywania nowych umiejętności, co można w pełni uzasadnić panującą sytuacją zamrożenia określonych dziedzin gospodarki, kultury i sportu. Również dla 87% badanych izolacja przyczyniła się do uczucia



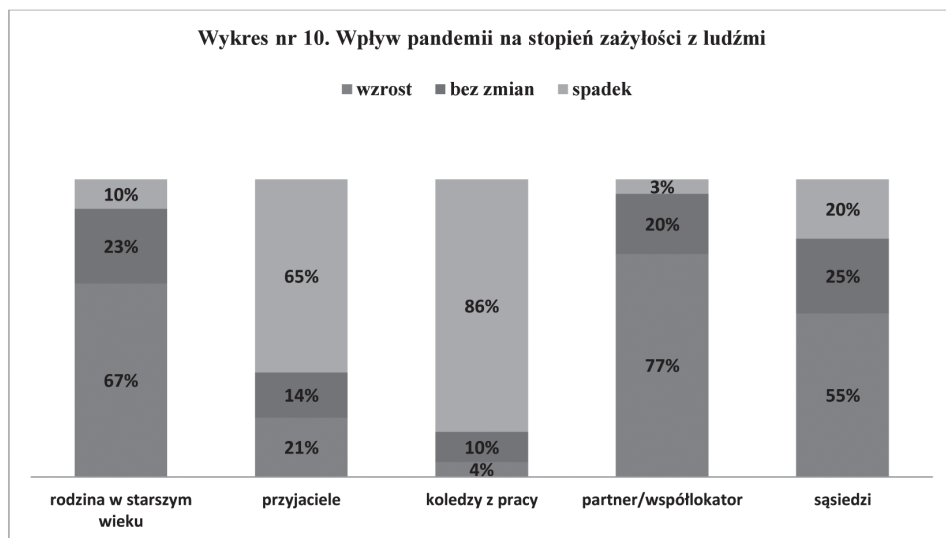
Źródło: Opracowanie własne.

rozleniwienia, czemu sprzyjało surfowanie po internecie lub oglądanie telewizji, jak to wynika z innych danych.

Wniosek: Czas izolacji społecznej ujawnił wiele interesujących zachowań społecznych, wśród których z jednej strony można było zaobserwować zrozumienie dla sytuacji i konieczności pozostawania w domu. Z drugiej strony szczególnie ludzie młodzi nie mogli pogodzić się i zrozumieć, dlaczego ich aktywność fizyczna czy towarzyska została tak restrykcyjnie ograniczona. Długotrwałość takiej sytuacji sprawiła, że wśród młodzieży zaczęło panować uczucie rozleniwienia i „nic nierobienia”, czemu sprzyjały okoliczności zewnętrzne, związane z brakiem możliwości realizacji zainteresowań na wielu polach aktywności.

Relacje interpersonalne z bliższym i dalszym otoczeniem to kolejna kwestia poruszana w przedmiotowym badaniu. Respondenci zostali poproszeni o ocenę, w jaki sposób pandemia wpłynęła na stopień ich zażyłości z ludźmi.

Otrzymane wyniki pozwalają stwierdzić, że w relacjach z osobami z najbliższego kręgu, to znaczy partnerem lub sublokaterem, rodziną w starszym wieku oraz sąsiadami nastąpił wzrost kontaktów, na co wskazało odpowiednio 77%, 67% i 55% respondentów. Z kolei jeżeli chodzi o stopień zażyłości w czasie pandemii z przyjaciółmi i kolegami z pracy, to można w tym obszarze zauważyć znaczący spadek – tak oceniło to odpowiednio 65% i 86% badanych. Dla prawie jednej czwartej badanych na jednakowym poziomie utrzymały się



Źródło: Opracowanie własne.

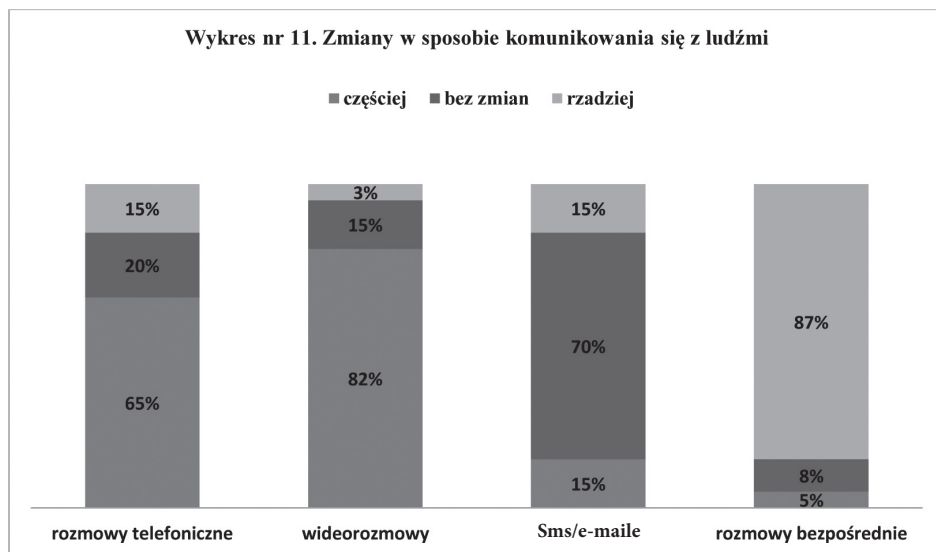
kontakty z rodziną w starszym wieku, sąsiadami i partnerem, a dla 14% i 10% respondentów z przyjaciółmi i kolegami z pracy.

Wniosek: wyniki badań potwierdzają wcześniej zaobserwowaną tendencję, że w czasie pandemii przede wszystkim utrzymywano kontakt z osobami będącymi we wspólnym gospodarstwie domowym oraz rodziną w starszym wieku, troszcząc się wzajemnie o siebie, a następnie z sąsiadami, co jest pozytywnym aspektem pandemii. Być może przyczyniły się do tego również internetowe kampanie społeczne zachęcające do troski o sąsiadów, typu ZakupyDlaSasiadow.pl.

Zmiany w sposobie komunikowania się z ludźmi w czasie pandemii były przedmiotem kolejnego pytania w prezentowanym badaniu. Uzyskane odpowiedzi prezentuje wykres nr 11.

Wobec sytuacji ograniczenia kontaktów bezpośrednich 87% respondentów potwierdziło, że rzadziej prowadzili rozmowy w taki sposób, natomiast częściej korzystali z wideorozmów (82% wskazań) oraz telefonu (65% wskazań). Dla 70% badanych wysyłanie SMS-ów i e-maili pozostało na tym samym poziomie.

Wniosek: Wobec ograniczenia kontaktów bezpośrednich osoby uczestniczące w badaniu zdecydowanie częściej korzystały z rozmów za pośrednictwem telefonii komórkowej oraz wideorozmów, co jest charakterystyczne dla społeczeństwa informacyjnego, a nawyki te zostały tylko utrwalone w okresie pandemii.



Źródło: Opracowanie własne.

Podsumowanie

Dokonując podsumowania przeprowadzonych badań, można sprecyzować następujące wnioski końcowe:

1. Większość ludzi w czasie trwania pandemii została zmuszona do wprowadzenia zmian w swoim dotychczasowym trybie życia przez przejście na zdalną naukę, pracę online z domu, zaprzestanie lub ograniczenie spotkań z bliskimi osobami. Wszystko to w pośredni lub bezpośredni sposób wpłynęło na społeczeństwo, a szczególnie na jego młodych przedstawicieli.
2. Korzyści płynące ze zdalnej pracy i nauki wynikały przede wszystkim z oszczędności czasu oraz miejsca ich wykonywania. Zdecydowanie negatywnie zostały natomiast ocenione możliwości kontaktów zawodowych oraz zarządzania czasem.
3. Zdecydowana większość badanych nie była zwolennikiem pracy i nauki zdalnej, stąd też po ustaniu zagrożenia chciałaby powrotu do ich wykonywania w warunkach rzeczywistych. Są jednak też zwolennicy dalszego nauczania i pracy wykonywanej online, co prawdopodobnie zostanie uwzględnione w wielu środowiskach zawodowych i uczelnianych.

4. Nie można jednoznacznie stwierdzić, iż narodowa kwarantanna miała negatywne skutki na społeczeństwo w każdym aspekcie ich życia. Z przeprowadzonej ankiety wynika, że respondenci zwiększyli swój czas na surfowanie w internecie i oglądanie telewizji, jednak dzięki pozostaniu w domu zacieśnili również więzi rodzinne i sąsiedzkie.
5. Zdecydowanie negatywnie należy ocenić ilość konfliktów domowych, będących w pewnym stopniu konsekwencją pracy zdalnej i pozostawania w domach z rodziną zazwyczaj dłużej niż normalnie. Za kolejny negatywny rezultat lockdownu można uznać zmniejszenie się aktywności fizycznej respondentów oraz sposobów spędzania czasu wolnego, najczęściej w domach, co doprowadziło do rozleniwienia i osłabienia zaangażowania w pracę i naukę.
6. Pandemia wpłynęła również negatywnie na kontakty międzyludzkie, zwłaszcza z przyjaciółmi i znajomymi, z którymi relacje utrzymywane były głównie za pomocą wideorozmów i telefonu. Można zauważyć, że jednak łatwiej dbać o dobre relacje w kontaktach bezpośrednich, spotykając się w przestrzeni rzeczywistej, a nie wirtualnej.
7. Wybuch pandemii spowodował pojawienie się wielu negatywnych emocji i obaw, głównie dotyczących zdrowia fizycznego i psychicznego. Wśród badanych pojawiło się poczucie bezczynności, osamotnienia, występowała apatia i sfrustrowanie. Odczuwanie takich emocji przez dłuższy czas może doprowadzić do depresji, na skutek której jednostka odcina się od reszty społeczeństwa.
8. Pozytywnym aspektem izolacji jest fakt, że respondenci częściej okazywali troskę o zdrowie bliskich, zwłaszcza będących w starszym wieku oraz sąsiadów. Może to świadczyć o tym, że na skutek globalnego zagrożenia ludzie potrafią wyzbyć się egoistycznego toku myślenia i zadbać również o inne osoby.

Bibliografia

- Brainerd, E., Siegler, M. 2003. The Economic Effects of the 1918 Influenza Epidemic, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=394606 (dostęp: 20.10.2020).

- <https://covid19psychologiacom.files.wordpress.com/2020/04/koronawirus-raport-2-jak-polacy-stosujacca8-siecca8-do-zalecenc81-w-zwiacca8kuz-ko....pdf> (dostęp: 25.05.2020).
- Pankowski K., *Rok 2020 pod znakiem pandemii*, Centrum Badania Opinii Społecznej, komunikat z badań, nr 15/2021, ISSN 2353-5822, Warszawa 2021.
- Scovil J., *Samopoczucie Polaków w roku 2020*, Centrum Badania Opinii Społecznej, komunikat z badań, nr 1/2021, ISSN 2353-5822, Warszawa 2021.
- Skrabacz A., *Bezpieczeństwo społeczne. Postawy teoretyczne i praktyczne*, Warszawa 2012.
- Skrabacz A., *Wpływ pandemii koronawirusa na wybrane aspekty bezpieczeństwa społeczno-ekonomicznego Polaków*, „Bezpieczeństwo. Teoria i Praktyka”, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2021, artykuł w druku.
- Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz. U. z 2020, poz. 374, 567, 568, 695 i 875.

Selected aspects of psychosocial behavior of young Poles in the era of the coronavirus pandemic

Abstract: Due to the new and massive phenomenon of the coronavirus pandemic and the crisis caused by it in many areas of the functioning of the state and society, the article presents the results of empirical research conducted on a group of respondents who are students of one of Warsaw's universities. The aim of the research was to diagnose and assess the impact of the pandemic on selected areas of life of this social group, with particular emphasis on work and study, relationships with people and ways of spending free time in the period of social isolation. The research results allow to present conclusions and generalizations that may be useful for conducting comparative research in other social environments.

Key words: pandemic, students, social isolation, interpersonal relations

dr hab. inż. Tadeusz A. Grzeszczyk

Politechnika Warszawska, Wydział Zarządzania

e-mail: tadeusz.grzeszczyk@pw.edu.pl

ORCID: 0000-0002-4898-1931

dr inż. Jacek Pelszyński

Narodowy Fundusz Zdrowia

e-mail: jacek.pelszynski@nfz.gov.pl

ORCID: 0000-0002-1011-2474

Rozdział 9

Ocena efektów społecznych projektów rozwojowych podlegających cyfrowej transformacji w warunkach pandemii COVID-19

Streszczenie: Od wiosny 2020 r. na całym świecie można było zaobserwować masową rezygnację z kontaktów osobistych na rzecz wymiany informacji drogą cyfrową. Wzrasta znaczenie oceny efektów społecznych projektów rozwojowych, które podlegają transformacji cyfrowej. Zwiększa się także zapotrzebowanie ze strony praktyków na systemy i metody wspomagające zarządzanie projektami rozwojowymi finansowanymi w czasie pandemii z budżetów instytucji publicznych, funduszy UE i innych. Poddawane ocenie projekty rozwojowe powinny umożliwiać osiągnięcie istotnych korzyści przyczyniających się do ograniczania negatywnych skutków społeczno-gospodarczych na poziomach lokalnym i regionalnym, spowodowanych pandemią COVID-19. Prawidłowe przeprowadzanie procesu oceny powinno pozwolić na ograniczanie ryzyka projektów z uwzględnieniem nie tylko nakładów i efektów finansowo-ekonomicznych, technicznych, ale także innych aspektów, do których można zaliczyć efekty społeczne. Podjęta w artykule problematyka oceny projektów rozwojowych ma związek z potrzebą naukowej oceny efektów społecznych projektów realizowanych przez instytucje publiczne i prywatne. W artykule odniesiono się do aspektów praktycznych i teoretycznych zarządzania projektami rozwojowymi, które wiążą się ze znacznymi efektami społecznymi. Podjęto próbę oceny efektów transformacji cyfrowej

projektu ogólnopolskiej infolinii, przyczyniającej się do ograniczania negatywnych skutków pandemii COVID-19 w społeczeństwie. W badaniach wykorzystano metodę studium przypadku, analizę wielokryterialną, badania literaturowe, wywiady bezpośrednie i obserwacje uczestniczące. Część opisową uzupełniono rysunkami, schematami oraz tabelami o znacznych walorach aplikacyjnych.

Słowa kluczowe: ocena efektów społecznych, zarządzanie projektami rozwojowymi, transformacja cyfrowa, pandemia SARS-CoV-2

Wprowadzenie

Zwrócenie uwagi na potrzebę oceny transformacji cyfrowej systemów teleinformatycznych wykorzystywanych do obsługi klienta w instytucjach medycznych zostało spowodowane zmianami zachodzącymi w ostatnim czasie. Wykorzystywana w takich rozwiązaniach integracja technologii teleinformatycznych, zastosowanie chmury obliczeniowej oraz wykorzystanie efektu synergii pozwalają na ich lepsze dostosowanie do potrzeb klientów. Ocena zmian technologicznych musi być jednak wsparta również oceną możliwych do osiągnięcia i uzyskiwanych efektów społecznych. Dzięki transformacji organizacyjnej oraz technicznej możliwe jest otrzymanie wzrostu uzyskiwanych efektów społecznych. Przedstawiona analiza dotyczy działów medycznych i z tego względu wymagana jest odpowiednio zrealizowana integracja systemów instytucji publicznych z zasobami firm zewnętrznych.

Zagadnienie przedstawione w tytule rozdziału ma swoje odzwierciedlenie w praktyce oraz opracowaniach naukowych, w których problem wielokryterialnej oceny efektów projektów teleinformatycznych jest analizowany z uwzględnieniem kryteriów technicznych, ekonomicznych lub innych. Oprócz wymienionych kryteriów często konieczna jest również ocena efektów społecznych stanowiących główny cel ich realizacji. Ocena taka zazwyczaj wiąże się z wyceną kosztów i korzyści społecznych przeprowadzaną z wykorzystaniem odpowiedniej metody, np. społecznego zwrotu z inwestycji SROI (*Social Return on Investment*). Metoda SROI wymaga ilościowego ujmowania efektów społecznych projektów rozwojowych w postaci zmonetyzowanej, jej wykorzystywanie często jedynie uzasadnia podejmowane decyzje dotyczące dużych projektów

i nie zawsze stanowi realne wsparcie w uzyskiwaniu rzetelnych wyników oceny projektów rozwojowych¹.

Wyniki przeprowadzonej w artykule analizy dotyczą ważnego i aktualnego problemu oceny efektów społecznych projektów teleinformatycznych w instytucjach medycznych, dzięki którym powinien zostać osiągnięty szybszy powrót na ścieżkę rozwoju gospodarczego oraz społecznego. Wykorzystana do oceny metoda (bazująca na łącznym zastosowaniu zmodyfikowanej analizy punktów funkcyjnych, analizy wielokryterialnej oraz podejścia systemowego²) pozwala na uniknięcie potrzeby wartościowania uzyskanych efektów społecznych w formie zmonetyzowanej dzięki wykorzystywaniu punktów społecznych.

Charakterystyka analizowanego projektu teleinformatycznego

Zarządzanie w odpowiedzialny sposób programami teleinformatycznymi związane jest z dążeniem do uzyskania znaczących efektów łączących się z realizacją różnych, powiązanych ze sobą projektów. W programach takich dużą wagę przywiązuje się zazwyczaj do prognozowania efektów społecznych związanych z ich wdrożeniem. Analiza prowadzonych działań może ułatwić organizacji osiągnięcie założonych efektów, jak również pomóc określić wymagane nakłady i czas niezbędny na ich osiągnięcie. W przypadku dużych programów zazwyczaj złożone są one z szeregu projektów i procesów. Ważniejsze pojęcia stosowane w niniejszej publikacji zdefiniowano jako:

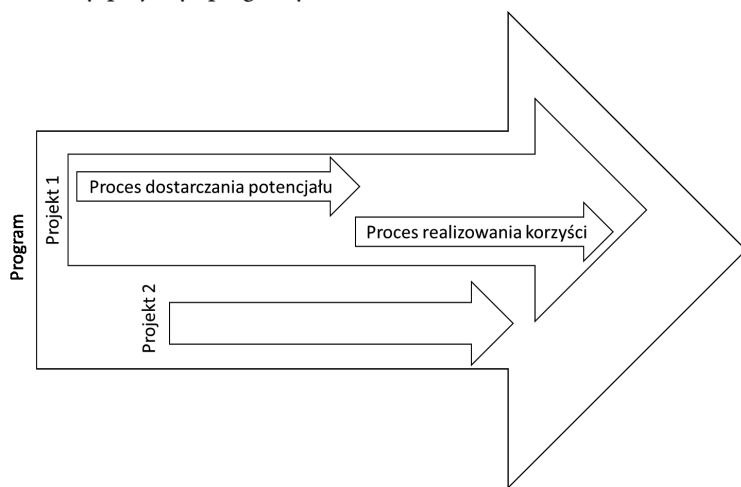
- program, w skład którego wchodzi poszczególne projekty; jego istotną cechą jest uwzględnienie w nim synergii zachodzącej między poszczególnymi projektami;
- projekt, który stanowi odrębny zbiór unikalnych i złożonych działań organizacji i może być realizowany w ramach programu;
- proces, który może stanowić jeden z istotnych elementów projektu i ma jednoznacznie zidentyfikowany cel.

Relacje zachodzące między procesami, projektami i programami przedstawiono na rysunku 1.

¹ A. Surdej, M. Kędzierski, *Metoda analizy kosztów i korzyści w polityce publicznej*, w: A. Surdej (red.), *Ewaluacja w polityce publicznej*, Difin, Warszawa 2013, s. 150.

² T.A. Grzeszczyk, J. Pełszyński, *Ocena efektywności społecznej projektów rozwojowych*, CeDe-Wu, Warszawa 2021.

Rysunek 1. Procesy, projekty i programy



Źródło: Opracowanie własne.

Proces dostarczania potencjału obejmujący zabezpieczenie zasobów materialnych i wprowadzenie zmian organizacyjnych wymaganych przy realizacji projektu stanowi podstawę do osiągnięcia określonych korzyści. W przypadku analizowanego w artykule programu dostarczenie potencjału można było obserwować we wdrożeniach pilotażowych, które miały istotne znaczenie dla rozwoju dalszych etapów transformacji. Kolejne etapy transformacji cyfrowych były zdeterminowane wzrostem liczby zachorowań na COVID-19 wiosną 2020 r. Istniejąca sytuacja wpływała na dynamiczny wzrost zapotrzebowania na usługi teleinformatyczne ze strony instytucji medycznych oraz powodowała potrzebę szybkich transformacji cyfrowych istniejących rozwiązań z uwzględnieniem oceny uzyskiwanych efektów społecznych.

Projekty realizowane w ramach analizowanego programu charakteryzowały się krótkimi wdrożeniami pilotażowymi oraz podziałem wprowadzanych zmian na etapy, realizowane w kolejnych miesiącach. Rozwiązanie takie przyjęto ze względu na ograniczoną dostępność zasobów materialnych, ludzkich oraz niewielkiej ówczesnej wiedzy na temat COVID-19. W początkowym etapie działania były przede wszystkim skoncentrowane na grupach najbardziej zagrożonych zachorowaniem oraz podatnych na szczególnie ciężki przebieg choroby, czyli np. personel medyczny, osoby starsze. W kolejnych etapach transformacja była realizowana pod kątem zwiększenia dostępności dla kolejnych grup społecznych i wiekowych. Określono również wtedy, że osoby młodsze w większym

stopniu korzystają z rozwiązań wspieranych technologią przy jednoczesnym ograniczaniu potrzeby przeprowadzania rozmów z konsultantami.

W oparciu o zidentyfikowanie określonych potrzeb poszczególne rozwiązania teleinformatyczne były wdrażane na podstawie uprawnień wynikających z ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów. Do koordynowania Narodowego Programu Szczepień (NPSz) wyznaczono Kancelarię Prezesa Rady Ministrów (KPRM). W programie tym uczestniczy Ministerstwo Zdrowia (MZ) oraz Narodowy Fundusz Zdrowia (NFZ). W ramach prowadzonych działań poszczególne organizacje w głównej mierze prowadzą:

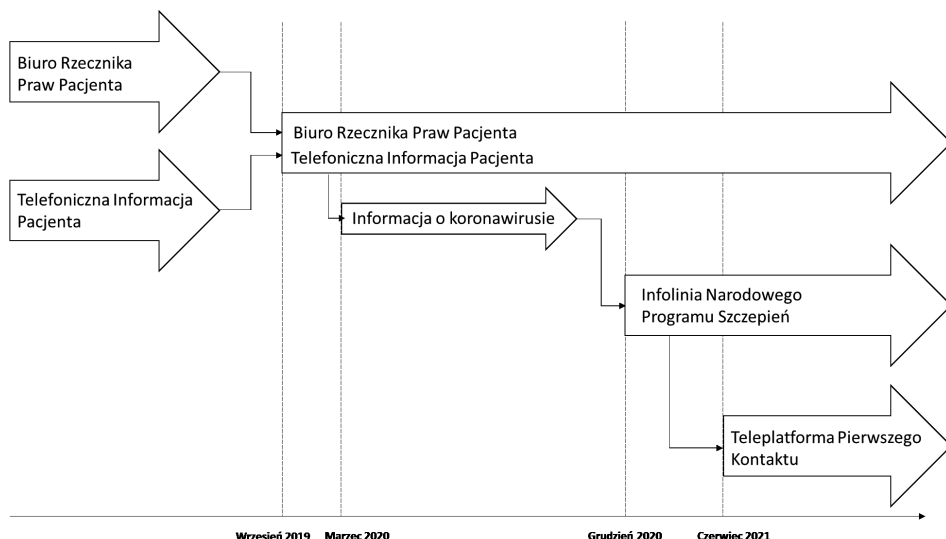
- KPRM – dostosowanie koncepcji do polityki ustalonej w ramach Narodowego Programu Szczepień zasad i kierunków działania MZ i NFZ;
- MZ – koordynowanie projektów i procesów w ramach Narodowego Programu Szczepień wykorzystujących usługi teleinformatyczne;
- NFZ – zapewnienie obsługi infolinii przeznaczonych do realizacji zadań dla Narodowego Programu Szczepień.

Ze względu na złożoność wdrażanych projektów w pracach z nimi związanych oprócz wymienionych powyżej organizacji uczestniczyły także inne instytucje oraz przedsiębiorstwa wspierające realizację poszczególnych projektów i procesów. Przy współpracy wszystkich organizacji kluczowe znaczenie ma dążenie do maksymalizacji efektu synergii oraz uzyskanych efektów społecznych.

W przypadku korzystania z efektu synergii zakłada się, że wydajność dwóch lub więcej połączonych elementów składowych (np. procesów, projektów) będzie większa od sumy wydajności poszczególnych elementów występujących i analizowanych oddzielnie. Synergia jest często wykorzystywana w kontekście łączenia pojedynczych projektów i procesów w celu osiągnięcia nowych wartości dzięki ich połączeniu. Jednakże aby synergia miała realny wpływ na organizację, powinna wiązać się z generowaniem np. większych efektów społecznych, oczekiwanych stóp wzrostu i dłuższego okresu wzrostu. Synergia oprócz umożliwiania uzyskiwania większych efektów społecznych może również wpływać na osiąganie mniejszych kosztów. Z tego powodu potrzeba uzyskania efektu synergii jest istotnym powodem tworzenia zespołów, dzięki czemu można uzyskać poprawę istotnych parametrów, która jest efektem połączenia pracy, wiedzy, umiejętności oraz doświadczenia wielu osób³.

³ P. Corning, *The Synergism Hypothesis: On the Concept of Synergy and its Role in the Evolution of Complex Systems*, „Journal of Social and Evolutionary Systems” 2000, nr 21(2).

Rysunek 2. Etapy transformacji cyfrowej projektu teleinformatycznego



Źródło: Opracowanie własne.

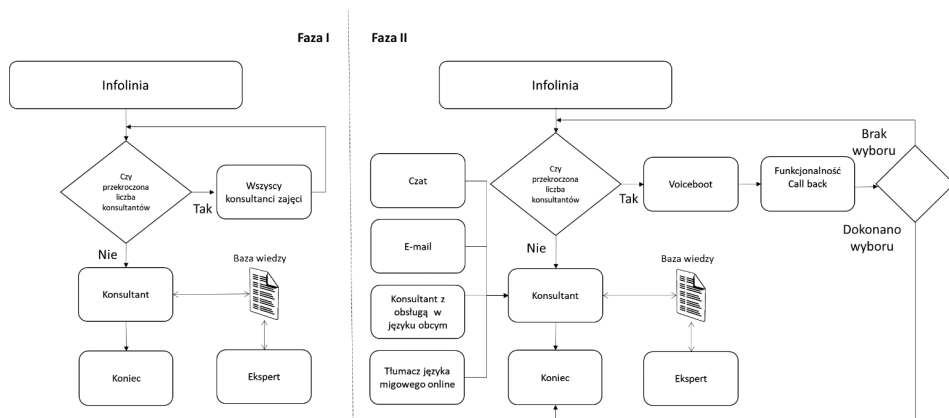
Wdrożenie Narodowego Programu Szczepień jest przykładem etapowego wdrażania transformacji cyfrowej. Zmiany funkcjonującego projektu przeznaczanego do realizacji zadań przed pandemią zostały zdeterminowane potrzebami społecznymi, spowodowanymi wzrostem liczby zachorowań i zgonów. Projekt infolinii podlegającej transformacji cyfrowej został wdrożony we wrześniu 2019 r. Było to poprzedzone implementacjami pilotażowymi opartymi na hybrydowym rozwiązaniu wykorzystującym telekomunikacyjne systemy cyfrowe i analogowe oraz rozproszone zasoby ludzkie i informatyczne. Pierwszym etapem zmian organizacyjnych i technicznych była integracja w ramach jednej infolinii usług świadczonych przez Biuro Rzecznika Praw Pacjenta oraz Narodowy Fundusz Zdrowia. Ze względu na pierwszą falę wzrostu zakażeń i dynamiczny wzrost liczby połączeń kierowanych na infolinię w marcu 2020 r. wyodrębniano poświęconą zakażeniom COVID-19 funkcjonalność infolinii. W grudniu 2020 r. ze względu na dostępność szczepionek i rozpoczęcie rejestracji na szczepienie z istniejącej infolinii wyodrębniono nową infolinię wchodzącą w skład Narodowego Programu Szczepień. Kolejny etap to uruchomienie Teleplatformy Pierwszego Kontakt obsługiwanej przez personel z uprawnieniami medycznymi.

Działania związane z transformacją cyfrową analizowanych projektów teleinformatycznych odnoszą się do projektów o specyficznych cechach, tzn.:

- wykorzystują unikatowe rozwiązania teleinformatyczne (często prototypowe);
- zespół projektowy wdraża opracowane rozwiązanie;
- organizacja prowadzi w tym samym czasie wiele projektów teleinformatycznych;
- zarządzanie projektem obejmuje wdrożenie oraz wsparcie użytkowników;
- projekty realizowane są pod presją czasu;
- część projektów teleinformatycznych w trakcie realizacji wymaga wprowadzania zmian w zakresie funkcjonalności, harmonogramu, budżetu.

Powyższe cechy wpływają na to, że zarządzanie takimi projektami wymaga utrzymania ścisłych relacji zespołu projektowego z otoczeniem. Jednocześnie zespół ten dąży do rozwoju oraz utrzymania stanu funkcjonalnej równowagi w dłuższej perspektywie czasowej. Warunek ten może zostać spełniony wówczas, gdy efektywne zarządzanie projektami wspierane jest przez działania ukierunkowane na przeciwdziałanie nieustannie pojawiającym się zakłóceniom równowagi z uwzględnieniem oddziaływań wewnętrznych oraz zewnętrznych⁴.

Rysunek 3. Transformacja cyfrowa projektu teleinformatycznego z podziałem na fazy



Źródło: Opracowanie własne.

⁴ A.K. Koźmiński, K. Obłój, *Zarys teorii równowagi organizacyjnej*, PWE, Warszawa 1989, s. 23.

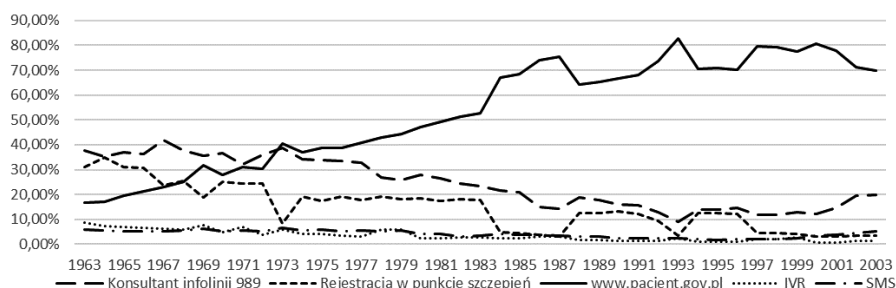
Na rysunku nr 3 przedstawiono transformację cyfrową analizowanego projektu teleinformatycznego z podziałem na fazy. W fazie pierwszej głównymi kanałami komunikacji były połączenie telefoniczne i wsparcie pracy konsultanta bazą wiedzy. W fazie drugiej dodano szereg funkcjonalności, tj.: komunikator czat, komunikację e-mail, obsługę w językach angielskim rosyjskim, ukraińskim, videokonferencje z udziałem tłumacza języka migowego, program voicebota i funkcjonalność *call back* w przypadku przeciążenia infolinii.

Ważnym elementem realizowanych działań na kolejnych etapach transformacji było włączenie projektu infolinii do Narodowego Programu Szczepień obejmującego rejestrację na szczepienia. W programie tym wykorzystywane są zasoby ludzkie wspierane rozwiązaniami technologicznymi oraz automatyczne rozwiązania teleinformatyczne.

Do wykorzystywanych w programie rozwiązań można zaliczyć:

- infolinię obsługiwaną przez konsultantów;
- rejestrację w punktach szczepień (6485 punktów szczepień)⁵;
- rejestrację za pośrednictwem aplikacji internetowej;
- rejestrację za pośrednictwem automatycznego procesu komunikatów głosowych IVR (*Interactive Voice Response*);
- rejestrację za pośrednictwem automatycznego procesu komunikatów tekstowych SMS (*Short Message Service*).

Rysunek 4. Wykres procentowego udziału rejestracji z wykorzystaniem poszczególnych kanałów



Źródło: Opracowanie własne.

⁵ Szczepienie przeciwko COVID-19. Mapa punktów szczepień, www.gov.pl/web/szczepimysie/mapa-punktow-szczepien#/ (dostęp: 23.04.2021).

Przeprowadzona analiza wykazała, że wyszczególnione metody wykorzystywane są z różną intensywnością przez poszczególne grupy wiekowe uprawnione do rejestracji na szczepienie. Zbadanie liczby rejestracji z podziałem na wykorzystanie poszczególnych metod osób urodzonych w latach 1963–2003 pozwoliło na porównanie efektów i wyciągnięcie wniosków wskazujących na to, że:

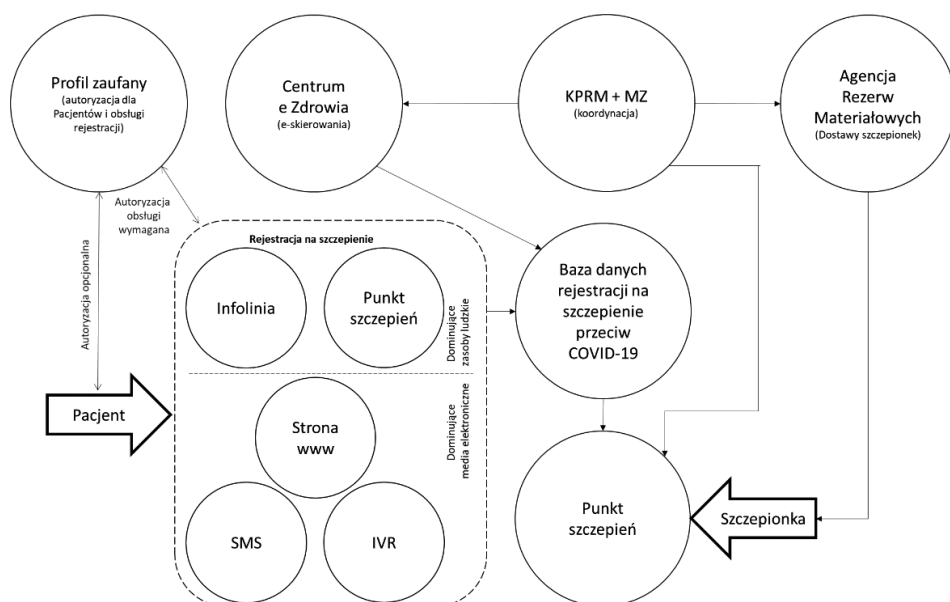
- media elektroniczne są dominującym kanałem rejestracji dla osób urodzonych w 1973 r. i później;
- kanał rejestracji przez IVR i SMS jest na ustabilizowanym poziomie i stanowi funkcjonalność uzupełniającą;
- sumaryczna liczba rejestracji za pośrednictwem punktów szczepień i konsultantów spada;
- istotne znaczenie w projekcie ma kanał informacyjny infolinii⁶.

W przeprowadzonej analizie wielokryterialnej, w celu ujednolicenia struktury danych, wartości liczbowe zostały przekształcone w wartości przedstawione w procentach. Wyniki procentowego udziału rejestracji dla poszczególnych grup wiekowych z wykorzystaniem poszczególnych kanałów przedstawiono na rysunku nr 4.

Wykorzystywane do rejestracji na szczepienie metody można podzielić na dwie grupy. W pierwszej dominującą rolę odgrywają zasoby ludzkie, w tym konsultanci infolinii oraz pracownicy punktów szczepień. W tych sposobach rejestracji praca ludzka jest wspierana przez systemy informatyczne. Druga grupa to metody oparte na rozwiązaniach teleinformatycznych, w przypadku których główna aktywność jest po stronie pacjenta. Kluczowe znaczenie w tej metodzie mają media elektroniczne i zespoły informatyków zapewniające dostępność usługi. Powiązanie poszczególnych projektów i funkcjonalności w rejestracji na szczepienie w ramach Narodowego Programu Szczepień przedstawia rysunek nr 5. Wskazana na rysunku Agencja Rezerw Materiałowych od 23 lutego 2021 r. została przekształcona w Rządową Agencję Rezerw Strategicznych.

⁶ W obsłudze infolinii 989 w kwietniu 2020 r. występowały trzy funkcjonalności: usługowa – rejestracja na szczepienie, zmiana terminu lub miejsca szczepienia, informacyjna – informacje zwiane z koronawirusem.

Rysunek 5. Schemat rejestracji na szczepienia



Źródło: Opracowanie własne.

Łącząc procentowy udział poszczególnych metod rejestracji w Narodowym Programie Szczepień w grupy (z dominującą rolą zasobów ludzkich i mediów elektronicznych), możliwe jest przeanalizowanie zachodzących w tym czasie zmian, których wyniki zamieszczono w tabeli 1.

Tabela 1. Procentowy udział rejestracji z wykorzystaniem poszczególnych zasobów

Lp.	Rok urodzenia	Zasoby ludzkie	Media elektroniczne
1	1963	68,72%	31,28%
2	1964	70,19%	29,81%
3	1965	68,32%	31,68%
4	1966	66,93%	33,07%
5	1967	65,48%	34,52%
6	1968	63,13%	36,87%
7	1969	54,34%	45,66%
8	1970	61,98%	38,05%

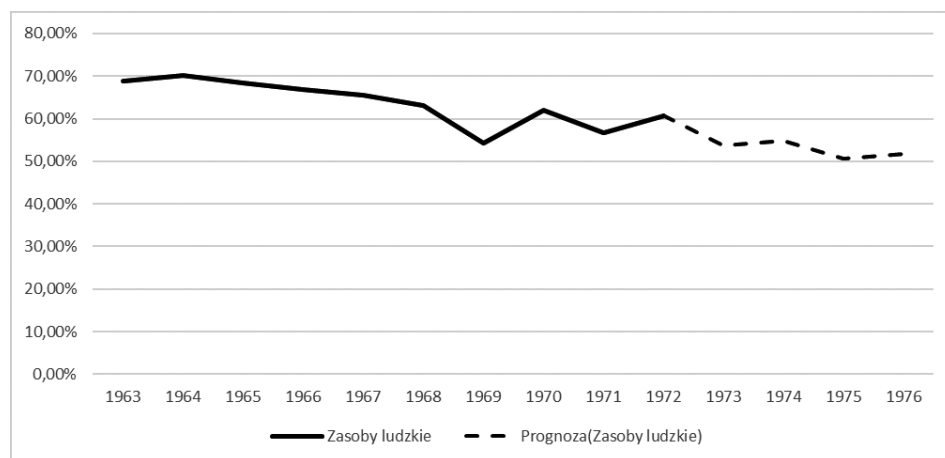
Ocena efektów społecznych projektów rozwojowych podlegających cyfrowej...

9	1971	56,58%	43,42%
10	1972	60,66%	39,34%
11	1973	47,03%	52,97%
12	1974	53,26%	46,74%
13	1975	51,18%	48,82%
14	1976	52,47%	47,53%
15	1977	50,59%	49,41%
16	1978	45,93%	54,07%
17	1979	43,85%	56,15%
18	1980	46,19%	53,81%
19	1981	44,12%	55,88%
20	1982	42,54%	57,46%
21	1983	41,02%	58,98%
22	1984	26,44%	73,56%
23	1985	25,33%	74,67%
24	1986	18,99%	81,01%
25	1987	17,65%	82,35%
26	1988	31,26%	68,74%
27	1989	30,27%	69,73%
28	1990	29,36%	70,64%
29	1991	27,86%	72,14%
30	1992	22,44%	77,56%
31	1993	12,41%	87,59%
32	1994	26,50%	73,50%
33	1995	26,48%	73,52%
34	1996	26,70%	73,30%
35	1997	16,32%	83,68%
36	1998	16,53%	83,47%
37	1999	17,24%	82,76%
38	2000	15,19%	84,81%
39	2001	17,81%	82,19%
40	2002	23,20%	76,80%
41	2003	23,55%	76,45%

Źródło: Opracowanie własne.

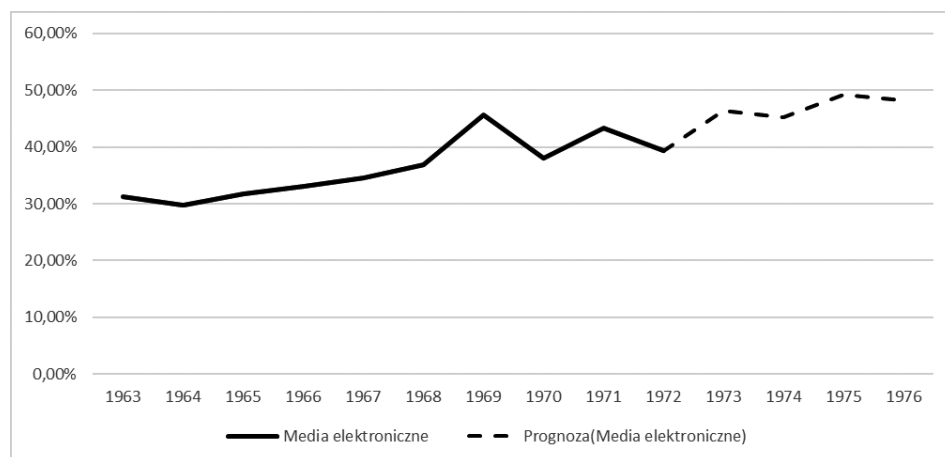
Zebrane dane pozwalają na opracowanie prognozy wskazującej na trendy mogące wystąpić w kolejnych okresach. Prognoza taka umożliwi przygotowanie odpowiednich zasobów technicznych i ludzkich. Na rysunkach nr 6 i 7 przedstawiano prognozy dla grupy usług z dominującą rolą zasobów ludzkich oraz mediów elektronicznych.

Rysunek 6. Prognoza procentowego udziału rejestracji z wykorzystaniem zasobów ludzkich



Źródło: Opracowanie własne.

Rysunek 7. Prognoza procentowego udziału rejestracji z wykorzystaniem mediów elektronicznych



Źródło: Opracowanie własne.

Ocena efektów społecznych

Badając efekty społeczne analizowanych projektów oprócz kryteriów ekonomicznych i technicznych ważne jest uzyskanie odpowiedzi na pytanie, który wariant rozwiązania jest odpowiedni oraz pozwala na lepsze wykorzystanie posiadanych zasobów w celu uzyskania większych efektów społecznych. Można jednocześnie założyć, że społeczeństwo, na które wpływa projekt, jako priorytetowe określa kryteria ochrony zdrowia, edukacji, stanu rynku pracy, usługi publiczne, bez względu na wysokość wymaganych na ich realizację nakładów. W związku z tym wykorzystanie w procesach oceny efektów społecznych wybranych kryteriów określanych jako priorytetowe pozwoli na przeprowadzenie prawidłowej transformacji cyfrowej projektu z punktu widzenia potrzeb społecznych. Dla potrzeb przeprowadzenia oceny przyjęto następujące kryteria związane z ochroną zdrowia, dostępnością edukacji, tworzeniem miejsc pracy, przeciwdziałaniem wykluczeniu społecznemu i jakością życia.

Ocenę efektów społecznych przeprowadzono w następujących trzech fazach: identyfikacji kryteriów oceny projektu, szacowania wartości kryteriów i wag, określenia oceny efektów społecznych. W ramach poszczególnych faz oceny wykorzystano dziesięć etapów przeprowadzenia oceny efektów społecznych, tj.⁷:

- 1) określenie celu, rodzaju i przedmiotu oceny;
- 2) gromadzenie danych;
- 3) identyfikacja granic projektu rozwojowego;
- 4) dekompozycja kryteriów społecznych;
- 5) oszacowanie stopnia złożoności aspektów społecznych;
- 6) wyznaczenie wartości kryteriów;
- 7) ustalenie wag dla poszczególnych kryteriów;
- 8) określenie współczynnika korygującego;
- 9) wyznaczenie liczby punktów społecznych;
- 10) ocena efektów społecznych.

Z wykorzystaniem tych etapów oceniono efekty społeczne projektu teleinformatycznego zaliczanego do Narodowego Programu Szczepień.

⁷ T.A. Grzeszczyk, J. Pełszyński, *Ocena...*, dz. cyt.

- 1) Określenie celu, rodzaju i przedmiotu oceny pozwala na rozpoczęcie procesu oceny. Dla usystematyzowania oceny dane zostały zgromadzone w formie tabelarycznej. Wyniki analiz związanych z pierwszym etapem przedstawiono w tabeli 2.

Tabela 2. Określenie celu, rodzaju i przedmiotu oceny

Parametr	Opis
Cel	Przeprowadzenie oceny efektów społecznych projektu
Rodzaj	Ocena bieżąca (<i>ongoing</i>) dokonana w trakcie wdrażania projektu, w dowolnym momencie, w przeciwieństwie do oceny <i>mid-term</i> nie ma tutaj ściśle określonego terminu jej realizacji
Przedmiot oceny	Projekt rozwojowy teleinformatyczny

Źródło: Opracowanie własne.

- 2) Zgromadzenie danych na temat projektu zostało częściowo przeprowadzone we wcześniejszej części. Istotne dla dalszej oceny efektów jest określenie liczby osób, na które on oddziałuje oraz jego wartość. Ze względu na wpływ czynników zewnętrznych na decyzję o przystąpieniu do szczepienia można na obecnym etapie oszacować liczbę osób, które zostaną objęte programem. Główny Urząd Statystyczny wykazał, że w 2019 r. liczba ludności wynosiła 38 mln 386 tys., z czego 81,9% to osoby, które ukończyły 18. rok życia⁸. Należy jednak uwzględnić to, że nie wszystkie osoby poddają się szczepieniu. Koszty związane z projektem nie przekroczyły 10 mln zł, co jest wartością pozwalającą określić w dalszej części jego złożoność.
- 3) Na identyfikację granic projektu rozwojowego miało wpływ to, że jego analiza została przeprowadzona w trakcie jego trwania (*ongoing*), co nie pozwala na odniesienie się do wszystkich efektów społecznych, które w fazie projektowania rozwiązania nie mogły być jednoznacznie ocenione. Jednym z ważniejszych czynników ryzyka jest dostępność szczepionek oraz aktywność ruchów antyszczepionkowych. W przypadku tego projektu istotne znaczenie odgrywa proces edukowania społeczeństwa.

⁸ GUS Mały Rocznik Statystyczny 2020, www.stat.gov.pl (dostęp: 29.04.2021).

Granice projektu wyznacza liczba obywateli zarejestrowanych na szczepienia. Zasady wyznaczania tych granic zobrazowano w tabeli 3.

Tabela 3. Identyfikacja granic projektu rozwojowego energetycznego

Lp.	Kryteria	Identyfikacja
1	Społeczne	Zwiększanie możliwości korzystania ze szczepień oraz efektów ochrony zdrowia obywateli
2	Inne	Ograniczenie liczby zajętych miejsc w szpitalach, poprawa funkcjonowania gospodarki

Źródło: Opracowanie własne.

- 4) Dekompozycję kryteriów społecznych przeprowadzono w związku z koniecznością dokładniejszego zidentyfikowania kryteriów społecznych wymaganych do przeprowadzenia oceny efektów społecznych. Analizie poddano dwa warianty rozwiązań, dla których wyodrębniono pięć grup kryteriów społecznych (tabela 4). Każde z kryteriów oceniono z zastosowaniem sześciostopniowej skali.

Tabela 4. Przykładowe kryteria oceny efektów społecznych projektu rozwojowego

Grupa	Kryterium
Zdrowie	Jaki jest wpływ projektu na ochronę zdrowia?
	Zapewnienie możliwości rejestracji na szczepienie obywateli
	Koordinowanie szczepienia personelu medycznego, nauczycieli i innych grup priorytetowych
	Wsparcie psychologiczne
	Wsparcie obsługi osób na kwarantannie
Edukacja	Jak projekt zwiększa dostępność edukacji?
	Analiza najczęściej poruszanych zagadnień przez pacjentów, przygotowanie materiałów informacyjnych dla samokształcenia
	Publikacja informatorów, materiałów reklamowych, edukacja zdalna
	Szkolenie konsultantów na podstawie przygotowanej bazy wiedzy

Praca	Jak projekt wpływa na tworzenie miejsc pracy?
	Tworzenie nowych miejsc pracy dla konsultantów
	Tworzenie miejsc pracy dla wolontariuszy np. z firm z ograniczonym zakresem działalności
	Wsparcie personelu medycznego
	Wskazywanie przedsiębiorcom możliwych źródeł dofinansowania
Wykluczenie	Jak projekt przeciwdziała wykluczeniu społecznemu?
	Obsługa osób niesłyszących
	Obsługa osób w języku angielskim, rosyjskim, ukraińskim
	Możliwość uzyskania informacji przez osoby z dysfunkcjami ruchowymi
Jakość życia	Jak projekt wpływa na jakość życia?
	Zwiększenie bezpieczeństwa poprzez ograniczenie potrzeby bezpośredniego kontaktu
	Wskazywanie miejsc udzielających lokalnie pomocy osobom chorym
	Wykorzystanie różnych mediów do komunikacji

Źródło: Opracowanie własne.

- 5) Oszacowanie stopnia złożoności aspektów społecznych przeprowadzono w oparciu o liczbę osób objętych oddziaływaniem efektów projektu. Dla tak zdefiniowanych kryteriów projekt teleinformatyczny określono jako złożony (tabela 5).

Tabela 5. Określenie złożoności aspektów społecznych

Wysokość nakładów w mln zł	Liczba osób objętych oddziaływaniem efektów projektów			
	<10	11<50	51<250	>250
<0,1	Prosty	Prosty	Średni	Złożony
0,11<1.0	Prosty	Średni	Złożony	Złożony
1,1<10	Średni	Złożony	Złożony	Złożony
10,1–100	Złożony	Złożony	Złożony	Złożony

Źródło: Opracowanie własne.

- 6) Wyznaczenie wartości kryteriów zrealizowano dla wariantu 1 (przed transformacją) oraz wariantu 2 (po transformacji). Ocenę każdego z kryteriów przeprowadzono z zastosowaniem sześciostopniowej skali (tabela 6). W przypadku braku wpływu na projekt określonego czynnika związanego z danym kryterium przypisana została mu wartość zero, a w sytuacji silnego wpływu innego czynnika, związanemu z nim kryterium przypisano wartość pięć. Stany pośrednie zostały ocenione w skali 1–4.

Tabela 6. Wyznaczenie wartości kryteriów społecznych dla analizy dwóch wariantów projektu teleinformatycznego

Grupa	Kryterium	Wariant 1	Wariant 2
Zdrowie	Jaki jest wpływ projektu na ochronę zdrowia?		
	Zapewnienie możliwości rejestracji na szczepienie obywateli	0	5
	Koordinowanie szczepienia personelu medycznego, nauczycieli	0	5
	Wsparcie psychologiczne	0	5
	Wsparcie obsługi osób na kwarantannie	5	5
	Suma	5	20
Edukacja	Jak projekt zwiększa dostępność edukacji?		
	Analiza najczęściej poruszanych zagadnień przez pacjentów, przygotowanie materiałów informacyjnych	5	5
	Publikacja informatorów, materiałów reklamowych	5	5
	Szkolenie konsultantów na podstawie przygotowanej bazy wiedzy	3	3
	Suma	13	13
Praca	Jak projekt wpływa na tworzenie miejsc pracy?		
	Tworzenie nowych miejsc pracy dla konsultantów	1	4
	Tworzenie miejsc pracy dla wolontariuszy np. z firm z ograniczonym zakresem działalności	0	4
	Wsparcie personelu medycznego	0	4
	Wskazywanie przedsiębiorcom możliwych źródeł dofinansowania	3	3
	Suma	4	15

Wykluczenie	Jak projekt przeciwdziała wykluczeniu społecznemu?		
	Obsługa osób niesłyszących	0	5
	Obsługa osób w języku angielskim, rosyjskim, ukraińskim	0	5
	Możliwość uzyskania informacji przez osoby z dysfunkcjami ruchowymi	5	5
	Liczba obsłużonych osób	1	4
	Suma	6	19
Jakość życia	Jak projekt wpływa na jakość życia?		
	Zwiększenie bezpieczeństwa poprzez ograniczenie potrzeby bezpośredniego kontaktu	5	5
	Wskazywanie miejsc udzielających lokalnie pomocy osobom chorym	5	5
	Wykorzystanie różnych mediów do komunikacji	1	5
	Suma	11	15

Źródło: Opracowanie własne.

Na tym etapie analizy największą liczbę punktów (82) uzyskał drugi wariant projektu teleinformatycznego.

7) Nastąpiło przyporządkowanie wag dla poszczególnych kryteriów (tabela 7).

Tabela 7. Wyznaczenie wartości wag dla poszczególnych kryteriów społecznych

Grupa kryteriów Prosty		Poziom złożoności aspektów społecznych projektu rozwojowego		
		Średni	Złożony	Złożony
Kryteria wpływające na ochronę zdrowia	W_1	7	10	15
Kryteria o oddziaływaniu edukacyjnym	W_2	5	7	10
Kryteria wpływające na tworzenie miejsc pracy	W_3	4	5	7
Kryteria wpływające na przeciwdziałanie wykluczeniu społecznemu	W_4	3	4	6
Kryteria wpływające na jakość życia	W_5	3	4	6

Źródło: Opracowanie własne.

Efekt zsumowania poddanych analizie kryteriów zdefiniowany został jako wstępna liczba punktów społecznych. Wynik ten możemy przedstawić za pomocą wzoru:

$$WLPS_j = W_1 \sum_i A_{ij} + W_2 \sum_i B_{ij} + W_3 \sum_i C_{ij} + W_4 \sum_i D_{ij} + W_5 \sum_i E_{ij},$$

gdzie:

$WLPS_j$ – wstępna liczba punktów społecznych,

$A_{ij}, B_{ij}, C_{ij}, D_{ij}, E_{ij}$ – wartości poszczególnych kryteriów społecznych dla j-tego wariantu, wybranej grupy (A, B, C, D lub E) oraz i-tej kolejności w określonej grupie,

W_k – wagi dla k -tej grupy kryteriów społecznych (A, B, C, D lub E).

W powyższych wzorach wyodrębniono trzy indeksy (i, j, k), tj.:

- indeks i określa miejsce danego kryterium oceny w grupie kryteriów (A, B, C, D lub E);
- indeks j determinuje numer jeden z dwóch wariantów ocenianego projektu;
- indeks k wiąże się z numerem konkretnej grupy kryteriów ($k \in \{1, 2, 3, 4, 5\}$).

Tabela 8. Wyznaczanie wstępnych liczb punktów społecznych dla poszczególnych wariantów projektu

Grupy kryteriów	Warianty projektu	
	Projekt 1	Projekt 2
Kryteria wpływające na ochronę zdrowia	5 * 15	20 * 15
Kryteria o oddziaływaniu edukacyjnym	13 * 10	13 * 10
Kryteria wpływające na tworzenie miejsc pracy	4 * 7	15 * 7
Kryteria wpływające na przeciwdziałanie wykluczeniu społecznemu	6 * 6	19 * 6
Kryteria wpływające na jakość życia	11 * 6	15 * 6
Suma	335	739

Źródło: Opracowanie własne.

Sumaryczne wartości wprowadzono do ostatniego wiersza tabeli 8.

8) W przypadku określenia współczynnika korygującego (tabela 9) zastosowano sześciostopniową skalę – podobnie jak we wcześniejszej części analizy.

Wartość współczynnika korygującego można wyznaczyć z następującego wzoru:

$$WK = \sum_{i=1}^{11} P_i$$

gdzie: WK – współczynnik korygujący, P_i – wartości parametrów uzupełniających.

Tabela 9. Określenie współczynnika korygującego

Lp.	Parametry uzupełniające	Wariant 1	Wariant 2
1	Działania antykorupcyjne	Czy w procesie przygotowania oraz eksploatacji projektu uwzględniono standardy antykorupcyjne?	
		5 – tak	5 – tak
2	Protesty społeczne/ konflikty	Osoby uczestniczące w protestach społecznych? (antyszczepionkowcy, negacja pandemii)	
		3 – istnieją grupy przeciwnie	3 – istnieją grupy przeciwnie
3	Koszty uczestnictwa w projekcie	Czy wymagane są opłaty za korzystanie z projektu?	
		5 – brak opłat	5 – brak opłat
4	Aplikowanie do udziału w projekcie	Czy istnieją formalne ograniczenia uczestniczenia w projekcie. Złożenie wniosku, dostępny dla każdego?	
		5 – prosta z wieloma formami rejestracja	5 – prosta z wieloma formami rejestracja
5	Dostępność projektu	Jaka jest dostępność korzystania z projektu?	
		2 – średnie ograniczenia	4 – bardzo słabe ograniczenia
6	Aktualizacja korzystania z projektu	Czy wymagane jest aktualizowanie uczestniczenia w projekcie?	
		5 – brak konieczności aktualizacji	5 – brak konieczności aktualizacji
7	Wielokrotne użycie	Czy projekt jest możliwy do wielokrotnego wykorzystania?	
		2 – możliwy do wielokrotnego wykorzystania po znaczącej modyfikacji	3 – możliwy do wielokrotnego wykorzystania po częściowej modyfikacji

8	Wdrożenie	Jaka jest złożoność procesu wdrożenia?	
		3 – średnio skomplikowane wdrożenie	1 – trudne wdrożenie
9	Eksploatacja	Jakie są koszty bieżącej eksploatacji projektu? (połączenia bezpłatne dla osób dzwoniących)	
		0-kosztowna w ponad 100% wartości projektu	0-kosztowna w ponad 100% wartości projektu
10	Wielokulturowość	Czy z projektu mogą korzystać różne grupy społeczne	
		0 – brak wielokulturowości	3 – średnia
11	Adaptacja projektu	Możliwości dostosowania projektu przez użytkownika	
		2 – utrudniona forma dostosowania	3 – średnio skomplikowana forma dostosowania
Suma		32	39

Źródło: Opracowanie własne.

- 9) Wyznaczenie liczby punktów społecznych odzwierciedlających efekty społeczne. Obliczenia prowadzone wcześniej umożliwiają na obecnym etapie wyznaczenie końcowej (ostatecznej) liczby punktów społecznych. Ostateczną liczbę punktów społecznych oblicza się według wzoru:

$$KLPS = WLPS + WK$$

gdzie:

KLPS – końcowa liczba punktów społecznych,

WLPS – wstępna liczba punktów społecznych,

WK – współczynnik korygujący.

Końcowa liczba punktów społecznych stanowi punkt wyjścia do przeprowadzenia oceny efektów społecznych projektu rozwojowego.

Tabela 10. Obliczenie wartości końcowej liczby punktów społecznych dla projektu

Lp.	Ocena	Warianty projektu	
		Wariant 1	Wariant 2
1	Wstępna liczba punktów społecznych	335	739
2	Współczynnik korygujący	32	39
3	Końcowa liczba punktów społecznych	367	778

Źródło: Opracowanie własne.

Uwzględniając obliczone wstępne liczby punktów społecznych oraz wartości współczynnika korygującego, wyznaczono końcowe liczby punktów społecznych dla obu wariantów ocenianego projektu teleinformatycznego (tabela 10).

- 10) Ocena efektów społecznych przeprowadzona dziesięcioetapową metodą pozwala na wskazanie wariantu związanego z większymi efektami społecznymi, przy czym na etapie *ex ante* (przed rozpoczęciem projektu) zazwyczaj analizowana jest większa liczba wariantów. W przypadku wyników oceny przedstawionej w tym artykule jako bardziej odpowiedni wskazano wariant 2 związany z transformacją cyfrową.

Podsumowanie

Zmiany, jakie zaistniały w funkcjonowaniu instytucji medycznych od marca 2020 r., sprawiły, że część działań przeniosła się z kontaktów bezpośrednich do przestrzeni online. Tempo tych zmian powiązane jest z kolejnymi transformacjami cyfrowymi. W wyniku powstawania nowych rozwiązań teleinformatycznych na miarę dzisiejszych wyzwań działania te skupiają się w głównej mierze na wprowadzaniu kolejnych innowacji w usługach medycznych. Wzmacnianie cyfrowej kultury organizacyjnej w modelach działania obejmujących współpracę interdyscyplinarnych zespołów pozwala na dostosowanie się do istniejących trendów i lepsze wykorzystanie posiadanych zasobów dzięki bazowaniu na efekcie synergii.

Na rodzaj prowadzonych działań projektowych i wprowadzanie nowych funkcjonalności mają wpływ również zmiany w zakresie preferencji osób korzystających z cyfrowych usług medycznych. Identyfikowane dla poszczególnych grup społecznych i wiekowych potrzeby są często konsekwencją wpływu transformacji cyfrowych dokonujących się w innych sektorach, np. bankowości. Dzięki możliwości prowadzenia skutecznych wieloaspektowych ocen w zakresie technologicznym i uzyskiwanych efektów społecznych możliwe jest nie tylko zwiększenie produktywności i niezawodności wykorzystywanych rozwiązań, ale także dążenie do maksymalizacji uzyskiwanych efektów społecznych.

Bibliografia

- Corning, P., *The Synergism Hypothesis: On the Concept of Synergy and its Role in the Evolution of Complex Systems*, „Journal of Social and Evolutionary Systems” 2000, nr 21(2).
- Grzeszczyk T.A., Pełszyński J., *Ocena efektywności społecznej projektów rozwojowych*, CeDeWu, Warszawa 2021.
- Koźmiński A.K., Obłój K., *Zarys teorii równowagi organizacyjnej*, PWE, Warszawa 1989.
- Surdej A., Kędzierski M., *Metoda analizy kosztów i korzyści w polityce publicznej*, w: Surdej A. (red.), *Ewaluacja w polityce publicznej*, Difin, Warszawa 2013.
- Szczepienie przeciwko COVID-19. Mapa punktów szczepień, www.gov.pl/web/szczepimysie/mapa-punktow-szczepien#/ (dostęp: 23.04.2021).
- GUS, *Mały Rocznik Statystyczny 2020*, www.stat.gov.pl (dostęp: 29.04.2021).

Assessment of the Social Effects of Development Projects Undergoing Digital Transformation in the Conditions of the COVID-19 Pandemic

Abstract: Since spring 2020, a massive resignation from personal contacts in favour of digital information exchange has been observed worldwide. The assessment of the social effects of development projects that are subject to digital transformation is increasing significantly. There is also an increasing demand from practitioners for systems and methods supporting the management of development projects financed during the pandemic from the budgets of public institutions, EU funds and other funds. The assessed development projects should achieve significant benefits contributing to reducing negative socio-economic impacts at local and regional levels caused by the COVID-19 pandemic. The proper conduct of the assessment process should reduce the risk of projects, taking into account financial, economic and technical outlays and effects, and other aspects, which may include social effects. Evaluating development projects discussed in the article is related to the need for the scientific evaluation of the social effects of projects implemented by public and private institutions. The article refers to the practical and theoretical aspects of managing development projects associated with significant social effects. An attempt

was made to assess the impact of the digital transformation of the nationwide hotline project, contributing to reducing the negative impact of the COVID-19 pandemic on society. The research used the case study method, multi-criteria analysis, literature research, face-to-face interviews, and participant observation. The descriptive part is supplemented with drawings, diagrams, and tables of significant application value.

Key words: social impact assessment, development project management, digital transformation, SARS-CoV-2 pandemic

Mikhail Kulapov*
Sergey Yashin**
Svetlana Zakharova***

Rozdział 10

Life quality change assessment of the population of Russia in the conditions of COVID-19 pandemics

Abstract: The steady increase in the life quality of the population as an indicator of effectiveness of implementation of national ideas and strategic tasks for development of Russian Federation was determined by Order of the President of the Russian Federation¹. The paper gives the model of interaction between subjects of socio-economic relations in contemporary Russia seen as a system that determines the life quality of the population. A role of different subjects of socio-economic relations was determined in increasing the life quality of the population. The changes during COVID-19 pandemics in the population life quality indicators distributed over the subjects of socio-economic relations were assessed based on the sociological studies. The primary anti-crisis state support measures for businesses and citizens aimed to support the country's general economic status and to increase the life quality of the population during COVID-19 pandemics in the years 2020 to 2021 were reviewed.

Key words: life quality of the population, subjects of socio-economic relations, anti-crisis measures, COVID-19 pandemics

* Doctor of Economics, Professor of the Russian University of Economics named after Plekhanov, the city of Moscow, Russia, kmn@mail.ru.

** Doctor of Economics, Professor, Head of the Management and State Administration Chair, National Research State University of Nizhniy Novgorod named after N.I. Lobachevsky, the city of Nizhniy Novgorod, Russia, jashinsn@yandex.ru.

*** PhD IN Economics, Assistant Professor of the Management and State Administration Chair, National Research State University of Nizhniy Novgorod named after N.I. Lobachevsky RF, the city of Nizhniy Novgorod, Russia, svetlana-nngu@mail.ru.

¹ Decree of the President dated May 7, 2018, No. 204 (rev. dated July 19, 2018) "On the national objectives and strategic tasks for development of the Russian Federation for the period of up to the year 2024".

Introduction

The introduction and usage of the contemporary management methods and technologies allow positive dynamics to be achieved in the certain statistical socio-economic indicators that, to some extent, characterize the qualitative changes in the development level of territories. But only the significant change in the life quality of the population may serve as the performance indicator of administrative reforms and be an appraisal of the performance results of authorities.

We understand life quality of the population as a satisfaction degree of the material, culture-spiritual, socio-economical, and medico-ecological needs of a human being who lives in the certain territory. A task of the authorities at both federal and regional levels is to develop and implement population life quality satisfaction degree via adequate growth programs.

The population life quality assessment approaches are of a great variety, and the human potential assessment method that involves four important life indicators is best known internationally. But these indicators do not give a full sense of the life quality of the population. The Russian scientists address a wide range of the issues associated with population life quality assessment. There are discussions to select the factors that characterize different population life aspects, and the economic and mathematical models of their impact on life quality are addressed, but no approved assessment technique has been adopted for this indicator so far. In particular, this is due to the fact that the life quality of the population is a complex integral indicator. This paper addresses the factorial approach to population life quality management as a part of evolving the corporate production factor management system. The population acts as one of the socio-economic relationship parties that own production factors. These factors include labour in a traditional way, which implementation yields an income in the form of wages. But it is the use of other production factors within the corporate management system that allows for high well-being level. However, the paper notes that the well-being level is just one of the four indicator groups, which are distributed over the parties having an impact on the life quality of the population, and their classification is provided. This paper's goal is to conduct the population life quality study for the years 2007 to 2020, and to assess the impact of COVID-19 pandemics on the changes in the population life quality indicators.

The separate study was conducted on those surveyed with incomplete higher education. Based on the sociological survey, the factors that had affected the life quality of the students during COVID-19 pandemics were assessed.

The study results gave an opportunity to assess the measures of State support for the Russian population and businesses in the troubled isolation period of COVID-19 pandemics.

The theoretical and methodological approaches to population life quality study

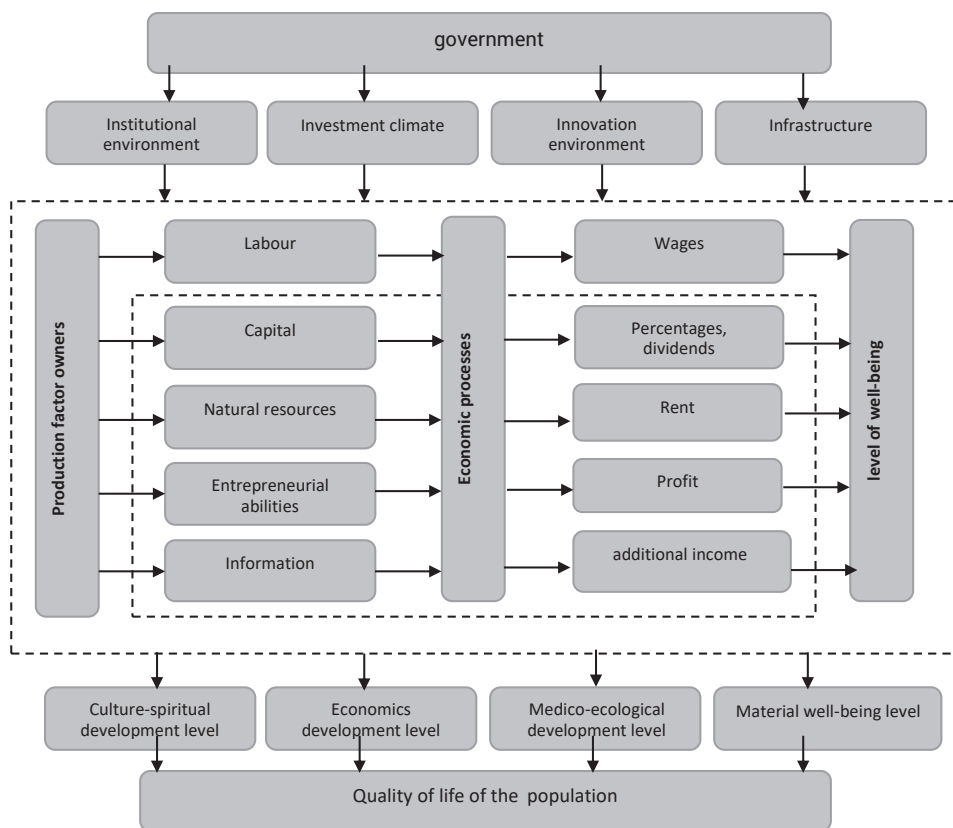
The system of the relationships between the subjects of socio-economic relations that are created in accordance with the accepted corporate management model based on the population life quality management factorial approach plays a special role in forming factors that have an impact on the life quality of the population². Fig. 1 shows the model of the relationships between subjects of socio-economic relations from the standpoint of the population life quality management factorial approach that allows for the visualization of the processes oriented to increasing the satisfaction of citizens with their life quality.

As is seen from the model provided, both the state and the municipality have an indirect impact on the life quality of the population by creating the institutional and investment environments as well as the investment climate and comfortable infrastructure for the development of socio-economic relations. In the middle, the production factor owner interaction system that yields an income is highlighted, from the standpoint of the population life quality management factorial approach. The population being one of the production factor owners participates in the economical processes by earning a definite level of income (well-being level). The economical business processes determine an economic development level, a culture-spiritual development level, a medico-ecological development level, and a material well-being level which are the very components of the life quality of the population. So, the population itself as well as the businesses, municipalities, and state should be designated as the primary subjects of socio-economic relations that have an influence on the life quality of the population. Each of them has its own objectives and tasks, and factors that have

² Zakharova S.G., *Population life quality management factorial approach*, *International Journal of Professional Science*, 2017, No. 1, pp. 33–40.

an influence on the life quality of population depend on their mutually beneficial co-operation and on the arrangement of integration cooperation to a great extent³.

Fig. 1. Model of the relationships between the subjects of socio-economic relations in the contemporary Russia



Source: Developed and compiled by authors.

Fig. 1 shows a list of the factors that have an influence on the life quality of the population, which is broken down by subjects of socio-economic relations.

³ Zakharova S.G., Borisov S.A., Lapshina E.N., Ozina A.M., Chernyshov A.N., *Specifics of Forming the Russian Middle Class According to the Factorial Model of Management Living Standards, Quality-Access to Success (QAS)*, Vol. 22, No. 181, 2021, pp. 110–116, https://www.srac.ro/calitatea/en/arhiva/2021/QAS_Vol.22_No.181_April.2021.pdf.

The factors, in their turn, characterize the indicator list. In total, this population life quality assessment model includes 100 indicators, but the questionnaire of descriptive version is more often used for widespread sociological survey. It should be noted that an indicator value exceeding 5 means that there are positive dynamics in changing an indicator value as compared to the previous year. An indicator value less than 5 scores means that this value is reduced as compared to the previous year: so, a difference between indicators for one year is taken into consideration, which is felt by the respondents as satisfaction with this factor as compared to the previous year.

The author-developed technique that involves recent Orders of the President of Russian Federation oriented to implementation of national objectives and strategic tasks for development of Russia was used for population life quality assessment. The technique includes sociological survey of respondents with higher and incomplete higher education.

An expert appraisal of factors that determine the life quality of population involves ten-scored assessment of these factors from 1 (very bad) through 5 (normal) to 10 (very good). It shall be particularly noted that the study shows no dynamic increase in indicators. The sociological assessment shows that indicators have changed as compared to previous year.

From the presuppositions and definitions given, authors have proposed a structure of indicators broken down by the subjects of socio-economic relations, which is provided in Fig. 2. The population life quality indicators were formed based on:

- An Ordinance of the Government of Russian Federation No. 1662-r dated November 17, 2008, (as amended on September 28, 2018) <On the Concept of Long-Term Socio-Economic Development of Russian Federation for the period of up to 2020> (together with “the Concept of Long-Term Socio-Economic Development of Russian Federation for the period of up to 2020”;
- A Decree of the President of Russian Federation dated May 07, 2018, No. 204 (as amended on July 19, 2018) “On the National Objectives and Strategic Tasks for development of Russian Federation for the period of up to 2024”;
- A National Program of Russian Federation “Academic and technological development of the Russian Federation for the years 2018 to 2025”.

Fig. 2. Classification of factors by the subjects of socio-economic relations that characterize life quality of the population



Source: Developed and compiled by authors.

Population life quality change study results for the years 2007, 2014, and 2019

The population life quality study on the group of the respondents aged 25 to 50 years and having higher and incomplete higher education is conducted annually on the basis of methodologic of National Research State University of Nizhniy Novgorod named after N. I. Lobachevsky. More than 1800 respondents of different ages and social groups in Nizhniy Novgorod Region participate in the questionnaire annually. The sociological life quality evaluation of representative groups in Nizhniy Novgorod Region that is the statistically-average territory of Russia can characterize the change in life quality on a nationwide scale.

For the visual reference and more detailed analysis of sociological evaluation of factors that determine life quality of the population, the radar plots grouped based on four subjects of socio-economic relationship—population, business, municipalities, and state—are used. A comparative analysis of respondents' opinions on the results of 2007, 2014 [2]⁴ and 2019 studies in comparison with average assessment of integral population life quality indicator is very interesting. The population life quality study results are provided in Fig. 3.

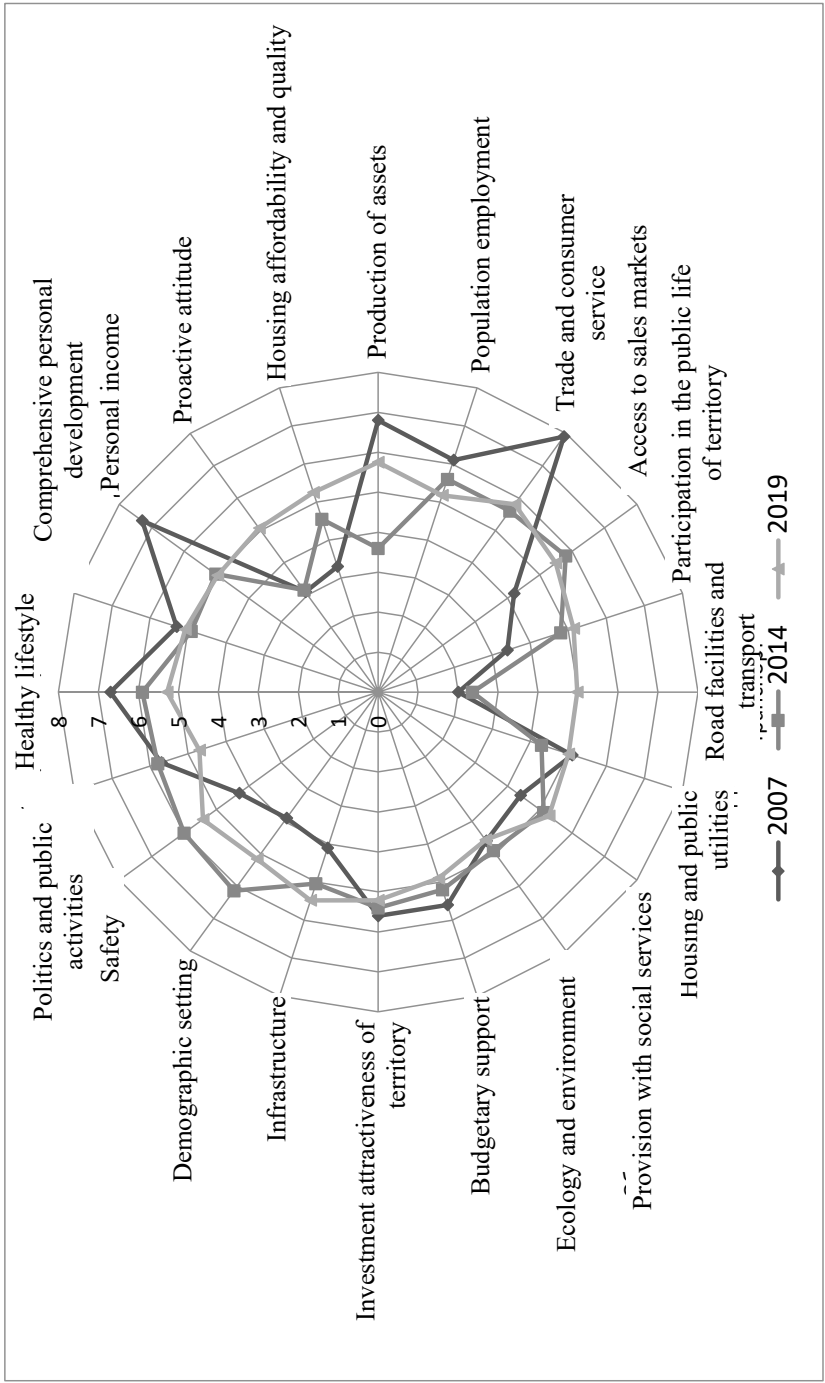
As is seen from figure provided above, the life quality of population in Russia has been assessed by the respondents over the last years as having steady positive dynamics as a whole. The indicator value “higher than five” means the positive change in this indicator as compared to the previous period. From the analysis conducted, it can be said that there are progressively positive changes in most of the indicators, without any significant surges and oscillations.

Population life quality change study results in Russia during COVID-19 pandemic (as compared to years 2018–2019–2020.)

At the same time, indicators were reduced in period of restrictions imposed due to COVID-19 pandemics during the year 2020 as compared to the previous year (Fig. 4). The population life quality values “less than average” were registered for such factors as population employment, demographic setting, politics and public activities.

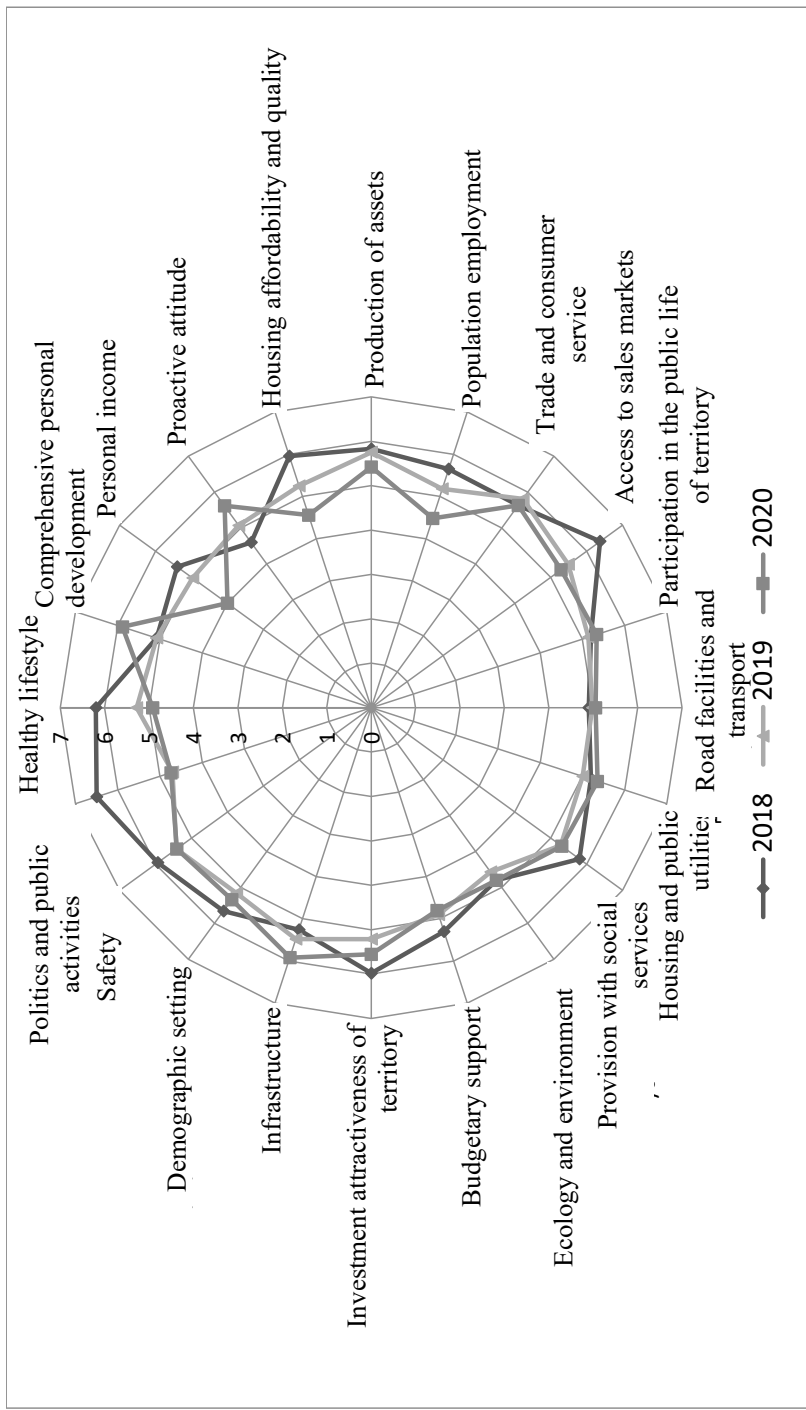
⁴ Zakharova S.G., Somenkova N.S., *Immediacy of the problem of transformation of the population life quality management processes*, Economics and society: International Journal of Research and Practice, No. 7–8 (12), 2019, pp. 3–8, <https://elibrary.ru/item.asp?id=39419231>.

Fig. 3 Population life quality assessment in Nizhniy Novgorod in years 2007, 2014, 2019



Source: Developed and compiled by authors.

Fig. 4. Factors influencing life satisfaction for the years 2018, 2019 and 2020



Source: Developed and compiled by authors.

The similar study was conducted on the group of “Young Students” that belonged to the most vulnerable categories of the population. During COVID-19 pandemics, the educational environment of higher educational institutions changed to “e-Learning”, as in many European countries⁵. The sociological questionnaire conducted shows what was changed in youth lives during pandemics (Fig. 5). The indicators as: “healthy lifestyle”, “comprehensive personal development”, and “increase in proactive attitude” specific to the growth in political activity became increased. It is noted that the communication between social groups changed to another format (social networks, Web-space)⁶ and had positive impact on relationships between economic entities and social institutes. The indicator “trade and consumer service” is better than in the previous year. The employment capabilities for students are increased because of the wide possibilities to implement professional competencies in cyberspace.

There are no complaints against the housing and public utilities system because the interaction with administrative establishments of different levels is simplified, and the use of a large list of services within digital economics saves time and excludes administrative red tape. Profession-wide social adaptation becomes easier, excludes social inequality, and depends on professional competence level and digital technology proficiency skills only⁷.

Corona virus pandemics have stimulated implementation of innovative technologies in every area of life incl. education⁸. The new digital technologies in education assist in the formation of high-demand digital competences and in quick and qualitative solution of real-life problems by changing image and life quality of students⁹. The on-line format becomes a source of creativity,

⁵ Najmul H., Yukun B., *Impact of «e-Learning crack-up» perception on psychological distress among college students during COVID-19 pandemic: A mediating role of «fear of academic year loss»*, Children and Youth Services Review, <https://doi.org/10.1016/j.childyouth.2020.105355>.

⁶ Aguilera-Hermida P., *College students' use and acceptance of emergency online learning due to COVID-19*, International Journal of Educational Research Open, <https://doi.org/10.1016/j.ijedro.2020.100011>.

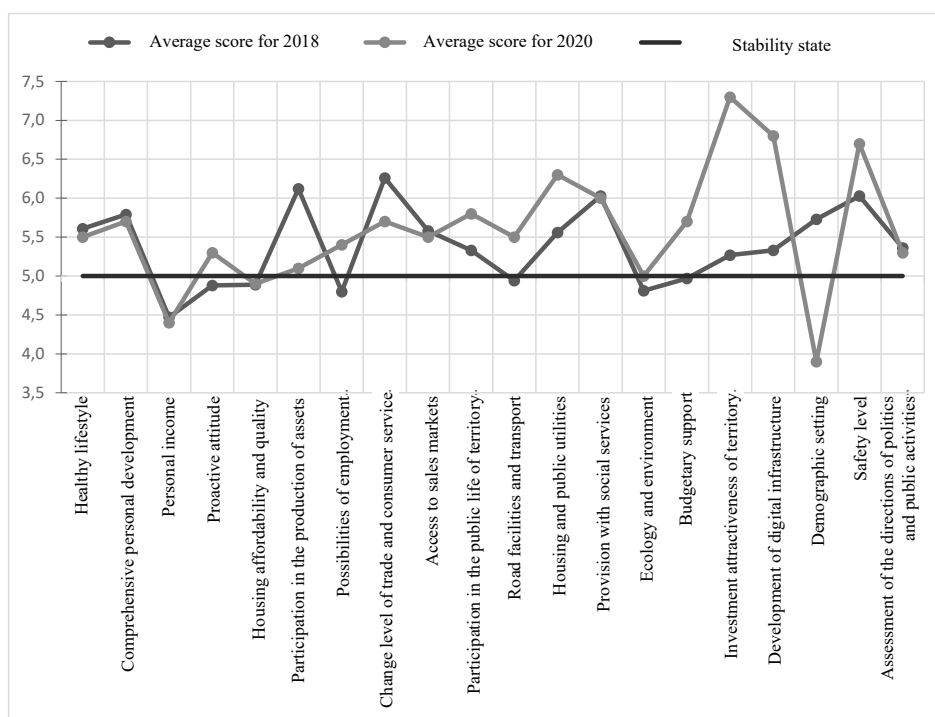
⁷ Ratten V., Jones P., *COVID-19 and entrepreneurship education: Implications for advancing research and practice*, The International Journal of Management Education, <https://doi.org/10.1016/j.ijme.2020.100432>.

⁸ Giordano L. et al., *Impact of COVID-19 on undergraduate and residency training*, The Surgeon, <https://doi.org/10.1016/j.surge.2020.09.014>.

⁹ Konstantinova D.S., Kudaeva M.M., *Digital competences as a basis for professional education transformation*, Labour Economics, Vol. 7, No. 11, 2020, doi:10.18334/et.7.11.111073.

gives an opportunity to develop a wide spectrum of professional competences¹⁰ as compared to traditional approach which main educational component is memorability. However, digitalization limits the ability to communicate and to create family relations, which is directly related to demography. Students note decrease in income level and housing affordability, even with mortgage rates decreased. Reviewing population life quality factorial approach model makes it apparent that earned income is unequal to the income generated from implementation of another production factors in economics¹¹.

Fig. 5. Change assessment of factors that have an influence on life quality of students



Source: Developed and compiled by authors

¹⁰ Batova M.M., *The formation of digital competences in the system "Education – Science – Production"*, Issues of innovation-based economics, Volume 9, No. 4, 2019, pp. 1573-1584, doi:10.18334/vinec.9.4.41467.

¹¹ Zakharova S.G., Borisov S.A., Lapshina E.N., Ozina A.M., Chernyshov A.N., *Specifics of Forming the Russian Middle Class According to the Factorial Model of Management Living Standards, Quality-Access to Success (QAS)*. Vol. 22, No. 181, 2021, pp. 110–116, https://www.srac.ro/calitatea/en/arhiva/2021/QAS_Vol.22_No.181_April.2021.pdf.

In adaptation to corona virus pandemics conditions in Russia, a global competitive infrastructure is created, and the life quality appears in correlations between changes and the significant life values based on social motivation of youth to progress. The foreign colleagues come to similar conclusions, and it is noted in a number of works¹², but technical and technological problems are noted as those among significant problems¹³.

The state support measures for population and business structures in Russian Federation during COVID-19 pandemic

In order to achieve the expected results foreseen by target development directions of Russia, the regulatory legal acts that support the various strata of the population were developed and put into effect. The primary state support measures for businesses and citizens during COVID-19 pandemics in the years 2020 to 2021 are provided in Fig. 6.

Even during such complex socio-economic situation and with the solid supporting measures taken by state authorities, there are always unhappy persons in high democratization conditions of the society who criticize and have nothing to propose.

In the years 2019 to 2020, the protest movement against restrictions imposed during pandemics became active in Moscow and other cities in Russia, just like in many European countries. The simple question of what the opposition movements could propose to improve the life quality of population remains unanswered, just like the question regarding contents of demands put forward by manifestation participants.

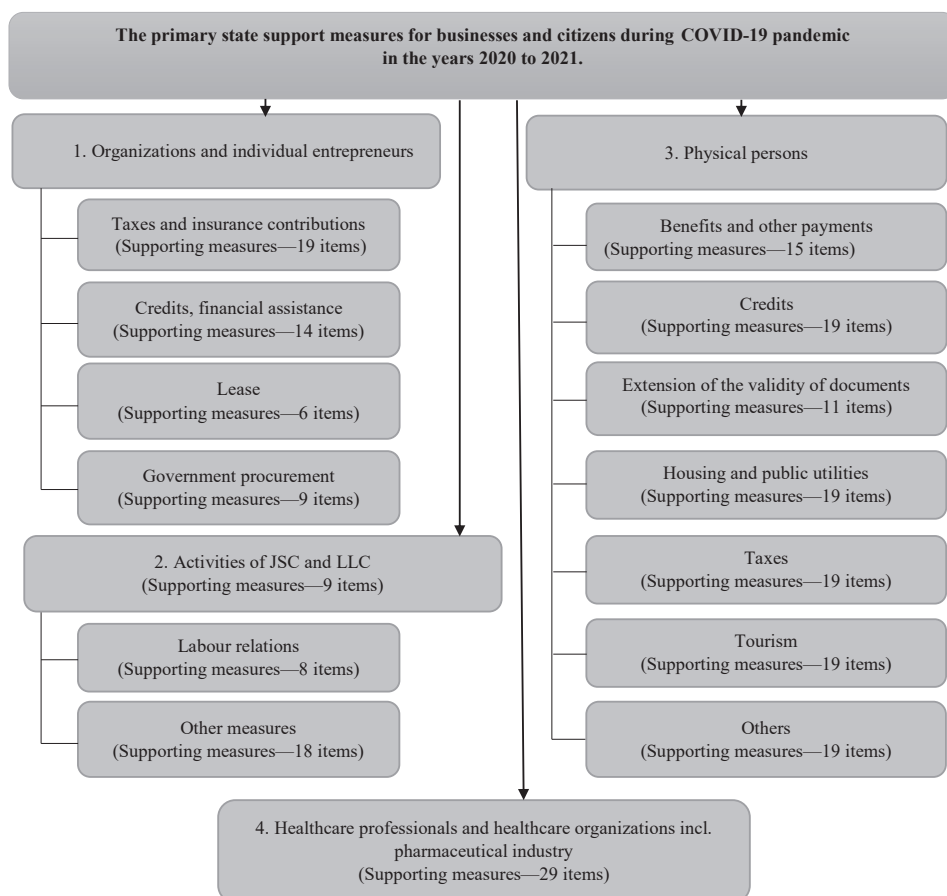
In order for the social initiatives of the active part of population to be implemented by state authorities, the annual open competition “Leader of Russia” was developed, and every citizen of Russia can participate in it. The competition’s program includes not only the comprehensive assessment of intellectual capacity of a person who has the high-performance capabilities as

¹² Radošević T., *Quality of life shown in correlations between significant socio-personal values of students and employees and their attitudes towards change*, International Journal for Quality Research, June 2019, <https://doi.org/10.18421/IJQR12.03-11>.

¹³ Hussein E., Daoud S., Alrabaiah H., Badawi R., *Exploring undergraduate students’ attitudes towards emergency online learning during COVID-19: A case from the UAE*, Children and Youth Services Review, <https://doi.org/10.1016/j.chilyouth.2020.105699>.

a public leader, but also offers the opportunity to provide its own program to solve a topical issue oriented to the specific social group. It is here that you can get a wide publicity of the project and get popular support. In modern Russian society, conditions are being created that allow your leadership potential to be implemented in practice, paying more and more attention to supporting social projects and society-important initiatives.

Fig. 6. The primary state support measures for businesses and citizens during COVID-19 pandemics in the years 2020-2021



Source: Developed and compiled by authors.

Conclusions

The paper defines and substantiates factors that have an impact on life quality of the population, and the indicator list is classified between different socio-economic relationship parties.

The results of the population life quality indicator change study conducted are given for the years 2007, 2014, 2019, and 2020 (the year of significant restrictions during COVID-19 pandemic). The assessment of COVID-19 pandemic impact on the changes in the population life quality indicators is provided as analytical drawings.

The results of the sociological survey of those surveyed with incomplete higher education on the assessment of factors that had an impact on their life quality during COVID-19 pandemic are highly interesting, and they are provided as analytical drawings as well.

In the troubled isolation period of COVID-19 pandemic, the Government of the Russian Federation developed a comprehensive list of measures of State support for businesses and citizens. The list of the supporting measures covers primarily following groups:

- Organizations and individual entrepreneurs (the supporting measures of 48 points),
- JSC and LLC activities incl. labour relationship and other measures (the supporting measures of 35 points),
- Physical persons incl. benefits and other payoffs, credit deferments, document validity prolongations, public utilities sector benefits, tax adjustments, tourism and other measures (the supporting measures of 121 points),
- Healthcare professionals and organizations incl. pharmaceutical industry (the supporting measures of 29 points).

Thus, in Russia certain factors that comprise the life quality of the population decreased during pandemic. However, it should be noted that no crisis-related conditions exist. The measures taken of State support allow for the support to business structures, especially to small businesses and the most vulnerable population, timely and selectively.

Literature

Decree of the President dated May 07, 2018, No. 204 (rev. dated July 19, 2018) "On the national objectives and strategic tasks for development of the Russian Federation for the period of up to the year 2024".

Zakharova S.G., Somenkova N.S., *Relevant problems of process transformation of living standards management*, Economics and business, No. 7–8 (12) 2019, <https://elibrary.ru/item.asp?id=39419231>.

Zakharova S.G., Borisov S.A., Lapshina E.N., Ozina A.M., Chernyshov A.N., *Specifics of Forming the Russian Middle Class According to the Factorial Model of Management Living Standards*, Quality-Access to Success (QAS), Vol. 22, No. 181, 2021, <https://doi.org/10.1051/shsconf/202110302005>.

Zakharova S.G., Yashin S.N., Sukhodoeva L.F, Somenkova N.S., Tumanov S.V. *Assessment of the professional competencies formation in students in the course of implementing online digital learning technologies*, International Scientific and Practical Conference "Solovyov Historical and Philosophical Readings. Russian and Foreign Experience in the System of Humanities Education: History, Modernity, Prospects" 2020, SHS Web of Conferences, Volume 103, 2021, <https://doi.org/10.1051/shsconf/202110302006>.

Zakharova S.G., Kulagova I.A., Makarycheva I.V., Oranova M.V., Rusakova T.J., *The Influence of Innovative Digital Technologies in Education on the Life Quality of Students During the Pandemic*, International Scientific and Practical Conference "Solovyov Historical and Philosophical Readings. Russian and Foreign Experience in the System of Humanities Education: History, Modernity, Prospects" 2020, SHS Web of Conferences, Volume 103, 2021, <https://doi.org/10.1051/shsconf/202110302005>.

Zakharova S.G., *Factorial approach to population life quality management*, *International Journal of Professional Science*, No. 1, 2017, <https://www.elibrary.ru/item.asp?id=28315377>.

Giordano L. et al., *Impact of COVID-19 on undergraduate and residency training*, The Surgeon, <https://doi.org/10.1016/j.surge.2020.09.014>.

Hussein E., Daoud S., Alrabaiah H., Badawi R., *Exploring undergraduate students' attitudes towards emergency online learning during COVID-19:*

- A case from the UAE*, Children and Youth Services Review, <https://doi.org/10.1016/j.childyouth.2020.105699>.
- Najmul H., Yukun Bao *Impact of «e-Learning crack-up» perception on psychological distress among college students during COVID-19 pandemic: A mediating role of «fear of academic year loss»*, Children and Youth Services Review, <https://doi.org/10.1016/j.childyouth.2020.105355>.
- Aguilera-Hermida P., *College students' use and acceptance of emergency online learning due to COVID-19*, International Journal of Educational Research Open, <https://doi.org/10.1016/j.ijedro.2020.100011>.
- Ratten V., Jones P., *COVID-19 and entrepreneurship education: Implications for advancing research and practice*, The International Journal of Management Education, <https://doi.org/10.1016/j.ijme.2020.100432>.
- Radošević T., *Quality of life shown in correlations between significant socio-personal values of students and employees and their attitudes towards change*, International Journal for Quality Research, June 2019, <https://doi.org/10.18421/IJQR12.03-11>.

Wydawnictwo
bernardinum

ISBN 978-83-8127-788-4



9 788381 277884