PRZEDSIĘBIORSTWO przyszłości

Kwartalnik Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej

Numer 3(52) lipiec 2022, Rok wyd. XIV ISSN: 2080-8461

Tytuł czasopisma w języku angielskim:

Enterprise of the Future

Wszystkie artykuły zamieszczane w kwartalniku są recenzowane
All articles published in the periodical are subject to reviews

ISSN 2080-8461

Projekt okładki
Krzysztof Waloszczyk

Adres wydawcy
Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej
ul. Jutrzenki 135, 02-231 Warszawa
tel.: 22 26 28 800
e-mail: wydawnictwo@uth.edu.pl
www.uth.edu.pl

Opracowanie redakcyjne
Joanna Paszkowska

Druk
Fabryka Druku Sp. z o.o.
ul. Zgrupowania AK „Kampinos" 6, 01-943 Warszawa
www.fabrykadruku.pl

SPIS TREŚCI

CONTENTS

Magdalena Ścigała

DOŚWIADCZANIE STRESU ORAZ BRAKU RÓWNOWAGI MIĘDZY PRACĄ A ŻYCIEM OSOBISTYM PODCZAS PRACY ZDALNEJ

Wstęp

Zmiany zachodzące w życiu każdego człowieka mogą stać się źródłem doświadczanego stresu. Wiążą się bowiem z koniecznością dostosowania do nowych warunków, nauczenia nowych sposobów funkcjonowania, przeorganizowania procesów, zmiany zwyczajów itp. Zmiany działają stymulująco, ale również obciążająco na system nerwowy człowieka. Nie bez powodu Abraham Maslow usytuował potrzebę bezpieczeństwa jako drugą w hierarchii ludzkich potrzeb. Dotyczy ona nie tylko bezpieczeństwa fizycznego, lecz także psychologicznego, czyli powtarzalności, rutyny, przewidywalności. Każda zmiana jest więc ze swej natury źródłem deprywacji w zakresie potrzeby bezpieczeństwa i tym samym może być źródłem stresu. Ponieważ różni ludzie mają różne zapotrzebowanie na stymulację i różny poziom tolerancji niepewności, w odmienny sposób reagują na te same zmiany zachodzące w otaczającym ich świecie.

Koncepcje stresu w psychologii

W ciągu 70 lat badań[1] psycholodzy ujmowali stres trojako, tj.:

1) jako bodziec (np. Irving Janis, Thomas Holmes, Richard Rahe);
2) jako reakcję (np. Hans Selye, David Mechanica, Tomasz Kocowski);

[1] Pojęcie stresu zostało wprowadzone do psychologicznej literatury naukowej w latach 50. ubiegłego wieku przez Hansa Selyego. W ujęciu biologicznym na początku XX wieku terminem tym operował już Walter Cannon w odniesieniu do reakcji zwierząt na sytuację zagrożenia (model „walcz lub uciekaj"), a jeszcze wcześniej termin ten stosowany był w fizyce do określania odporności metali na obciążenia. A. Grygorczuk, *Pojęcie stresu w medycynie i psychologii*, „Psychiatria" 2008, t. 5, nr 3, s. 111–115.

3) jako transakcję (np. Richard Lazarus, Susan Folkman, Stevan Hobfoll, Tadeusz Tomaszewski, Janusz Reykowski, Jan Strelau)[2].

W ujęciu stresu jako bodźca zakłada się, że stresem jest „zmiana w otoczeniu, która typowo, tj. u przeciętnego człowieka, wywołuje wysoki stopień napięcia emocjonalnego”[3] i może utrudniać funkcjonowanie. Stresem są więc różne wydarzenia, jak w ostatnich latach pandemia COVID-19, wojna na Ukrainie, wysoka inflacja, groźba utraty pracy, a także zmiany obowiązujących przepisów. W takim ujęciu nasilenie doświadczanego stresu można określić przez ocenę zdarzeń z pominięciem faktycznego indywidualnego wpływu zdarzeń na osobę. W badaniach z lat 60. ubiegłego wieku zidentyfikowano szereg ogólnych stresorów, wydarzeń życiowych, które ujęto w tzw. listę 43 stresujących zdarzeń życiowych[4] (Skala społecznego ponownego przystosowania się, SRRS – Social Readjustment Rating Scale Thomasa Holmesa i Richarda Rahe'a[5]). W badaniach tych autorów okazało się, że istnieje wysoka zgodność (korelacja na poziomie 0,9) oceny stopnia trudności i poziomu stresu poszczególnych wydarzeń życiowych w różnych grupach badanych (zróżnicowanych ze względu na wiek, płeć, wykształcenie, stan cywilny)[6]. Takie wyniki wskazują na istnienie tzw. obiektywnych stresorów. Na liście aż 33 razy wymieniono zdarzenia, które dotyczą bezpośrednio zmian w życiu, a dziewięć dotyczy zmian w obszarze życia zawodowego, np. reorganizacja firmy, zmiana stopnia odpowiedzialności w życiu zawodowym, zmiana warunków pracy czy wzmożenie wysiłku dla wykonywania jakiegoś zadania, zwolnienie z pracy, konflikty z przełożonym. Z badań Holmesa i Rahe'a wynika zależność statystyczna między stresorami a prawdopodobieństwem wystąpienia konsekwencji somatycznych w postaci choroby. Związek stresu ze zdrowiem podkreślany jest od samego początku prowadzenia badań nad stresem, czyli lat 30. XX wieku.

Kolejne i zdecydowanie odmienne ujęcie stresu utożsamia go z reakcją, np. dyskomfortu, i wskazuje na konkretne reakcje człowieka[7]. Stres jest więc niczym innym jak reakcją na sytuację. Tak rozumiany stres objawia się na trzech poziomach: fizjologicznym, psychologicznym i behawioralnym. Twórca pojęcia stresu i jego adaptator na gruncie psychologii, Hans Selye, koncentrował się na rozumieniu stresu jako reakcji fizjologicznej. Według niego stres to niespecyficzna reakcja

---

[2] I. Heszen, *Psychologia stresu*, Wydawnictwo Naukowe PWN, Warszawa 2014.

[3] *Ibidem*, s. 22.

[4] T.H. Holmes, R.H. Rahe, *The Social Readjustment Rating Scale*, „Journal of Psychosomatic Research” 1967, nr 10, s. 121–132.

[5] Polska wersja skali to Kwestionariusz zmian życiowych (KZŻ).

[6] J. Strelau, A. Jaworowska, K. Wrześniewski, P. Szczepanik, *Kwestionariusz radzenia sobie w sytuacjach stresowych. Podręcznik*, Pracownia Testów Psychologicznych, Warszawa 2013, s. 5–7.

[7] To odmienne rozumienie stresu znajduje swoje odbicie w potocznym opisywaniu doświadczeń związanych ze stresem. Mówi się np. „miałem dziś taki stres” (bodziec) albo „bardzo się zestresowałem” (reakcja).

organizmu powstająca w odpowiedzi na stawiane mu żądania, działanie bodźców szkodliwych. W psychologii oprócz reakcji na poziomie fizjologicznym akcentuje się wymiary: poznawczy, emocjonalny i behawioralny. Najczęstsze przykłady reakcji obrazuje tabela 1. Reakcje te są traktowane jako oblicza, ale i oznaki doświadczanego stresu.

Tabela 1. Typowe reakcje odczuwane przez człowieka w związku z doświadczanym stresem

Reakcje na poziomie fizjologicznym	Reakcje na poziomie psychologicznym	Reakcje na poziomie behawioralnym
• przyśpieszony puls, kołatanie serca, drżenie, bóle w klatce piersiowej, • napięcie mięśni, sztywność karku, • rozszerzenie źrenic, • potliwość, • suchość w jamie ustnej, ucisk w gardle, • nadmierna ruchliwość, • uczucie gorąca, zimna, • ból brzucha, biegunki lub zaparcia, • bezsenność lub wzmożona senność, • utrata apetytu lub nadmierny apetyt, • zawroty w głowie, • osłabienie popędu płciowego, • osłabienie odporności, • wypadanie włosów, • przyśpieszenie procesów starzenia się	• rozdrażnienie, wrogość, agresja, złość, • apatia, przygnębienie, poczucie bezsilności, osamotnienia, • zachwianie poczucia własnej wartości, • brak zadowolenia z życia, • lękliwość, • osłabienie pamięci, problemy z koncentracją, • wahania nastroju, • depresja	• tiki nerwowe, obgryzanie paznokci, • sięganie po używki, • obniżona wydajność, • wycofanie z relacji społecznych, • konfliktowość, pobudliwość, • brak decyzyjności, • brak aktywności, • nadmierna aktywność

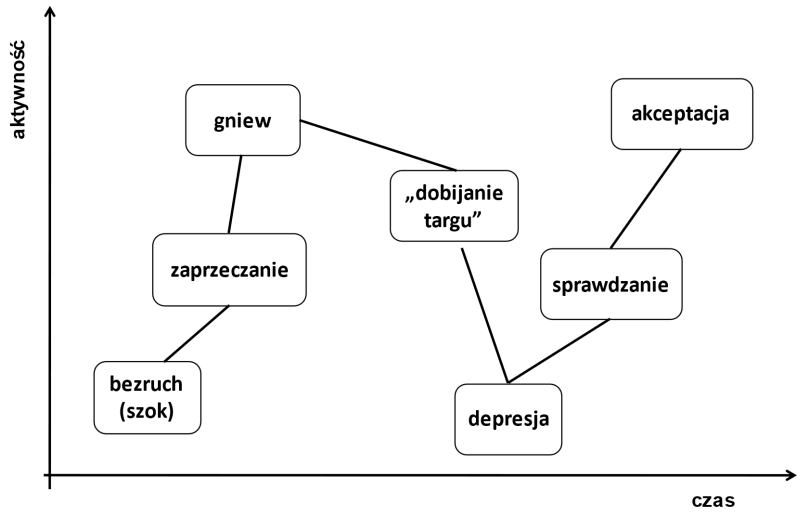
Źródło: opracowanie własne.

W prezentowanej koncepcji stres jest reakcją na niepożądane bodźce, tj. organizm odpowiada na zaistniałą trudną sytuację, reagując w określony sposób. Praktycznie zawsze w tym ujęciu stres wiąże się z zaburzeniem równowagi, homeostazy, a więc z pewną zmianą w środowisku. Jedną z najczęściej opisywanych reakcji na zmiany jest m.in. opór wobec zmian. Robert K. Merton[8] zauważa, że w obliczu zmian ludzie reagują: konformizmem, innowacją, potrzebą działania, rytualizmem, wycofaniem lub buntem. Wszystkie te zachowania to reakcje dosyć typowe w obliczu doświadczanego stresu, dyskomfortu. Natomiast trzy ostatnie

[8] M. Sobka, *Zmiany organizacyjne w teorii i praktyce*, Politechnika Lubelska, Lublin 2014, s. 49.

z wymienionych reakcji to także różne przejawy oporu czy to biernego, nieujawnianego, czy też czynnego, otwartego. Można więc pokusić się o stwierdzenie, że jedną z przyczyn oporu wobec zmian jest stres doświadczany w organizacji.

Zmiany w życiu zawodowym, które najczęściej ujmowane są jako proces i mają swój przebieg i dynamikę, wywołują długotrwałe napięcie emocjonalne. Selye pisał o zróżnicowanym reagowaniu jako przechodzeniu przez kolejne trzy stadia: najpierw przez fazę alarmu, gdy następuje pełna mobilizacja i bunt, potem fazę odporności, gdy utrwalają się wypracowane metody radzenia sobie z sytuacją, najczęściej przez długotrwałe stawianie oporu, aż po fazę wyczerpania, kiedy organizm doświadcza nadmiernej utraty sił i poddaje się[9]. Stres rozumiany jako reakcja na zmianę to także z całą pewnością proces przechodzenia przez fazy o odmiennej specyfice emocjonalnej (od gniewu przez smutek do akceptacji), o odmiennym ładunku emocjonalnym aktywizującym do działania (od bezruchu, bezczynności po przeciwdziałanie, a potem sprawdzanie nowych metod pracy). Mariusz Bratnicki ujmuje proces reagowania na zmiany organizacyjne w sposób analogiczny do modelu Elisabeth Kubler-Ross (rys. 1)[10].



Rys. 1. Fazy reakcji na zmiany organizacyjne według modelu M. Bratnickiego

Źródło: opracowanie własne na podstawie: M. Sobka, *Zmiany organizacyjne w teorii i praktyce*, Politechnika Lubelska, Lublin 2014, s. 52; M. Bratnicki, *Zarządzanie zmianami w przedsiębiorstwie*, Wydawnictwo Akademii Ekonomicznej, Katowice 1998, s. 72; A. Zarębska, *Zmiany organizacyjne w przedsiębiorstwie*, Difin, Warszawa 2002, s. 170–172.

[9] A. Grygorczuk, *Pojęcie stresu…*, *op.cit.*

[10] W modelu E. Kubler-Ross chodzi o sprawy ostateczne, tj. o reakcję na informację o śmiertelnej chorobie lub reakcję na informację o śmierci bliskiej osoby. E. Kubler-Ross, *Rozmowy o śmierci i umieraniu*, Media Rodzina, Poznań 1998.

Niedostatki obu podejść, traktujących stres czy to jako bodziec, czy to jako reakcję, związane z faktem, że stres nie jest zlokalizowany całkowicie ani w człowieka, ani w jego otoczeniu, zaowocowały podejściem relacyjnym. W ujęciu relacyjnym stres jest wynikiem nieodpowiedniego stosunku wymagań środowiska do możliwości podmiotu poradzenia sobie z zaistniałą sytuacją. Dodatkowo relacja ta naznaczona jest subiektywizmem, gdyż to podmiot ocenia, na ile dana sytuacja przerasta jego możliwości poradzenia sobie z nią, na ile posiada zasoby adekwatne do poradzenia sobie z zaistniałymi okolicznościami. Co więcej, to podmiot ocenia, czy sytuacja nosi znamiona stresującej. Wymagania sytuacji i środowiska mogą być obiektywne lub istniejące tylko w wyobrażeniach jednostki, jak również możliwości podmiotu mogą być realne lub subiektywnie oceniane. Podmiot może być bowiem nieświadomy posiadania odpowiednich kompetencji, zasobów. W poznawczo-transakcyjnej koncepcji stresu i radzenia sobie ze stresem Richarda Lazarusa i Susan Folkman „stres to określona relacja między osobą a otoczeniem, która jest oceniana przez osobę jako obciążająca lub przekraczająca jej zasoby oraz zagrażająca jej dobrostanowi”[11]. Zgodnie z tą koncepcją transakcja (czyli relacja wymagań sytuacji do możliwości poradzenia sobie z nią przez jednostkę) może zostać zaklasyfikowana przez podmiot jako: niemająca znaczenia, sprzyjająco-pozytywna albo stresująca. Ta ostatnia z kolei może mieć charakter: straty/krzywdy, zagrożenia albo wyzwania[12]. Doświadczenie straty/krzywdy wiąże się z koniecznością poradzenia sobie z czymś, co już się wydarzyło. Zagrożenie i wyzwanie mają charakter antycypacyjny, pojawiający się wówczas stres może mieć charakter mobilizujący do działania, a więc konstruktywny.

Doświadczanie stresu w związku z wdrażaniem zmian organizacyjnych

W ujęciu transakcyjnym zmiana organizacyjna i stopień, w jakim może być ona źródłem stresu, wydają się szczególnie interesujące. Oprócz posiadanych kompetencji radzenia sobie z sytuacją zmiany w dużej mierze reakcja na zmianę wiąże się z cechami temperamentalnymi, a doświadczanie stresu związanego ze zmianą wiąże się z uwarunkowaniami osobowościowymi. Na przykład osoby o niskiej wytrzymałości i wysokiej perseweratywności[13] oceniają zdarzenia i zmiany życiowe jako bardziej uciążliwe, natomiast osoby o wysokiej reaktywności emocjonalnej

[11] R.S. Lazarus, S. Folkman, *Stress, appraisal and coping*, Springer, New York 1984, s. 19.
[12] *Ibidem*, s. 28–30.
[13] M. Cyniak-Cieciura, B. Zawadzki, J. Strelau, *Formalna charakterystyka zachowania – kwestionariusz temperamentu: wersja zrewidowana. Podręcznik*, Pracownia Testów Psychologicznych, Warszawa 2016.

i wysokiej perseweratywności odczuwają więcej objawów psychosomatycznych, czyli stres w większym stopniu wpływa na ich stan zdrowia. Okazuje się też, że takie cechy osobowościowe, jak: otwartość na nowe doświadczenia, ugodowość, ekstrawersja oraz wewnętrzne umiejscowienie kontroli, sprzyjają występowaniu postawy innowacyjnej[14], która cechuje się dążeniem do zmian, przekonaniem, że zmiana to raczej okazja niż zagrożenie. Osoby o postawie innowacyjnej łatwiej adaptują się do zmian, nowych rozwiązań i nowych metod pracy, odczuwają mniejszy stres i radzą sobie z nim w sposób bardziej proaktywny. Przeciwieństwem postawy innowacyjnej jest postawa zachowawcza, której towarzyszy często przekonanie, że zmiana to zagrożenie. Osoby zachowawcze preferują sytuacje znane, sprawdzone metody pracy, dążą do utrzymania status quo, cenią bezpieczeństwo i przewidywalność, mogą też stosunkowo częściej niż inni pracownicy przeciwstawiać się zmianom, bo odczuwają wyższy poziom stresu związanego z wdrażaniem zmian w organizacji. Faktycznie obie te postawy to dwa krańce kontinuum opisującego różnice indywidualne w reagowaniu na zmiany organizacyjne[15].

Oprócz czynników osobowościowych na zachowanie pracownika w sytuacji postrzeganej jako stresowa wpływ ma indywidualny, preferowany styl radzenia sobie ze stresem, który może być pewną dyspozycją do reagowania w określony sposób. W psychologii zdrowia styl radzenia sobie definiowany jest jako „posiadany przez jednostkę, charakterystyczny dla niej repertuar preferowanych strategii radzenia sobie z sytuacjami stresowymi”[16]. Równocześnie styl może być adaptacyjny, czyli elastyczny, zmienny i dostosowywany w zależności od specyfiki sytuacji. Pracownicy natomiast różnią się nie tylko pod względem bogactwa repertuaru strategii, ale również pod względem łatwości zmiany strategii (zachowania) w zależności od sytuacji.

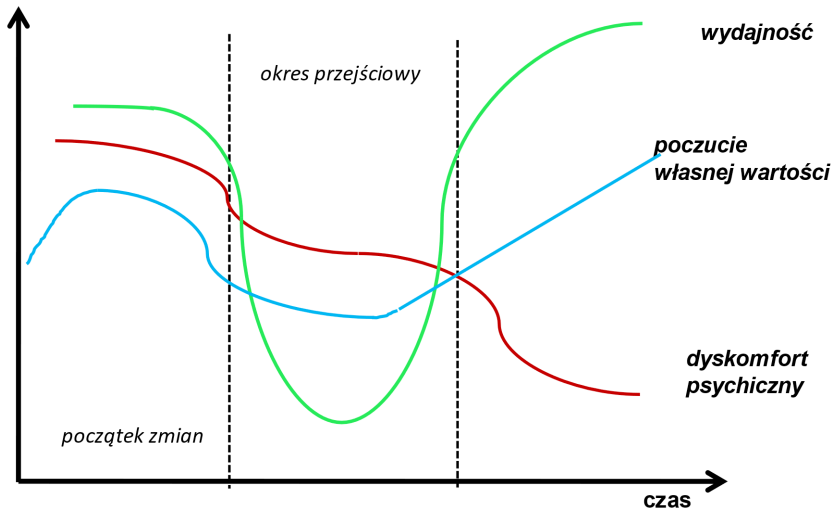
Stres organizacyjny związany ze zmianami, nowymi wymaganiami roli, koniecznością dostosowywania się i przeorganizowania metod pracy jest codziennością współczesnych pracowników. Największy dyskomfort występuje zwykle na początku procesu zmian, jeśli jednak proces zmian nie jest odpowiednio zarządzany (brak otwartej komunikacji, wsparcia w procesie uczenia się nowych rzeczy, włączania pracowniów i angażowania w proces zmiany), wówczas może utrzy-

[14] M. Sobka, *Zmiany organizacyjne…*, *op.cit.*; A. Rogozińska-Pawełczyk, *Osobowościowe uwarunkowania gotowości pracowników do zmian organizacyjnych,* „Zarządzanie Zasobami Ludzkimi” 2013, nr 2(91), s. 95–106; M. Wolan-Nowakowska, *Wybrane wymiary osobowości a postawa wobec zmian pracowników firm prywatnych i państwowych*, w: *Człowiek wobec zmiany. Rozważania psychologiczne*, D. Kubacka-Jasiecka (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2002, s. 157–168.

[15] I. Nowakowska-Buryła, *Gotowość do zmiany a nabywanie kompetencji międzykulturowych przez nauczycieli wczesnej edukacji – o potrzebie eksploracji zagadnienia*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio J. Paedagogia–Psychologia” 2019, t. 32, nr 2, s. 95–108.

[16] I. Heszen, *Psychologia stresu*, *op.cit.*, s. 100.

mywać się przez długi czas i faktycznie utrudniać wdrażanie zmian. Odczuwany w procesie zmian stres, dyskomfort psychiczny, niepewność przyszłości wpływają na poczucie wartości pracowników, ich poczucie skuteczności, a w efekcie samą produktywność. Wzajemne relacje między dyskomfortem psychicznym (stresem), poczuciem własnej wartości pracowników, ich wydajnością oraz czasem wdrażania zmian prezentuje orientacyjnie rys. 2.



Rys. 2. Dyskomfort psychiczny, poczucie własnej wartości i wydajność pracowników podczas wprowadzania zmian organizacyjnych
Źródło: opracowanie własne na podstawie: A. Zarębska, *Zmiany organizacyjne…*, *op.cit.*

Okres przejściowy jest jednym z trudniejszych okresów, gdyż charakteryzuje się spadkiem wydajności, spadkiem poczucia własnej wartości oraz ciągle względnie wysokim poziomem stresu utożsamianym m.in. z odczuwanym dyskomfortem psychicznym. Aby zmiana organizacyjna została zaakceptowana i przyniosła oczekiwane rezultaty, potrzebuje czasu. Współcześni przedsiębiorcy, menedżerowie i pracownicy, przyzwyczajeni do szybkich wyników, są niecierpliwi. Brak widocznych efektów ich frustruje, spadek wydajności zniechęca do zmian, skłania do porzucenia obranej ścieżki. Tymczasem spadek wydajności jest nieunikniony w obliczu wdrażania zmian organizacyjnych. Pracownicy muszą nauczyć się funkcjonowania w nowy sposób, nabrać biegłości, a sama organizacja jako twór dosyć bezwładny musi przestawić się na tzw. nowe tryby. Zjawisko spadku wydajności i równoczesnego nasilającego się spadku wiary w powodzenie zmiany nazywane

bywa w literaturze długą, ciemną nocą innowatora[17]. Owa noc przytrafia się najczęściej pracownikom przechodzącym przez złożony i długotrwały proces zmian, a znajduje odzwierciedlenie w wątpliwościach dotyczących tego, czy warto było wprowadzać zmianę, w pesymizmie i utracie entuzjazmu wobec wydłużającego się okresu przejściowego. Jest to szczególnie widoczne wtedy, gdy zmiany mają charakter antycypacyjny, czyli wiążą się z realizowaniem śmiałych wizji innowatorów. Rzadziej zjawisko to dotyka pracowników podczas zmian o charakterze adaptacyjnym, czyli takich, które są koniecznością wynikającą ze zmian przepisów lub sytuacji gospodarczej, jak pandemia COVID-19 i konieczność wdrożenia rozwiązań pracy zdalnej.

Doświadczanie stresu w związku z wybuchem pandemii COVID-19 i pracą zdalną

Wybuchy epidemii lub pandemii[18] od zawsze wiązały się z dużą śmiertelnością. Dlatego też wybuch pandemii COVID-19 wiosną 2020 roku wywołał silne poczucie zagrożenia, naruszył bezpieczeństwo fizyczne i zdrowie obywateli, a w konsekwencji doprowadził do bardzo emocjonalnych, lękowych reakcji, w tym paniki. Zwykle dopiero po jakimś czasie od wybuchu pandemii zwraca się uwagę na jej psychologiczne konsekwencje, podobnie stało się też tym razem[19]. Pierwszym odczuwanym zagrożeniem było bowiem zagrożenie życia, potem dostrzeżono negatywne konsekwencje gospodarcze związane z ograniczeniem funkcjonowania niektórych sektorów gospodarki, głównie usług. Dopiero później zaczęto akcentować zagrożenie zdrowia psychicznego i dobrostanu społeczeństwa. Tym, co generowało szczególnie wysoki poziom stresu i w konsekwencji prowadziło do pogorszenia zdrowia psychicznego, były: poczucie bezradności, niewiedza[20], lęk

[17] A. Zarębska, *Zmiany organizacyjne w przedsiębiorstwie*, Difin, Warszawa 2002, s. 181.

[18] Epidemia definiowana jest jako występowanie ponadprzeciętnej liczby zachorowań na określoną chorobę zakaźną w określonym czasie na określonym terenie. Pandemia natomiast dotyczy szerszego zasięgu terytorialnego, np. na wielu kontynentach (minimum dwóch).

[19] „Psychologiczne i psychiatryczne konsekwencje epidemii w czasach nam współczesnych, przy niespotykanym przyspieszeniu transmisji wirusa na cały świat w wyniku globalizacji, zmian klimatycznych i szybkości przemieszczania się ludności, to dominujące, subiektywnie odczuwane, rzeczywiste lub domniemane poczucie zagrożenia ze strony innych ludzi, strach, niepewność i niepokój, a także objawy, jakie się pojawiają w reakcji na traumatyczny stres" – J. Heitzman, *Wpływ pandemii COVID-19 na zdrowie psychiczne*, „Psychiatria Polska" 2020, nr 54(2), s. 188.

[20] W zasadzie można tu mówić o niewiedzy w obliczu nadmiaru informacji dostępnych w sieci, co może być uznane za źródło infostresu. W dobie intensywnego rozwoju technologii informacyjnych i korzystania z nich w codziennym życiu i pracy rośnie znaczenie wcześniej pomijanego typu stresu, tzw. stresu informacyjnego (infostresu), stresorem często staje się nadmiar informacji. Człowiek, mając ograniczone możliwości przetwarzania poznawczego, nie radzi sobie ze zbyt licznymi, nieustannie emitowanymi informacjami (nadprodukcja informacji), doświadcza przeciążenia umysłu,

o siebie i najbliższych, niepewność co do przyszłości, izolacja społeczna, a nawet konieczność zmiany nawyków w różnych obszarach życia człowieka.

W związku z wybuchem pandemii 9,5 proc. aktywnych zawodowo Polaków przeszło obowiązkowo na pracę zdalną, a 17,5 proc. dostało taką możliwość, z czego większość skorzystała[21]. Przed wybuchem pandemii zaledwie 5,3 proc. pracowników korzystało z tego rozwiązania regularnie i 9,8 proc. okazjonalnie[22]. Zdalne świadczenie pracy dotyczyło w największym stopniu grupy pracowników klasyfikowanej jako specjaliści, czyli osób z wykształceniem wyższym. W obliczu zagrożenia zdrowia i życia zmiana nawyków związanych ze sposobem i miejscem wykonywania pracy wydawała się zaledwie drobnym stresorem. Jednak ze względu na fakt, że pracownicy spędzają w pracy średnio osiem godzin dziennie, stresor ten można zaliczyć do stresorów uporczywych, długotrwałych. Także z perspektywy upływającego czasu widać, że konsekwencje tego rozwiązania dla dobrostanu pracowników były znaczące i nie zawsze korzystne.

Badanie sondażowe przeprowadzone przez Hays we wrześniu 2020 roku, a więc po pierwszej fali pandemii, wykazało, że do pogorszenia stanu zdrowia psychicznego doszło w przypadku 32 proc. pracowników (specjalistów i menedżerów). „Najtrudniejszymi do zaakceptowania okazały się: brak bezpośrednich interakcji z zespołem, pełnienie nowej, innej niż przed pandemią roli, a także praca z domu"[23]. W badaniu przeprowadzonym równo rok później przez firmę rekrutacyjną MichaelPage okazało się, że ponad 60 proc. badanych odczuwa negatywne skutki pandemii, a 42 proc. wymieniło brak równowagi między pracą a życiem jako jedną z ważniejszych negatywnych konsekwencji przejścia na pracę zdalną. Respondenci, wskazując na skutki pandemii i przejścia na pracę zdalną, wymieniali m.in.: wyższy poziom stresu (22 proc.), utratę lub przyrost wagi (20 proc.), pogorszenie jakości snu (19 proc.), wyższy poziom frustracji i złości (18 proc.) oraz niższy poziom motywacji do pracy (17 proc.)[24].

---

co jest również zaliczane do źródeł stresu. M. Ledzińska, *Człowiek współczesny w obliczu stresu informacyjnego*, Wydawnictwo Instytutu Psychologii PAN, Warszawa 2009.

[21] *Pół Polski przeszło na pracę zdalną? Rzeczywiste liczby zaskakują*, 20.10.2020 r., https://businessinsider.com.pl/firmy/praca-zdalna-w-polsce-w-czasie-pandemii-ilu-z-nas-pracowalo-z-domu/c5rwvdm, dostęp: 20.01.2022 r.; *Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce w pierwszym kwartale 2021 r.,* GUS, 10.06.2020 r., https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5820/4/5/1/wplyw_epidemii_covid-19_na_wybrane_elementy_rynku_pracy_w_polsce_w_1_kwartale_2021_roku.pdf, dostęp: 20.01.2020 r.

[22] Eurostat – Data Explorer (europa.eu), http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do, dostęp: 18.01.2022 r.; *Working from home in UE*, Eurostat, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180620-1, dostęp: 18.01.2022 r.

[23] Https://www.hays.pl/blog/insights/trendy-i-wyzwania-w-nowej-rzeczywistosci, dostęp: 09.09.2022 r.

[24] *Mental Health & Well Being*, Candidate Pulse, https://www.michaelpage.pl/sites/michaelpage.pl/files/2021-09/Candidate%20Pulse%20slot%203%20Infographic%20PL_0.pdf, dostęp: 15.09.2022 r.

Wbrew pozorom możliwość pracy zdalnej to nie tylko szansa na spędzanie większej ilości czasu z najbliższymi w domu, brak kosztowych i czasochłonnych dojazdów, ale również wiele ograniczeń, np. w kontaktach ze współpracownikami i utrudnień w rozgraniczeniu sfery pracy i sfery prywatnej. Oto zestawienie najczęstszych stresorów, jakie towarzyszyły i nadal towarzyszą pracy zdalnej, z pespektywy pracownika:

- zła organizacja czasu pracy;
- brak samodyscypliny;
- poczucie bycia nieustannie w pracy;
- zacieranie się granicy między pracą a życiem osobistym;
- dłuższy czas pracy;
- brak bezpośredniego kontaktu ze współpracownikami i przełożonymi;
- ograniczona komunikacja, brak wymiany informacji, konsultacji;
- ograniczona współpraca;
- poczucie izolacji, osamotnienia i wyobcowania;
- słabsza więź z organizacją;
- brak życia społecznego, brak możliwości poznania nowych współpracowników i utrudnienia w komunikacji z nowo zatrudnionymi członkami zespołu;
- większe zmęczenie w związku z pracą w domu w obecności licznych dystraktorów (toczące się życie rodzinne, remonty sąsiadów), pogorszenie komfortu życia;
- konieczność samodzielnego rozwiązywania problemów bez odpowiedniego wsparcia np. technicznego, brak doraźnej pomocy;
- brak odpowiedniego wyposażenia stanowiska pracy (praca w warunkach sprzecznych z zasadami ergonomii);
- awarie sieci;
- zwiększenie kosztów utrzymania domu (np. opłat za energię elektryczną);
- poczucie bycia niedostrzeganym przez przełożonych, brak informacji zwrotnej;
- trudność w obiektywnej ocenie efektywności, produktywności pracowników;
- trudności w zakresie onboardingu;
- godziny pracy[25].

Każda zmiana w zakresie wykonywania obowiązków służbowych jest źródłem stresu. Zmiana polegająca na stworzeniu w przestrzeni domu biura i godzeniu w tym samym czasie i miejscu obowiązków z dwóch sfer życia: prywatnej i za-

[25] Na podstawie: *Aspekty pracy zdalnej z perspektywy pracownika, pracodawcy i gospodarki*, 15.12.2021 r., https://www.parp.gov.pl/storage/publications/pdf/Praca_zdalna_last.pdf.

wodowej okazała się również istotnym źródłem stresu. Przejście na pracę zdalną, z którego skorzystało wiele organizacji, nie zawsze wpłynęło korzystnie na równowagę między pracą a życiem (*work-life balance*). Wśród charakterystycznych zjawisk zachodzących podczas pracy zdalnej wymienia się efekt żonglowania zadaniami (*task juggling*), polegający na pracy w krótszych sekwencjach czasu z dłuższymi przerwami na wykonywanie obowiązków domowych lub rodzinnych. W efekcie rozwiązanie to prowadziło do wolniejszego, mniej efektywnego wykonywania zadań i dłuższego dnia pracy. Wykonywanie pracy zdalnej z domu sprzyjało pracy w nadgodzinach oraz dniach uznawanych za wolne, np. w weekendy, święta. Nie bez znaczenia było również psychologiczne obciążenie wynikające z nieustannego przechodzenia między rolą zawodową a domową (rodzinną). Krzyżowanie się tych sfer życia i nakładanie pozornie oddzielnych tożsamości jednostki (tj. zawodowej i prywatnej, np. rodzicielskiej) zgodnie z teorią granic może prowadzić do zmian psychologicznych i behawioralnych, a także konfliktu między sferą życia i pracy[26].

Z badań wynika, że w przypadku pracowników mających dzieci w największym stopniu na zaburzenie równowagi praca–życie miało wpływ zastosowanie modelu podwójnej zmiany, w którym kobieta pracuje zdalnie i równocześnie opiekuje się dziećmi pozostającymi w domu na nauczaniu zdalnym. Okazało się, że ten model sprzyjał zamknięciu kobiet w domu, mniejszej ilości czasu wspólnego (rodzinnego), mijaniu się partnerów, brakowi czasu na rozwój zawodowy oraz relaks i rezygnacji z własnych zajęć. Co ciekawe, negatywnych konsekwencji dla *work-life balance* nie zauważono w przypadku zastosowania modelu drugiej zmiany (zdalnie pracuje tylko mężczyzna) i modelu dzielonej podwójnej zmiany (zdalnie pracują zarówno kobieta, jak i mężczyzna)[27]. Brak równowagi między pracą a życiem jako źródło stresu jest także jednym z czynników ryzyka rozwoju wypalenia zawodowego.

Podsumowanie

Zdrowie psychiczne pracowników było przez lata tematem marginalizowanym w obszarze zarządzania, pozostającym raczej w domenie psychologii zdrowia oraz psychologii organizacji i pracy. Jednak odczuwany przez pracowników długotrwały stres, bardzo często niewidoczny dla pracodawcy i często lekceważony, generuje

[26] C. Kylin, *Coping with boundaries – A study on the interaction between work and non-work life in home-based telework*, Karlstads Universitet, January 2007, https://www.researchgate.net/publication/278000468, dostęp: 15.09.2022 r.

[27] P. Binder, *Praca zdalna w czasie pandemii i jej implikacje dla rodzin z dziećmi – badanie jakościowe*, „Przegląd Socjologii Jakościowej" 2022, t. 18, nr 1, s. 82–110.

koszty. Światowa Organizacja Zdrowia szacuje, że koszty obniżonej produktywności i wydajności spowodowanej zdrowiem psychicznym pracowników to około biliona dolarów. Tyle mniej więcej przedsiębiorstwa tracą rocznie z powodu problemów pracowników ze zdrowiem psychicznym[28]. Są to nie tylko spadki produktywności wywołane zwolnieniami lekarskimi, nieplanowaną absencją, błędami pracowników, ale także wysoką fluktuacją jako konsekwencją spadku motywacji i zaangażowania.

Dziś nie ulega już wątpliwości, że organizacje powinny dbać o dobrostan pracowników, w tym szczególnie pracowników będących w procesie zmian, którzy narażeni są na wyższy poziom stresu. Z jednej strony rośnie świadomość znaczenia kondycji psychicznej pracowników dla sprawnego i skutecznego działania organizacji. Z drugiej – podczas wprowadzania zmian ostatnią kwestią, o której zaczyna myśleć pracodawca i o którą próbuje zadbać menedżer, jest komfort psychiczny załogi.

Bibliografia

Literatura

Binder P., *Praca zdalna w czasie pandemii i jej implikacje dla rodzin z dziećmi – badanie jakościowe*, „Przegląd Socjologii Jakościowej" 2022, t. 18, nr 1.

Bratnicki M., *Zarządzanie zmianami w przedsiębiorstwie*, Wydawnictwo Akademii Ekonomicznej, Katowice 1998.

Cyniak-Cieciura M., Zawadzki B., Strelau J., *Formalna charakterystyka zachowania – kwestionariusz temperamentu: wersja zrewidowana. Podręcznik*, Pracownia Testów Psychologicznych, Warszawa 2016.

Grygorczuk A., *Pojęcie stresu w medycynie i psychologii*, „Psychiatria" 2008, t. 5, nr 3.

Heitzman J., *Wpływ pandemii COVID-19 na zdrowie psychiczne*, „Psychiatria Polska" 2020, t. 54, nr 2.

Heszen I., *Psychologia stresu*, Wydawnictwo Naukowe PWN, Warszawa 2014.

Holmes T.H., Rahe R.H., *The Social Readjustment Rating Scale*, „Journal of Psychosomatic Research" 1967, nr 10.

Kubler-Ross E., *Rozmowy o śmierci i umieraniu*, Media Rodzina, Poznań 1998.

Lazarus R.S., Folkman S., *Stress, appraisal and coping*, Springer, New York 1984.

Ledzińska M., *Człowiek współczesny w obliczu stresu informacyjnego*, Wydawnictwo Instytutu Psychologii PAN, Warszawa 2009.

Nowakowska-Buryła I., *Gotowość do zmiany a nabywanie kompetencji międzykulturowych przez nauczycieli wczesnej edukacji – o potrzebie eksploracji zagadnienia*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio J. Paedagogia–Psychologia" 2019, t. 32, nr 2.

Rogozińska-Pawełczyk A., *Osobowościowe uwarunkowania gotowości pracowników do zmian organizacyjnych*, „Zarządzanie Zasobami Ludzkimi" 2013, t. 91, nr 2.

[28] *Mental health in the workplace*, https://www.who.int/teams/mental-health-and-substance-use/promotion-prevention/mental-health-in-the-workplace, dostęp: 22.09.2022 r.

Sobka M., *Zmiany organizacyjne w teorii i praktyce*, Politechnika Lubelska, Lublin 2014.

Strelau J., Jaworowska A., Wrześniewski K., Szczepanik P., *Kwestionariusz radzenia sobie w sytuacjach stresowych. Podręcznik*, Pracownia Testów Psychologicznych, Warszawa 2013.

Wolan-Nowakowska M., *Wybrane wymiary osobowości a postawa wobec zmian pracowników firm prywatnych i państwowych*, w: *Człowiek wobec zmiany. Rozważania psychologiczne*, D. Kubacka-Jasiecka (red.), Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2002.

Zarębska A., *Zmiany organizacyjne w przedsiębiorstwie*, Difin, Warszawa 2002.

Netografia

Aspekty pracy zdalnej z perspektywy pracownika, pracodawcy i gospodarki, 15.12.2021 r., https://www.parp.gov.pl/storage/publications/pdf/Praca_zdalna_last.pdf.

Eurostat – Data Explorer (europa.eu), http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do.

Https://www.hays.pl/blog/insights/trendy-i-wyzwania-w-nowej-rzeczywistosci.

Https://www.stress.org/holmes-rahe-stress-inventory-pdf.

Kylin C., *Coping with boundaries – A study on the interaction between work and non-work life in home-based telework*, Karlstads Universitet, January 2007, https://www.researchgate.net/publication/278000468.

Mental Health & Well Being, Candidate Pulse, https://www.michaelpage.pl/sites/michaelpage.pl/files/2021-09/Candidate%20Pulse%20slot%203%20Infographic%20PL_0.pdf.

Mental health in the workplace, https://www.who.int/teams/mental-health-and-substance-use/promotion-prevention/mental-health-in-the-workplace.

Pół Polski przeszło na pracę zdalną? Rzeczywiste liczby zaskakują, 20.10.2020 r., https://businessinsider.com.pl/firmy/praca-zdalna-w-polsce-w-czasie-pandemii-ilu-z-nas-pracowalo-z-domu/c5rwvdm.

Working from home in UE, Eurostat, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180620-1.

Wpływ epidemii COVID-19 na wybrane elementy rynku pracy w Polsce w pierwszym kwartale 2021 r., GUS, 10.06.2020 r., https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5820/4/5/1/wplyw_epidemii_covid-19_na_wybrane_elementy_rynku_pracy_w_polsce_w_1_kwartale_2021_roku.pdf.

Streszczenie

Artykuł porusza kwestię stresu doświadczanego przez pracowników w obliczu zmian organizacyjnych, tj. zmian w zakresie wykonywania obowiązków zawodowych. Pandemia COVID-19 spowodowała wprowadzenie rozwiązań pozwalających na świadczenie obowiązku pracy zdalnie z miejsca zamieszkania. Zorganizowanie biura w domu i wykonywanie pracy zawodowej w nowych warunkach fizycznych (nie zawsze dostosowanych do realizacji tych zadań) okazało się źródłem dyskomfortu i stresu. Nie wszyscy pracownicy, którzy przeszli w czasie pandemii na pracę zdalną, oceniają ją pozytywnie. Rozwiązanie to nie zawsze wpłynęło korzystnie na równowagę między pracą a życiem (*work-life balance*). Wśród nowych niekorzystnych zjawisk wystąpił m.in. efekt żonglowania zadaniami (*task juggling*), który

prowadził do wolniejszego, mniej efektywnego wykonywania zadań i dłuższego dnia pracy, pracy w nadgodzinach i w dni wolne od pracy (weekendy, święta). Nieustanne przechodzenie między rolą zawodową a prywatną, krzyżowanie się tych do niedawna oddzielonych sfer życia i tożsamości generowało dodatkowe obciążenie psychiczne. Koszty utraty zdrowia psychicznego są wysokie dla organizacji i całej gospodarki, w związku z tym autorka wskazuje na konieczność dbania o dobrostan pracowników przechodzących przez zmiany organizacyjne.

Summary

In face of organizational changes people feel stressed. Pandemic COVID-19 triggered new solution in the organizations i.e., where, and how people work. Remote work, especially at home caused that plenty of people had to work in physical environment that wasn't adjust to it. Remote work and home office was in many cases the reason of stress, physical and mental discomfort. Working from home ruined sometimes work- life balance. Disadvantages of this solution are for example task juggling effect that influences productivity. People work longer because of more breaks caused by their home/family duties. For the same reason they work more often during weekends and generally spend more time working. Stress was induced by switching between professional identity and personal identity (e.g. parental identity) all the time. Loss of mental health was belittled and disregarded or even ignored for a long time. But the fact is that the costs of it are too serious for organizations to be ignored any more. The article shows how the stress and discomfort relate to changes in workplace and remote work and how important is to pay attention to employees' wellbeing.

Słowa kluczowe

Stres, równowaga między pracą z życiem, zmiana organizacyjna.

Keywords

Stress, work-life balance, organizational change.

Magdalena Ścigała – dr, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie, ORCID: 0000-0001-8073-7122.

Przemysław Jóskowiak

STARTUP A PRZEDSIĘBIORSTWO KLASYCZNE – CECHY DEFINIUJĄCE W KONTEKŚCIE E-COMMERCE

Wprowadzenie

Strategia cyfrowa „Kształtowanie cyfrowej przyszłości Europy”[1] zakłada, że do 2030 roku liczba startupów (i scaleupów), głównie z obszaru nowych technologii oferujących unikatowe rozwiązania wspierające proces cyfryzacji, wzrośnie o połowę[2]. Ten bardzo ambitny cel wymaga adekwatnego przygotowania i stworzenia odpowiednich warunków ramowych. Ma temu służyć inicjatywa „Startup Nations Standard of Excellence” będąca wspólną deklaracją 24 państw członkowskich Unii Europejskiej[3] i Islandii, aby wspierać startupy europejskie na każdym etapie ich rozwoju.

Zgodnie z treścią deklaracji startupy mają niezaprzeczalny potencjał do tego, aby tworzyć przełomowe innowacje, nowe miejsca pracy, współpracować z klasycznymi przemysłami[4] oraz służyć jako fundamenty przyśpieszenia procesu zielonej i cyfrowej transformacji. Ich rozwój wymaga jednak szerokiego wsparcia instytucjonalnego ułatwiającego m.in. dostęp do właściwego finansowania[5] oraz gwarantującego korzystne uwarunkowania i równe szanse rozwoju dla wszystkich biznesów z każdego regionu Unii Europejskiej.

---

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Kształtowanie cyfrowej przyszłości Europy, Bruksela 2020, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0067&from=PL, dostęp: 01.07.2022 r.

[2] W strategii mowa jest o tzw. jednorożcach (*unicorns*), które cechują się wysokim poziomem innowacyjności i wartością rynkową powyżej 1 bln USD.

[3] Austria, Belgia, Cypr, Czechy, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Irlandia, Włochy, Łotwa, Litwa, Luksemburg, Malta, Niderlandy, Polska, Portugalia, Rumunia, Słowacja, Słowenia, Hiszpania i Szwecja.

[4] Komisja Europejska – Komunikat prasowy, 24 EU Member States commit at Digital Day to take action to support growth of EU Startups, Bruksela, 2021, https://digital-strategy.ec.europa.eu/en/news/24-eu-member-states-commit-digital-day-take-action-support-growth-eu-startups, dostęp: 01.07.2022 r.

[5] Zgodnie z raportem „The State of European Tech 2020” w 2020 roku zdecydowanie trudniej było pozyskać środki na założenie biznesu, https://2020.stateofeuropeantech.com/chapter/state-european-tech-2020/article/exec-sum/, dostęp: 1.07.2022 r.

Ostatecznym celem jest stworzenie odpowiednich warunków do tego, aby powstawało więcej startupów z potencjałem rozwoju w kierunku innowacyjnych przedsiębiorstw (sektor MŚP), które mogą konkurować także na arenie globalnej i przyczynić się do większej niezależności technologicznej całej Europy.

W kontekście wspomnianej deklaracji i strategii cyfryzacji istotne wydaje się wyraźne rozróżnienie pomiędzy przedsiębiorstwami, które można nazwać startupami w rozumieniu Komisji Europejskiej, a tymi, które mają cechy klasycznych biznesów. Rozważania dotyczące ich cech definiujących można przenieść na grunt szeroko rozumianej sprzedaży w sieci (e-commerce), ponieważ przestrzeń ta stanowi naturalne miejsce rozwoju przedsięwzięć o charakterze innowacyjnym. Widać to na przykładzie wielu popularnych startupów funkcjonujących wyłącznie jako biznesy internetowe.

Celem artykułu jest zatem podjęcie próby określenia kluczowych cech rozróżniających startupy od przedsiębiorstw klasycznych w kontekście sprzedaży w sieci poprzez identyfikację oraz analizę kluczowych kryteriów determinujących działalność na szeroko pojętym rynku e-commerce.

Podstawowe założenie

Mimo że startup jest pojęciem powszechnie znanym od długiego czasu, wciąż brakuje jednej definicji, która miałaby globalne zastosowanie w odniesieniu do wszystkich branż i podmiotów biznesowych. Jest to oczywiście zrozumiałe, gdyż pojęcie to ma charakter bardziej jakościowy i nie bazuje na typowych liczbowych kryteriach podziału przedsiębiorstw. W praktyce startup może być więc mikroprzedsiębiorstwem, małym lub średnim biznesem o różnych wielkościach obrotów i różnej formie prawnej.

W literaturze najczęściej przywoływana jest definicja startupu jako „ludzk[iej] instytucj[i] stworzon[ej] z myślą o budowaniu nowych produktów lub usług w warunkach skrajnej niepewności”[6]. Niepewność ta wynika z myślenia innowacyjnego, które w swoim założeniu ma wykraczać poza standardy (np. znane i zdefiniowane rynki) i tworzyć nową jakość (i nowe rynki). Jest to oczywiście doskonale zbieżne z równie popularną koncepcją błękitnego oceanu, gdzie „błękitne oceany są określane jako niewykorzystana przestrzeń rynkowa, kreowanie popytu i szansa na zyskowny wzrost”[7]. W tym sensie startupy to właśnie przedsiębiorstwa, które podążają ścieżką błękitnego oceanu, przesuwając istniejące granice rynków i tworząc własne grupy odbiorców.

[6] E. Ries, *Metoda Lean Startup*, Wydawnictwo Helion, Gliwice 2011, s. 28.

[7] W. Chan Kim, E. Mauborgne, *Strategia błękitnego oceanu,* Wydawnictwo MT Biznes, Warszawa 2010, s. 19.

Inna także chętnie cytowana definicja przedstawia startup jako „tymczasową organizację zajmującą się poszukiwaniem skalowalnego, powtarzalnego i rentownego modelu biznesowego”[8]. Owa tymczasowość oznacza oczywiście, że nie ma pewności, co będzie efektem końcowym działań podejmowanych przez startup poza gwarancją, iż przedsięwzięcie nie będzie już znajdowało się w punkcie wyjściowym. Istotą jest bowiem eksperymentowanie w celu wypracowania skutecznego sposobu generowania przychodów (modelu biznesowego) na dotychczas nieznanych przestrzeniach rynkowych. Tymczasowy charakter potęguje niepewność, o której była mowa wcześniej.

Aby móc rozgraniczyć przedsiębiorstwa typu startup i przedsiębiorstwa klasyczne i tym samym określić ich cechy definiujące w zakresie działalności e-commerce, choć nie tylko, konieczne jest przyjęcie konkretnych kryteriów porównawczych. Powinny one odnosić się do typowych obszarów decyzyjnych podmiotów rozpoczynających swoją działalność w sieci niezależnie do oferowanego produktu.

Rys. 1. Kluczowe obszary decyzyjne przedsiębiorstw działających w sieci
Źródło: opracowanie własne

W przypadku większości przedsiębiorstw szeroko pojętego rynku e-commerce pojawia się konieczność określenia następujących uwarunkowań:

- poziomu innowacyjności;
- znaczenia użytkownika sieci;

[8] S. Blank, B. Dorf, *Podręcznik startupu. Budowa wielkiej firmy krok po kroku*, Wydawnictwo Helion, Gliwice 2013, s. 19.

- wymogów technologicznych;
- potrzeb kapitałowych;
- dostępności modelu biznesowego;
- potencjału osiągnięcia rentowności.

Kryterium innowacyjności

Wydaje się oczywiste, że przedsiębiorstwa startupowe powinny różnić się od tych klasycznych poziomem swojej innowacyjności. Wynika to z samej definicji innowacji rozumianej jako „środ[ek], przy pomocy którego przedsiębiorca albo tworzy nowe zasoby, będące źródłem bogactwa, albo wyposaża istniejące zasoby w potencjał do jego kreowania”[9]. Bazując na wcześniejszych definicjach można niewątpliwie stwierdzić, iż tworzenie nowych zasobów utożsamiane jest głównie z działalnością startupów, podczas gdy biznesy klasyczne dokonują bardziej modyfikacji istniejących zasobów (dyferencjacja). Od „firm nowoczesnych”[10] oczekuje się bowiem podążania nie już przetartymi i sprawdzonymi ścieżkami, lecz poszukiwania, a nawet kreowania nowych dróg.

W praktyce zastosowanie kryterium innowacyjności do odróżnienia startupów od przedsiębiorstw klasycznych wiąże się jednak z licznymi wyzwaniami. Po pierwsze, trudno jednoznacznie określić, jaki poziom innowacyjności jest rzeczywiście konieczny, aby móc mówić już o startupie, a nie o biznesie tradycyjnym realizującym np. strategię dyferencjacji. Niewątpliwie każda firma może i powinna podejmować działania na rzecz optymalizacji swojej oferty także w ramach wyróżniania się na tle konkurencji. To może sprawiać trudności porównawcze. Po drugie, pojawia się pytanie, czy jest możliwa obiektywna ocena tego, czym innowacyjność startupowa różni się od innowacyjności klasycznej. A jeżeli tak, to kto powinien dokonać takiej oceny. Po trzecie, samo pojęcie innowacyjności[11] daje duże pole do interpretacji, co oczywiście dodatkowo utrudnia zdefiniowanie skali innowacyjności, która może być już tylko dziełem startupów.

---

[9] P.F. Drucker, *Classic Drucker. Klasyczne teksty Druckera z Harvard Business Review*, Wydawnictwo MT Biznes, Warszawa 2010, s. 109.

[10] W rozumieniu E. Riesa firma nowoczesna to taka, która „cechuje się dużą dyscypliną w rygorystycznym realizowaniu podstawowej działalności […] ale jednocześnie stosuje komplementarne zestawy narzędzi zarządzania przedsiębiorczego w celu radzenia sobie z sytuacjami nacechowanymi skrajną niepewnością” (E. Ries, *Droga startupu. Metoda sukcesu*, Wydawnictwo Helion, Gliwice 2018, s. 50).

[11] Według R. Kaplana i D. Nortona można wyróżnić cztery procesy innowacyjne w przedsiębiorstwie: identyfikację szans dla nowych produktów, badania i rozwój, projektowanie nowych produktów i ich wprowadzenie na rynek (R. S. Kaplan, D. P. Norton, *Mapy strategii w biznesie. Jak przełożyć wartości na mierzalne wyniki*, Wydawnictwo GWP, Sopot 2011, s. 161). W teorii procesy te mogą zachodzić zarówno w przedsiębiorstwach typu startup, jak i w klasycznych, tak więc dopiero ocena ich skali oraz praktycznej realizacji pozwala dokonać jednoznacznego rozróżnienia.

Jednak mimo tych trudności interpretacyjnych właściwe wydaje się stwierdzenie, że cechą definiującą większość przedsiębiorstw klasycznych jest działalność na bazie znanych i sprawdzonych mechanizmów rynkowych. Dotyczy to przykładowo klasycznych biznesów e-commerce, czyli sklepów internetowych sprzedających towary fizyczne[12]. Jeżeli pojawia się element innowacyjności, to ma on zwykle charakter dyferencjacji i sprowadza się do ulepszania istniejącej oferty, czyli jakości tego, co już jest rozpoznawalne przez użytkowników i klientów na rynku.

W przypadku startupów mówimy natomiast o poszukiwaniu nowej drogi, o chęci wprowadzenia nowej jakości na rynek i o testowaniu mechanizmów rynkowych w konfrontacji z „nową ofertą". Jest to niewątpliwie inny rodzaj innowacyjności, który nie będzie miał odniesienia do wszystkich branż i rodzajów działalności. W obszarze e-commerce będą to przede wszystkim przedsięwzięcia, które wykraczają poza standardowe rozumienie e-commerce, a więc np. usługi systemowe (serwisy internetowe)[13].

W tym miejscu warto podkreślić, że pojęcia „nowej oferty" nie należy utożsamiać z „unikalnością" w dosłownym znaczeniu tego słowa. Startupem nie będzie wyłącznie przedsiębiorstwo, które wykreowało zupełnie „nowy produkt". Startup to przedsięwzięcie oferujące konkretnej grupie odbiorców jakość, którą dana grupa odbiorców może odbierać jako innowacyjną, tj. odmienną od tego, z czym dotychczas miała do czynienia. „Unikalność" startupu będzie więc zawsze miała charakter subiektywny i ograniczony.

Kryterium użytkownika sieci

Konsekwencją różnic w obszarze innowacyjności jest inne pojmowanie użytkownika przez przedsiębiorstwa klasyczne i startupy. W obu przypadkach obowiązuje wprawdzie ten sam podział na użytkownika anonimowego (który odwiedza nasze strony), subskrybenta (który zapisał się do listy subskrypcyjnej), użytkownika zarejestrowanego (który założył konto użytkownika) i klienta (który dokonał zakupu), ale ocena wartości tego użytkownika jest zwykle odmienna.

[12] Według najnowszego raportu *E-commerce w Polsce 2021* do najczęściej kupowanych kategorii produktów w Polsce należą wciąż odzież i akcesoria – 71 proc., obuwie – 61 proc., kosmetyki i perfumy – 57 proc. (*E-commerce w Polsce 2021. Gemius dla e-Commerce Polska*, Gemius Polska 2021, s. 143). Sprzedaż realizowana jest przede wszystkim przez platformy sprzedażowe typu marketplace (np. Allegro) oraz indywidualne sklepy internetowe (np. Answear).

[13] Google, Facebook, Spotify, Netflix to przykłady nowoczesnych biznesów e-commerce, gdzie oferta ma charakter cyfrowy w postaci odpłatnie udostępnianej powierzchni reklamowej oraz odpłatnego odbioru treści audio lub wideo (streaming). Od strony technicznej są to szeroko pojęte serwisy internetowe oferujące usługi o charakterze systemowym, czyli wykonywane przez maszyny i algorytmy.

Dla klasycznych sklepów i serwisów internetowych działających w obszarze e-commerce użytkownik to przede wszystkim potencjalny klient, który może bezpośrednio uruchomić proces generowania przychodów kluczowy dla rentowności biznesu. Celem jest w miarę szybkie przekształcenie anonimowego użytkownika w płacącego klienta, czyli użytkownika, który dokonuje zakupu (najchętniej jako użytkownik zarejestrowany). Każdy użytkownik to szansa na sprzedaż jednego produktu lub jednej usługi. Dodatkowo przez oferowanie listy subskrypcyjnej, czyli newslettera, można zwiększyć szanse na pozyskanie klienta powracającego. To przykład schematu myślenia i działania typowego biznesu e-commerce, gdzie liczy się przede wszystkim sprzedaż bezpośrednia, czyli na rzecz klienta finalnego (przede wszystkim B2C).

Tabela 1 pokazuje znaczenie kategorii użytkownika sieci dla klasycznego przedsiębiorstwa e-commerce, jakim w dużym w stopniu wciąż pozostaje sklep internetowy Zalando. Wśród kluczowych wskaźników efektywności możemy odnaleźć liczbę odwiedzających stronę sklepu (przede wszystkim użytkownicy anonimowi) oraz liczbę aktywnych klientów, do których zalicza się użytkowników zarejestrowanych, którzy złożyli przynajmniej jedno zamówienie w okresie ostatnich 12 miesięcy. Dodatkowo marka wylicza korzyści płynące z liczby aktywnych klientów w odniesieniu do łącznego obrotu towarowego brutto oraz łącznej liczby zamówień. Mamy tutaj zatem przykład skutecznego przekształcenia użytkownika anonimowego w płacącego klienta, co stanowi potwierdzenie efektywności realizowanego modelu biznesowego.

Tabela 1. Kluczowe wskaźniki efektywności sklepu Zalando w latach 2020–2021

Kluczowe wskaźniki efektywności	2020	2021
Obrót towarowy brutto (w mln euro)	10 696,0	14 348,4
Liczba odwiedzających stronę (w mln)	5393,6	7461,3
Liczba aktywnych klientów (w mln)	38,7	48,5
Liczba zamówień (w mln)	185,5	252,2
Średni obrót towarowy brutto na jednego aktywnego klienta (w euro)	276,3	295,8
Średnia liczba zamówień na jednego aktywnego klienta	4,8	5,2

Źródło: opracowanie własne na podstawie raportu rocznego Zalando, https://corporate.zalando.com/en/investor-relations/key-figures-2021, dostęp: 6.07.2022 r.

W przypadku startupu nawet użytkownik anonimowy może mieć ogromną wartość, co zależy od etapu rozwoju przedsiębiorstwa, oferowanego produktu,

jak również sposobu generowania przychodów[14]. Bardzo często mamy do czynienia z tzw. sprzedażą pośrednią, gdzie użytkownik jest jedynie środkiem do celu. W praktyce oznacza to konieczność gromadzenia jak największej liczby użytkowników, przede wszystkim zarejestrowanych, aby ci w sposób pośredni przyczynili się do generowania przychodów lub innych korzyści. Tym samym użytkownik nie staje się bezpośrednio płacącym klientem, jak w przypadku przedsiębiorstwa klasycznego, lecz jest fundamentem stymulującym „sprzedaż" lub zwiększającym atrakcyjność biznesu. Przykładem mogą być tutaj startupy, których modelem biznesowym jest sprzedaż powierzchni reklamowej (np. Facebook) lub pośrednictwo pomiędzy „kupującymi" a „sprzedającymi" (np. Booking), oraz startupy poszukujące inwestorów do dalszego rozwoju (np. Brainly).

O ile zatem w klasycznych przedsiębiorstwach użytkownik ma przede wszystkim wartość jakościową, tj. każdy użytkownik może bezpośrednio dokonywać zakupów, o tyle dla startupów liczy się bardzo często liczba dostępnych użytkowników, gdyż za użytkownikami podążają realni klienci (np. reklamodawcy i inni partnerzy) lub inwestorzy.

Kryterium technologii

Wyższy poziom innowacyjności oraz nierzadko konieczność gromadzenia i utrzymania dużej liczby aktywnych użytkowników stanowią duże wyzwania technologiczne, którym sprostać muszą przede wszystkim przedsiębiorstwa typu startup. Współczesne usługi systemowe (np. reklama, pośrednictwo, streaming) bazują na niestandardowych rozwiązaniach, które wymagają zastosowania autorskiej infrastruktury technologicznej (stworzonej przez tzw. dewelopera). Należy pamiętać, że w przypadku wielu startupów działających na rynku e-commerce najważniejszym produktem jest sama technologia (serwis internetowy), która ma służyć gromadzeniu użytkowników. Narzędzie to powinno być zatem odpowiednio „innowacyjne", „przyjazne" i „unikalne" w odczuciu swojej grupy odbiorców. Zwykle wiąże się to z koniecznością wdrożenia zaawansowanej funkcjonalności, jak również wymaga wysokiej sprawności pod względem technologicznym, zwłaszcza jeśli przedsiębiorstwo celuje w obsługę bardzo dużej liczby aktywnych użytkowników. Nie da się tego osiągnąć standardowymi mechanizmami, do których zalicza się typowe rozwiązania sprzedaży e-commerce dostępne w modelu SaaS lub opensource[15].

[14] Szerzej na temat wskaźników efektywności w startupach: E. Ries, *Metoda Lean Startup*, *op.cit.*, s. 101–128.

[15] Do uruchomienia klasycznego sklepu lub serwisu internetowego wykorzystywane jest najczęściej gotowe oprogramowanie, które dostępne jest odpłatnie w modelu SaaS (software as as service) lub

W przeciwieństwie do startupów potrzeby technologiczne przedsiębiorstw klasycznych są raczej ograniczone w takim sensie, iż technologia nie stanowi głównej oferty, lecz jest jedynie narzędziem do realizacji sprzedaży. Nie ma więc potrzeby wdrażania autorskich rozwiązań, choć można ulepszać ogólnie dostępne rozwiązania, np. funkcjonalność w sklepie internetowym w ramach strategii dyferencjacji. Nie ma też potrzeby gromadzenia i utrzymania bardzo dużej liczby użytkowników, najczęściej więc korzysta się ze standardowych mechanizmów. Tej grupie przedsiębiorstw dedykowana jest szeroka oferta rozwiązań typu SaaS, które same mogą być przykładami startupów, oraz typu opensource.

Kryterium kapitału

Klasyczną sprzedaż e-commerce za pośrednictwem sklepu lub serwisu internetowego można uruchomić i utrzymać względnie niewielkim kosztem (wykluczając potrzebę finansowania szerokich działań marketingowo-promocyjnych)[16]. Potrzeby kapitałowe startupu zdefiniowanego na podstawie wcześniej omówionych kryteriów są natomiast wprost proporcjonalne do wymaganego poziomu innowacyjności oraz koniecznej liczby aktywnych użytkowników.

Przedsiębiorstwo typu startup nie wystartuje z reguły bez dużego kapitału na start i nie będzie w stanie się rozwijać bez stałego dofinansowania, co z reguły wiąże się z koniecznością pozyskania zewnętrznych inwestorów i przejścia przez kilka rund finansowania[17]. W przypadku klasycznego biznesu e-commerce zwykle natychmiast uruchamiana jest sprzedaż bezpośrednia, która ma służyć finansowaniu rozpoczętej działalności w sieci. I w tym przypadku mogą być wymagane większe nakłady finansowe, ale na zdecydowanie niższym poziomie.

Kryterium modelu biznesowego

Potrzeba pozyskania dużego kapitału do uruchomienia biznesu typu startup jest dodatkowo uwarunkowana kwestią dostępności modelu biznesowego. W przypadku przedsiębiorstw klasycznych, które od samego początku stawiają na bezpośrednią sprzedaż e-commerce, model biznesowy wynika z tego, co jest oferowane potencjalnym klientom. Sklep internetowy, który sprzedaje towary fizyczne, generuje więc przychody z każdym sprzedanym produktem. Biznes, który oferuje swoje

nieodpłatnie w modelu opensource (otwarty kod źródłowy). Szerzej o dostępnych rozwiązaniach technologicznych: *E-commerce manager – Profesjonalista w e-handlu. Tom I – Prawo, logistyka & technologia*, A. Zygadlewicz (red.), Fundacja Polak 2.0, Poznań 2014, s. 153–178.

[16] Koszty wdrożenia standardowego sklepu internetowego mogą wynieść w zależności od wielkości asortymentu od kilku do kilkunastu tysięcy złotych. *Ibidem*, s. 163.

[17] Szerzej na temat finansowania startupów: E. Ries, *Droga startupu. Metoda sukcesu*, *op.cit.*, s. 234–242.

specjalistyczne usługi, otrzymuje płatność za każdą wykonaną usługę. W teorii możliwe jest to od pierwszego momentu uruchomienia sprzedaży.

Startup cechuje się natomiast brakiem precyzyjnie zdefiniowanej ścieżki pozyskania przychodów, ponieważ – zgodnie z wcześniej przytoczonymi definicjami – oferuje „nowe produkty lub usługi w warunkach skrajnej niepewności" oraz „musi dopiero znaleźć powtarzalny i rentowny model biznesowy"[18]. Zakłada to oczywiście możliwość braku dostępności modelu biznesowego odpowiadającego potrzebom danego biznesu.

W praktyce wydaje się to jednak nie do końca słusznym założeniem. Modele biznesowe dostępne na rynku są w takim stopniu wykorzystywane przez przedsiębiorstwa klasyczne jak i „nowoczesne". Różnica sprowadza się do tego, jak wąsko lub jak szeroko definiuje się pojęcie modelu biznesowego. Klasyczne podejście bazuje na samym mechanizmie generowania przychodów (np. płatność za towar lub usługę), w szerszym ujęciu mechanizm wiąże się z innowacyjnością całego biznesu (np. płatność za towar spersonalizowany specjalnym kreatorem online)[19].

Poszukiwanie modelu biznesowego przez startupy należy rozumieć jako próby spieniężenia stworzonej oferty produktowej na tak dużą skalę, aby wcześniej czy później przekroczyć próg rentowności. Z pewnością czas wdrożenia właściwego modelu biznesowego jest wielokrotnie dłuższy niż w przypadku przedsiębiorstw klasycznych, startupy więc mogą być nierentowne nawet przez kilka lat od momentu rozpoczęcia swojej działalności.

Kryterium rentowności

Wyzwania związane z modelem biznesowym i generowaniem przychodów mają bezpośredni wpływ na wynik finansowy przedsiębiorstw typu startup, które cechuje swoista „sprzeczność finansowa". Z jednej strony istnieją ogromne potrzeby kapitałowe związane z koniecznością wdrożenia odpowiedniego poziomu innowacyjności (koszt rozwiązania technologicznego, koszt pozyskania i utrzymania dużej liczby aktywnych użytkowników), z drugiej strony niepewność modelu biznesowego sprawia, że brakuje gwarancji stałych przychodów przez dłuższy okres.

Luka istniejąca pomiędzy kosztami działalności a uzyskiwanymi przychodami wymaga regularnego dofinansowania zewnętrznego oraz powoduje, iż startupy mają o wiele mniejszy potencjał osiągnięcia względnie szybkiej rentowności. Inwestycja w tego typu przedsięwzięcia wiąże się zatem także z o wiele większym

[18] S. Blank, B. Dorf, *Podręcznik startupu…, op.cit.*, s. 16.

[19] Szerokie spojrzenie na model biznesowy pokazuje szablon modelu biznesowego opracowany przez Alexandra Osterwaldera: A. Osterwalder, Y. Pigneur, *Tworzenie modeli biznesowych. Podręcznik wizjonera*, Wydawnictwo Helion, Gliwice 2012.

ryzykiem inwestycyjnym, gdyż na wycenę startupu mniejszy wpływ ma „realna wartość tego, co zostało już stworzone", a większy „prawdopodobieństw[o] przyszłego sukcesu" oraz „skal[a] przyszłego sukcesu"[20].

O atrakcyjności przedsiębiorstw typu startup decyduje zatem perspektywa dużego sukcesu finansowego[21], wielokrotnie wyższego niż w przypadku biznesów klasycznych, które jednak względnie szybko mogą przekroczyć swój indywidualny próg rentowności.

Podsumowanie

Rozróżnienie pomiędzy startupami a przedsiębiorstwami klasycznymi w kontekście sprzedaży w sieci jest tematem złożonym i wymagającym uwzględnienia wielu czynników. Analiza kluczowych determinantów działalności na szeroko pojętym rynku e-commerce, w tym kwestii innowacyjności, użytkownika sieci, technologii, kapitału, modelu biznesowego oraz rentowności, pozwala na podjęcie próby zdefiniowania przedsiębiorstwa typu startup jako przeciwieństwa przedsiębiorstwa klasycznego.

Startupem w sieci będzie zatem w dużym stopniu przedsięwzięcie, którego celem jest wprowadzenie na rynek nowego produktu charakteryzującego się wysokim poziomem innowacyjności. Jego fundamentem będzie zastosowanie odpowiedniej technologii skierowanej do bardzo dużej liczby aktywnych użytkowników, których pozyskanie i utrzymanie wiąże się z dużymi nakładami finansowymi. Duża potrzeba kapitałowa przy jednoczesnym braku sprawdzonego modelu biznesowego i tym samym sposobu generowania stałych przychodów zmniejsza potencjał osiągnięcia szybkiej rentowności i wymusza poszukiwanie zewnętrznego dofinansowania.

W przeciwieństwie do startupu przedsiębiorstwo klasyczne opiera się natomiast na o wiele bardziej sprawdzonych mechanizmach rynkowych i od samego początku dąży do realizacji sprzedaży bezpośredniej produktów już znanych na rynku oraz uzyskania przychodu od każdego potencjalnego klienta, który tym samym jest fundamentem prostego modelu biznesowego służącego osiągnięciu szybszej rentowności. Innowacyjność jest elementem strategii dyferencjacji w ramach standardowych rozwiązań technologicznych, których wdrożenie i utrzymanie wiąże się z o wiele niższymi kosztami niż w przypadku startupu.

[20] E. Ries*, Droga startupu. Metoda sukcesu*, *op.cit.*, s. 85.

[21] Według E. Riesa „jednoprocentowa szansa na osiągnięcie w przyszłości wyceny rynkowej na poziomie 100 miliardów dolarów jest warta miliard dolarów". *Ibidem*, s. 85.

Bibliografia

Literatura

Blank S., Dorf B., *Podręcznik startupu. Budowa wielkiej firmy krok po kroku*, Wydawnictwo Helion, Gliwice 2013.

Chan Kim W., Mauborgne E., *Strategia błękitnego oceanu*, Wydawnictwo MT Biznes, Warszawa 2010.

Drucker P.F., *Classic Drucker. Klasyczne teksty Druckera z Harvard Business Review*, Wydawnictwo MT Biznes, Warszawa 2010.

E-commerce manager – Profesjonalista w e-handlu. Tom I – Prawo, logistyka & technologia, A. Zygadlewicz (red.), Fundacja Polak 2.0, Poznań 2014.

E-commerce w Polsce 2021. Gemius dla e-Commerce Polska, Gemius Polska 2021.

Kaplan R.S., Norton D.P., *Mapy strategii w biznesie. Jak przełożyć wartości na mierzalne wyniki*, Wydawnictwo GWP, Sopot 2011.

Osterwalder A., Pigneur Y., *Tworzenie modeli biznesowych. Podręcznik wizjonera*, Wydawnictwo Helion, Gliwice 2012.

Ries E., *Droga startupu. Metoda sukcesu*, Wydawnictwo Helion, Gliwice 2018.

Ries E., *Metoda Lean Startup*, Wydawnictwo Helion, Gliwice 2011.

Netografia

Https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0067&from=PL.

Https://digital-strategy.ec.europa.eu/en/news/24-eu-member-states-commit-digital-day-take-action-support-growth-eu-startups.

Https://2020.stateofeuropeantech.com/chapter/state-european-tech-2020/article/exec-sum/.

Https://corporate.zalando.com/en/investor-relations/key-figures-2021.

Streszczenie

Celem artykułu jest podjęcie próby określenia kluczowych cech rozróżniających przedsiębiorstwa typu startup od przedsiębiorstw klasycznych poprzez identyfikację oraz analizę kluczowych kryteriów determinujących działalność na szeroko pojętym rynku e-commerce, w tym kryterium innowacyjności, użytkownika sieci, technologii, kapitału, modelu biznesowego oraz rentowności. Rozważania dotyczą sprzedaży w sieci (e-commerce), przestrzeń ta stanowi bowiem naturalne miejsce rozwoju przedsięwzięć o charakterze innowacyjnym. Startupem w sieci będzie przedsięwzięcie, którego celem jest wprowadzenie na rynek nowego produktu o wysokim poziomem innowacyjności bazującym na zastosowaniu kapitałochłonnej technologii oraz niewielkiej szansy na szybką rentowność. Przedsiębiorstwo klasyczne bazuje natomiast na sprawdzonych i mniej innowacyjnych mechanizmach rynkowych oraz od samego początku dąży do wygenerowania przychodów gwarantujących osiągnięcie rentowności.

Summary

The purpose of this article is to try to identify the key characteristics that distinguish startup companies from classic ones by identifying and analyzing the key criteria that determine activity in the broader e-commerce market, including the criterion of innovation, user, technology, capital, business model and profitability. Consideration is given to online sales (e-commerce), as this space is a natural place for innovative ventures to grow. An online startup will be a venture that aims to launch a new product with a high level of innovation based on the use of capital-intensive technology and a small chance of quick profitability. A classic company, on the other hand, relies on proven and less innovative market mechanisms and from the very beginning seeks to generate revenues that guarantee profitability.

Słowa kluczowe

Startup, e-commerce, innowacyjność, model biznesowy, rentowność.

Keywords

Startup, e-commerce, innovation, business model, profitability.

Przemysław Jóskowiak – dr, Uniwersytet Warszawski.

Krzysztof Surdyk

OSINT W EPOCE WIELKICH ZBIORÓW DANYCH

Wstęp

Według Allena Dullesa, jednego z twórców amerykańskiej Centralnej Agencji Wywiadowczej (CIA), „w wywiadzie zagranicznym pozyskiwanie informacji przebiega na różne sposoby, nie wszystkie z nich są jednak tajemnicze czy sekretne”[1]. Odnosi się to zwłaszcza do wywiadu jawnego, w którym informacje pochodzą z gazet, książek, czasopism naukowych i technicznych, oficjalnych sprawozdań z obrad rządu czy z radia i telewizji. Nawet powieść lub przedstawienie może zawierać przydatne informacje, np. o stanie społeczeństwa. Działalność polegająca na zdobywaniu informacji ze źródeł jawnych i ogólnie dostępnych w polskiej literaturze często nazywana jest białym wywiadem. Metoda ta była i jest powszechnie znana i wykorzystywana na całym świecie, ale samo pojęcie białego wywiadu jest czysto polskim pomysłem. Za granicą (przede wszystkim na Zachodzie) zwykło się raczej używać amerykańskiego akronimu OSINT (ang. Open Source INTelligence), którego rozwinięcie można przetłumaczyć jako „wywiad ze źródeł otwartych” lub „wywiad jawno-źródłowy”.

Podstawą wszelkiego rejestrowania, udostępniania i wyszukiwania danych, niezależnie od ich rodzaju – od kodu komputerowego, po opowieści wojenne opowiadane przez dziadków i po publiczne zapisy księgowe – jest język. Nie inaczej jest w przypadku działań OSINT. Praktycy OSINT zbierają i oceniają treści generowane przez człowieka za pomocą języka opartego na otwartym kodzie źródłowym (języka naturalnego), a także wykorzystując ludzki język zakodowany za pomocą języków komputerowych do postaci zrozumiałej przez komputery.

Obecne środowisko OSINT wypełnione jest narzędziami, które pozwalają gromadzić i wybierać dane, a niektóre z nich pozwalają również na badanie uzyskanych danych. Wszystkie te narzędzia wykorzystują ten sam schemat funkcjono-

[1] A. Dulles, *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*, Guilford 2016. Cytowany fragment pochodzi z książki Bartosza Saramaka pt. *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Wydział Dziennikarstwa i Nauk Politycznych, Uniwersytet Warszawski, Warszawa 2015.

wania: za pomocą specjalnie sformatowanego języka zapytań ze strumieni danych wybierane i gromadzone są zapotrzebowane dane. Przykładem tego jest logika Boole'a[2], wykorzystująca do zapytania zestawy słów kluczowych. Nawet oparta na regułach RPA (zrobotyzowana automatyzacja procesów)[3] automatyzacja gromadzenia danych w swojej istocie opiera się na strukturze dopasowywania słów kluczowych. I chociaż ten system gromadzenia danych jest w większości skuteczny, to wyzwaniem ciągle pozostaje duża ilość tzw. fałszywych alarmów (niepoprawnie wybranych danych).

Rozwój technologii cyfrowych i pojawienie się w telekomunikacji wielu nowych rozwiązań i źródeł danych, przede wszystkim internetu, mediów społecznościowych, internetu rzeczy (Internet of Things, IoT), SCADA[4] czy bodynetu[5], doprowadziły do powstania ogromnych repozytoriów danych cyfrowych. Dane te są w większości powszechnie dostępne, ale żeby z nich skorzystać, trzeba umieć do nich dotrzeć i wybrać z oceanu danych te, które są niezbędne do przeprowadzenia analiz konkretnych rozwiązań, zdarzeń lub sytuacji. Ta swego rodzaju cyfrowa rewolucja doprowadziła do ogromnego wzrostu znaczenia OSINT jako rodzaju działań wywiadowczych, który oczywiście korzysta ze źródeł otwartych, ale nie ogranicza się do prostego przeglądania internetu i czytania wiadomości, a stosuje nowe technologie gromadzenia i analizy danych.

Prezentowany artykuł poświęcono metodom prowadzenia wywiadu ze źródeł otwartych (OSINT), w przypadku gdy gromadzone, weryfikowane i analizowane są dane ustrukturyzowane[6], nieustrukturyzowane[7] bądź częściowo ustrukturyzo-

[2] Logika boolowska – oparta na założeniu, że świat można opisać za pomocą zdań, którym przypisywana jest jedna z dwóch wartości: PRAWDA (T) lub FAŁSZ (F).

[3] Zrobotyzowana automatyzacja procesów (ang. Robotic Process Automation) – technologia automatyzacji powtarzalnych procesów biznesowych z wykorzystaniem programów komputerowych – robotów symulujących pracę człowieka. Zrobotyzowana automatyzacja procesów znajduje zastosowanie w gospodarce, wykonując zadania powierzane wcześniej konkretnym pracownikom.

[4] SCADA (ang. Supervisory Control and Data Acquisition) – system informatyczny nadzorujący przebieg procesu technologicznego lub produkcyjnego. Jego główne funkcje obejmują zbieranie aktualnych danych (pomiarów), ich wizualizację, sterowanie procesem, alarmowanie oraz archiwizację danych.

[5] Bodynet (ang. sieć ciała) – sieć okolic ciała, zwana także bezprzewodową siecią okolic ciała lub siecią czujników ciała lub medyczną siecią okolic ciała, jest bezprzewodową siecią noszonych urządzeń komputerowych.

[6] Dane ustrukturyzowane – dane generowane w systemie zarządzania relacyjnymi bazami danych (ang. Relational Database Management System, RDBMS). Do danych ustrukturyzowanych zaliczamy m.in. transakcje sprzedaży, rejestrację aktywności bankomatu, rezerwacje lotów czy zbiory nazwisk i numerów telefonów.

[7] Dane nieustrukturyzowane to zawartość pola tekstowego w wiadomościach mailowych, zawartość platform społecznościowych, pliki obrazów oraz wideo, dane z czujników i wszystkie inne dane złożone. Te rodzaje danych mogą być generowane zarówno przez ludzi, jak i maszyny.

wane[8], pochodzące z tzw. wielkich zbiorów danych (big data[9]). W artykule zwrócono uwagę na wzrost potencjału OSINT w epoce wielkich zbiorów danych, ale także na wiele nowych wyzwań, jakie big data przyniosły wywiadowi ze źródeł otwartych, głównie z powodu dużych ilości nieustrukturyzowanych, generowanych w sposób ciągły danych.

Otwarte źródła informacji i wywiad z otwartych źródeł – pojęcia podstawowe

W polskim ustawodawstwie na próżno szukać definicji białego wywiadu lub wywiadu z otwartych źródeł informacji. Określenie pojęcia „Open Source Intelligence" (OSINT) znaleźć można natomiast w dokumencie NATO Open Source Intelligence Reader z 2002 roku: „OSINT to wynik przeprowadzenia pewnych czynności w stosunku do informacji. Są one specjalnie poszukiwane, porównywane ze sobą co do treści i spośród nich wybierane są te najważniejsze dla odbiorcy procesu". Do otwartych źródeł informacji należą m.in.:

- życie publiczne, wypowiedzi przedstawicieli państwa;
- internet, w tym serwisy społecznościowe Facebook, YouTube i inne, czyli tzw. środki nowej komunikacji otwartej;
- sondy społeczne, prasa (szczególnie lokalna oraz specjalistyczna), radio, telewizja i inne środki masowego przekazu, materiały konferencyjne;
- dokumentacja, jaką przedsiębiorstwa lub instytucje państwa muszą udostępnić według wymagań prawa, ogólnie dostępne rejestry, sądowe ogłoszenia upadłości i postanowienia o postępowaniu układowym;
- wydawnictwa marketingowe: biuletyny, informatory, reklamy, a także analizy produktów (inżynieria odwrotna) itp.

W literaturze można spotkać się z dwoma zasadniczymi pojęciami dotyczącymi otwartych źródeł informacji – Open Source Data (OSD) i Open Source Information (OSIF) – oraz z dwoma pojęciami dotyczącymi zdobywania informacji ze źródeł otwartych – Open Source Intelligence (OSINT) i Validated OSINT (OSINT-V). OSD to wszystkie nieobjęte klauzulą niejawności dane w stanie „surowym", przedstawione w najprostszej formie, pochodzące od pierwotnego źródła, w postaci drukowanej, z mediów, stron internetowych, zdjęć satelitarnych, fotografii itp. OSIF to dane, które zostały poddane analizie, zgrupowane w jednym dokumencie, a następ-

[8] Dane częściowo ustrukturyzowane – ich doskonałym przykładem są e-maile. Zawierają one zarówno informacje ustrukturyzowane (takie jak nazwa odbiorcy i nadawcy), jak i nieustrukturyzowane (wiadomość tekstowa w mailu jest plikiem tekstowym, który stanowi dane nieustrukturyzowane).

[9] Big data – termin odnoszący się do dużych, zmiennych i różnorodnych zbiorów danych, których przetwarzanie i analiza są trudne, ale jednocześnie wartościowe, ponieważ mogą prowadzić do zdobycia nowej wiedzy.

nie przekazane osobom zarządzającym celem rozpowszechnienia. OSINT to etap (poziom), w którym realizowane jest zaplanowane uzyskanie informacji, a dane zostają przekazane jedynie wybranym osobom zgodnie z zasadami określonymi przez składającego zapytanie. W tym miejscu mowa jest właśnie o klasycznym znaczeniu pojęcia OSINT. Na etapie (poziomie) OSINT-V następuje weryfikacja informacji, którym można przypisać wysoki poziom pewności, zostają one bowiem potwierdzone z różnych innych źródeł, w większości przypadków jawnych, ale niekiedy także tajnych.

Warto dodać, że choć informacje zdobywane z otwartych źródeł informacji są jawne, działania i operacje zmierzające do pozyskania tych informacji mogą nie mieć charakteru jawnego, szczególnie wtedy, kiedy prowadzone są przez państwowe agencje wywiadowcze.

Według wspomnianego już Allena Dullesa: „Właściwa analiza danych wywiadowczych, które można uzyskać za pomocą jawnych, normalnych i otwartych źródeł informacji, powinna zapewnić ponad 80 proc. informacji niezbędnych do kierowania polityką krajową". Jednocześnie Dulles podkreślał, że „ze względu na pewien urok i tajemniczość, nadmierny nacisk położony jest na to, co nazywa się wywiadem tajnym"[10], „podczas gdy większość zbierania i przetwarzania danych wywiadowczych odbywa się zwykle za pomocą normalnych metod", do których zaliczał bezpośrednią interakcję dyplomatyczną, relacje osobiste, a także radio, prasę i diasporę za granicą.

Taką samą regułę 80 proc. można znaleźć w dokumentach NATO[11] i w pracy Arthura Hulnicka[12] z 2004 roku, chociaż dla Europolu (Agencji Unii Europejskiej ds. Współpracy Organów Ścigania), dla ministerstw obrony Wielkiej Brytanii, Szwecji i Holandii, a także dla amerykańskiej Agencji Wywiadu Obronnego (DIA) wywiad ze źródeł otwartych OSINT stanowi „co najmniej 90 proc." wszystkich danych uzyskiwanych w wyniku działań wywiadowczych[13]. Oznacza to, że przeważająca część działań wywiadowczych koncentruje się na gromadzeniu danych ze źródeł otwartych i odnajdywaniu powiązań i niuansów występujących między nimi, a nie na wykorzystywaniu popularnej i nieco mistycznej praktyce wywiadu (szpiegostwa) osobowego, czyli HUMINT[14].

---

[10] R. Dover, M. Goodman, C. Hillebrand, *Routledge Companion to Intelligence Studies*, Routledge 2015, s. 125.

[11] *NATO Open Source Intelligence Reader*, 2002, https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf.

[12] A.S. Hulnick, *Keeping Us Safe: Secret Intelligence and Homeland Security*, Praeger Publishers, Westport, CT, 2004.

[13] *The Oxford Handbook of National Security Intelligence*, L.K. Johnson (red.), Oxford University Press 2012.

[14] A. Ünver, *Digital Open Source Intelligence and International Security: A Primer*, http://edam.org.tr/en/digital-open-source-intelligence-and-international-security-a-primer/, dostęp: 17.07.2018 r.

Właściwe wykorzystanie OSINT określa podstawy i wzajemne zależności między funkcjami realizowanymi przez agencje wywiadowcze i zapewnia tym agencjom dwie kluczowe korzyści.

Pierwszą z nich jest określenie sytuacji politycznej, wojskowej, gospodarczej, w jakiej przychodzi działać wywiadom. W tym wypadku za pomocą OSINT można ustalić spektrum wydarzeń, aktorów sceny politycznej i ich role, które określają tzw. względność strategiczną. Chodzi o to, jak zdefiniować interesy kraju w odniesieniu do trwających wydarzeń, a także jakie aktywa należy uruchomić, aby zabezpieczyć te interesy. Bez zrozumienia wydarzeń na świecie, mechanizmów przyczynowych między zachodzącymi procesami i wyraźnymi interesami głównych aktorów sceny politycznej agencje wywiadowcze mogą rozwiązywać problemy jedynie w sposób reaktywny, nie mając możliwości powstrzymania określonych procesów lub możliwości zarządzania nimi, zanim dotrą do granic kraju lub co gorsza, zanim przenikną na jego obszar.

Po drugie, OSINT pozytywnie wpływa na wydajność stosowania innych metod wywiadowczych, pozwalając agencjom na wcześniejsze, dokładne ustalenie, jakie informacje są dostępne ze źródeł otwartych, a jakie wymagają zastosowania specjalnych metod ich pozyskania. Dzięki temu agencje mogą oszczędniej korzystać z innych funkcji i metod wywiadowczych, co ma znaczenie szczególnie w przypadku konieczności stosowania bardziej agresywnych mechanizmów zdobywania informacji, takich jak wywiad osobowy czy kradzież tajnych materiałów. W ten sposób wywiady zmniejszają prawdopodobieństwo pomyłek w swoich kalkulacjach podczas przygotowywania operacji wywiadowczych, unikają także zbędnej eskalacji napięć z innym krajem w razie ewentualnej dekonspiracji swoich działań wywiadowczych. Wykorzystanie OSINT zmniejsza również koszty zdobywania danych za pomocą innych metod wywiadowczych, eliminując jednocześnie wiele domysłów[15].

OSINT w warunkach rewolucji cyfrowej

Eksplozja technologii informacyjnych sprawiła, że życie z OSINT stało się łatwiejsze i trudniejsze zarazem; łatwiejsze ze względu na szeroki dostęp do informacji w wielu kanałach telekomunikacyjnych, trudniejsze ze względu na równie szerokie rozprzestrzenianie się informacji śmieciowych lub wprowadzających w błąd. Poważnym problemem stała się skuteczność weryfikacji treści uzyskiwanych danych. To sprawia, że w ramach OSINT musi być realizowane nie tylko zbieranie i przetwarzanie danych cyfrowych, ale także rozwijanie mechanizmów

[15] R. Dover, M. Goodman, C. Hillebrand, *Routledge Companion*…, *op.cit*., s. 14.

ich weryfikacji i atrybucji[16] oraz rozumienie, co stanowi zawartość śmieciową, a co nie.

Dla oceny, które informacje cyfrowe lub jaki typ danych są ważne z wywiadowczego punktu widzenia, służby wywiadowcze potrzebują infrastruktury technicznej i wysokiej jakości specjalistów (lub odpowiedniego outsourcingu[17]), aby zrozumieć internet i jego stale zmieniające się wzorce rozpowszechniania i przechowywania danych. W tym celu większość agencji wywiadowczych wykorzystujących OSINT zaczęła tworzyć oddzielne struktury zajmujące się badaniem internetu[18]. Poza tym wywiady, które zawsze konkurowały ze sobą w zdobywaniu informacji, teraz muszą konkurować nie tylko ze sobą, ale ze względu na szeroką społeczną dostępność źródeł internetowych również z indywidualnymi analitykami i analitykami prywatnych firm, wykorzystującymi narzędzia OSINT.

Te dwie nowe, „wschodzące" kategorie uczestników działań wywiadowczych – analitycy indywidualni i analitycy prywatnych firm – nie są związane z biurokratycznymi i formalnymi ograniczeniami, jakim podlegają agencje wywiadowcze, a zatem mogą szybciej dostosowywać się do technicznych zmian zachodzących w technikach OSINT. Prywatni analitycy mogą z własnej inicjatywy tworzyć lub przejmować nowe techniki gromadzenia, przechowywania i analizy danych cyfrowych, co w przypadku agencji wywiadowczych wymaga legitymizacji prawnej.

Od zwalczania terroryzmu po cyberbezpieczeństwo, od monitorowania broni masowego rażenia po analizę protestów – w przypadku OSINT firmy technologiczne i tzw. cywile wykorzystują te same typy danych i informacji co większość państwowych służb wywiadowczych. I chociaż analitycy niepaństwowi nie dysponują takimi środkami finansowymi jak wywiady państwowe, w pełni nadrabiają ten brak autonomicznym i szybkim działaniem, a także zdolnością do improwizacji.

Oprócz wymienionych do nowych aspektów, które należy uwzględnić we współczesnym OSINT, należy kwestia wielkich zbiorów danych. Rewolucja big data przyniosła nowości, takie jak: nowe technologie przechowywania i transmisji danych, dostępność sieci danych 3G/4G i 5G, a także masowy dostęp do Wi-Fi i technologii chmury, dzięki którym jesteśmy teraz w stanie tworzyć, przechowywać i udostępniać bezprecedensowe ilości informacji. Technologie te sprawiają,

[16] Atrybucja – przypisywanie komuś lub czemuś pewnych cech. W psychologii pojęcie atrybucji odnosi się do tego, jak ludzie wyjaśniają przyczyny swojego bądź cudzego zachowania, tzw. naiwne teorie przyczynowości. Termin ten funkcjonuje również w gramatyce języka polskiego oraz w dziedzinie marketingu biznesowego.

[17] Outsourcing (z ang. *outside resource using*) – wydzielenie ze struktury organizacyjnej przedsiębiorstwa niektórych realizowanych przez nie samodzielnie funkcji i przekazanie ich do wykonania innym podmiotom.

[18] E.J. Appel, *Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence*, Second Edition, CRC Press 2014, s. 157.

że wytwarzanie, przechowywanie lub przesyłanie pojedynczej jednostki danych (bajtu) staje się coraz tańsze. Umożliwia także wytwarzanie i gromadzenie danych społecznych (zwłaszcza danych osobowych) o wysokim stopniu szczegółowości. Ostatecznie nasze dane osobowe, dane dotyczące naszej aktywności, zachowań, poglądów itp. służą nie tylko celom administracyjnym lub statystycznym, dla których zostały utworzone, ale również celom reklamowym, a nawet przestępczym. Na przykład dane podatkowe lub dane dotyczące zatrudnienia mogą być wykorzystywane do profilowania naszych zachowań zakupowych, opcji opieki zdrowotnej, wyboru miejsca zamieszkania, zachowań wyborczych.

Różnego rodzaju dane dotyczące konkretnych osób lub grup społecznych uzupełniane są dzięki naszym cyfrowym zachowaniom w internecie. Do ich uszczegółowienia przyczyniają się m.in.: posiadanie znajomych na Facebooku, polubienia, retweety na Twitterze, posty na Instagramie, przesyłanie zdjęć z lokalizacją geograficzną i filmów Snapchat[19]. Wszystko to pozwala zarówno państwowym, jak i prywatnym analitykom OSINT na dostęp do ogromnej, stale rosnącej i niezwykle szczegółowej puli informacji behawioralnych[20] milionów ludzi.

Wreszcie, biorąc pod uwagę ogromne ilości danych pochodzących z internetu rzeczy, od zegarków fitness po urządzenia domowe, można zauważyć, że ta największa w historii pula danych społecznych i osobowych staje się nie tylko ogromna, ale również wystarczająco szczegółowa, aby z dużą rozdzielczością profilować całe społeczeństwa i narody. Dla każdego analityka – państwowego lub prywatnego – zajmującego się takimi kwestiami, jak: moralność, interesy polityczne poszczególnych ugrupowań, preferencje wyborcze, potencjał sił społeczno-politycznych w społeczeństwie przeciwnika, dysponowanie takimi danymi jest historycznym zwrotem w zdolnościach wywiadowczych[21].

Kadry i narzędzia dla cyfrowego OSINT

Nie wszystkie państwa mogą skutecznie uzyskiwać i wykorzystywać wymienione dane. Aby mogły zostać one przetworzone w cenną informację wywiadowczą,

[19] Snapchat to bezpłatna aplikacja na Androida lub iOS-a, służąca do wymiany snapów – zdjęć lub filmików, które mogą być wzbogacone filtrem, napisem, naklejką lub elementem animacji dostosowującym się do twarzy. Główną cechą Snapchata jest znikanie publikowanych treści po 10 sekundach od odebrania przez adresata. Trzeba jednak pamiętać, że każde zdjęcie czy film mogą zostać zapisane na telefonie odbiorcy, a następnie podane dalej.

[20] Behawioralny (z ang. *behavior* lub *behaviour* – zachowanie) – oznacza każdą dającą się zaobserwować reakcję człowieka lub zwierzęcia na bodźce płynące z otoczenia. Podłożem terminu „behawioralny" jest XX-wieczny nurt naukowo-filozoficzny zwany behawioryzmem. Według niego zachowanie rozumiane jest jako zespół fizycznych reakcji organizmu na bodźce zewnętrzne. Są to właśnie reakcje behawioralne.

[21] A. Ünver, *Digital Open Source…*, *op.cit*.

służby wywiadowcze muszą mieć odpowiedni potencjał kadrowy o różnorodnym zestawie kompetencji, a także narzędzia informatyczne i analityczne, za których rozwojem państwa zwykle nie nadążają.

Pierwszym z wielu problemów państwowych agencji wywiadowczych jest kwestia przyciągania młodych talentów. Agencje te bardzo często przegrywają z takimi firmami technologicznymi, jak Facebook, Google czy Amazon, zapewniającymi swoim pracownikom znaczną swobodę, niezależność i lepsze płace. Dlatego większość wysoko wykwalifikowanych analityków danych odwraca się od służby państwowej. Powoduje to przesunięcie środka ciężkości potencjału wywiadu cyfrowego, wykorzystującego otwarte źródła informacji, z organów państwowych na firmy prywatne.

Drugim problemem jest kwestia rozwoju, adaptacji i modernizacji infrastruktury wywiadu cyfrowego, która dla silnie zbiurokratyzowanej struktury wywiadów państwowych jest problematyczna. Nowy sprzęt jest drogi, a inteligentne rozwiązania, takie jak recykling technologiczny (regeneracja starego sprzętu po niższych kosztach) lub usprawnienia modernizacyjne, wymagają mniej rozbudowanego i sprawniejszego systemu podejmowania decyzji[22].

Po trzecie, rosnąca cywilizacja OSINT stworzyła informację jako ruch oporu, w którym tzw. aktywizm cyfrowy[23] implikuje proces ujawniania i rozpowszechniania danych o złym zarządzaniu państwem, korupcji i represji. Kultura cyfrowego ruchu oporu zakłada konieczność lepszej ochrony tożsamości cyfrowej, szczególnie po ujawnieniu nadużyć nadzoru państwowego w tym zakresie, po rewelacjach Snowdena, wyciekach Wikileaks i Chelsea Manning. I chociaż państwa teoretycznie mogą korzystać z tej „cywilnej" puli OSINT, kultura i tożsamość obecnej społeczności internetowej ma dzisiaj w większości charakter antypaństwowy.

Państwa mogą zarówno korzystać z OSINT, jak i ponosić określone straty w wyniku jego stosowania. Władze państwowe często starają się wykorzystać OSINT realizowany przez własne służby wywiadowcze nie tylko w rozgrywce z innymi państwami, a także w walce politycznej z własną opozycją. Jednakże wywiad ze źródeł otwartych jest z natury mieczem obosiecznym i władze muszą liczyć się z tym, że OSINT może być doskonałym narzędziem dla ujawnienia ich niekompetencji, biurokracji i korupcji. Poza tym, o ile wycieki danych pojedyn-

[22] S. Tongur, M. Engwall, *The Business Model Dilemma of Technology Shifts*, „Technovation" 2014, vol. 34, nr 9, s. 525–535, https://doi.org/10.1016/j.technovation.2014.02.006.

[23] Aktywizm cyfrowy, cyberaktywizm (ang. *digital activism, cyberactivism*) jest ruchem ludzi na całym świecie, którzy za pomocą internetu i telefonów komórkowych chcą wpływać na rzeczywistość społeczną i polityczną. Obrazowo można go opisać jako zbiór małych elementów, które są ze sobą luźno połączone, ale w określonym celu potrafią się szybko zorganizować, aby po jego osiągnięciu znów się rozproszyć. Aktywizm cyfrowy to zagadnienie, które nie zostało jeszcze zbyt dobrze zbadane. Wstępną próbę scharakteryzowania tego ruchu podjęli autorzy raportu *Digital Activism Survey Report 2009*, https://www.othersidegroup.com/2009/07/digital-activism-survey-results/.

czych osób (dane wyborców, szczegóły opieki zdrowotnej, historii zakupów itp.) szkodzą tym jednostkom, to wycieki danych na poziomie państwowym bardziej szkodzą rządom i ich agencjom wywiadowczym ze względu na niejawny charakter większości wycieków.

Przykłady wykorzystania OSINT w wielkich zbiorach danych

Coraz więcej informacji przechowywanych jest w postaci cyfrowej. Postać taką przyjmują: wiadomości, blogi, dane z sieci społecznościowych, muzyka, filmy, książki, artykuły naukowe. Digitalizowane są analogowe dotychczas ogromne zbiory książkowe, w tym najsłynniejsze biblioteki. Przeszukiwanie tych zbiorów za pomocą współczesnych narzędzi OSINT jest możliwe dzięki zastosowaniu tzw. słów kluczowych, pod warunkiem jednak, że uwzględnione zostaną takie ich cechy charakterystyczne, jak: brak hierarchii tematycznej, brak możliwości skupienia się na konkretnej tematyce, a także brak możliwości analizowania powiązań między dokumentami[24].

Chociaż narzędzia OSINT szybko ewoluują, najpopularniejsze metody pozyskiwania danych wywiadowczych w ogólnodostępnych zbiorach cyfrowych można podzielić na cztery główne kategorie:

1) metody językowe i tekstowe;
2) metody wykorzystujące systemy informacji geograficznej (GIS) – teledetekcję;
3) metody oparte na teorii sieci;
4) metody wykorzystujące kryminalistykę wizualną.

Metody językowe i tekstowe (oparte na tekście)

Metody językowe i tekstowe OSINT ściśle wiążą się z maszynowym przetwarzaniem języka naturalnego. Językami naturalnymi określamy języki (np. język polski, angielski, francuski) służące do komunikacji interpersonalnej. W przeciwieństwie do języków formalnych[25] (języków programowania) języki naturalne nie zostały stworzone przez człowieka, tylko ewoluowały w sposób naturalny i charakteryzują się niejednoznacznością. Język formalny natomiast to język zrozumiały przez komputer w sposób dosłowny, zwięzły oraz pozbawiony dwuznaczności. Prawdziwym wyzwaniem dla językoznawców i badaczy AI (sztucznej inteligencji) jest przetwarzanie języka naturalnego[26].

[24] D. Brzeziński, *Top modeling*, http://www.cs.put.poznan.pl/alabijak/emd/11_Topic_modeling.pdf.

[25] Język sztuczny (formalny) to ściśle określony system znaków wraz z regułami postępowania z tymi symbolami, a także regułami ich interpretowania.

[26] Przetwarzanie języka naturalnego (ang. Natural Language Processing, NLP) – interdyscyplinarna dziedzina, łącząca zagadnienia sztucznej inteligencji i językoznawstwa, zajmująca się automatyzacją analizy, rozumienia, tłumaczenia i generowania języka naturalnego przez komputer. System

W latach 50. XX wieku Alan Turing próbował znaleźć odpowiedź na pytanie, czym jest myślenie. Zaprojektował słynny test Turinga, którego celem było sprawdzenie, czy podczas rozmowy tekstowej maszyna zdoła oszukać osobę prowadzącą z nią konwersację, imitując zdolności komunikacyjne człowieka. Umiejętności interpretacji i generowania języka naturalnego, prowadzące do oszukania człowieka, który nie zauważa, że nie rozmawia z żywą osobą, miałyby, według Turinga, świadczyć o inteligencji maszyny.

Współczesny wywiad ze źródeł otwartych, chcąc nie chcąc, zmuszony jest wykorzystywać do organizowania, wyjaśniania, analizy w czasie, przeszukiwania i streszczania dużych zbiorów danych modele tematyczne OSINT zapisane w języku formalnym, takie jak: korpusy tekstowe[27], zbiory czasopism i dokumentów, zbiory obrazów, muzyki, sieci społecznościowych, a także transakcje, przebiegi czasowe, dane genetyczne. Wymaga to dostosowania zapytań OSINT do komputerowych baz danych. Dostosowanie to realizuje się za pomocą modelu, który

generujący język naturalny przekształca informacje zapisane w bazie danych komputera na język łatwy do odczytania i zrozumienia przez człowieka. System rozumiejący język naturalny przekształca próbki języka naturalnego na bardziej formalne symbole, łatwiejsze do przetworzenia dla programów komputerowych. Wiele problemów NLP wiąże się zarówno z generacją, jak i rozumieniem języka, np. model morfologiczny zdania (struktura słów), który komputer powinien zbudować, jest potrzebny zarazem do tego, by zdanie było zrozumiałe i gramatycznie poprawne.

[27] Korpus tekstowy (ang. *text corpus*) (z łac. *corpus* – ciało) – zbiór tekstów służący badaniom lingwistycznym, np. określaniu częstości występowania form wyrazowych, konstrukcji składniowych, kontekstów, w jakich pojawiają się wyrazy. Jest zwykle główną pulą danych dla tekstowych metod OSINT, stanowi zbiór słów i słów kluczowych, na podstawie których dokonywane są analizy statystyczne. Korpusy językowe znalazły szerokie zastosowanie we współczesnej leksykografii. Są też wykorzystywane jako zbiory danych uczących i testowych w metodach uczenia maszynowego stosowanych w przetwarzaniu języków naturalnych. Aby korpusy były bardziej przydatne do prowadzenia badań językowych, często poddaje się je procesowi zwanemu adnotacją. Przykładem adnotacji w korpusie tekstowym jest tagowanie lub tagowanie POS, w którym informacje o części mowy każdego słowa (czasownik, rzeczownik, przymiotnik itp.) są dodawane do korpusu w postaci tagów.

Adnotacja – współczesne duże korpusy dają użytkownikowi wiele możliwości analizy danych, a także ją ułatwiają dzięki temu, że teksty są adnotowane, co oznacza, że zgromadzone w nich dane językowe są wzbogacone o dodatkowe informacje dotyczące np. źródła danych, struktury tekstu oraz czasu i okoliczności powstania tekstu czy cech gramatycznych. Dzięki temu można zadawać znacznie precyzyjniejsze pytania (np. jakie rzeczowniki występują z danym wyrazem w kolokacjach), a oprogramowanie, które działa, kiedy używa się NKJP (Narodowego Korpusu Języka Polskiego) z poziomu strony internetowej, umożliwia wykonywanie półautomatycznych analiz.

Tagowanie (ang. *tagging* – oznaczanie, zakładkowanie) – metoda oznaczania i umieszczania referencji do bloków danych. Pozwala na odwoływanie się do nich według pewnej ich cechy, np. tagowanie poszczególnych części mowy w pliku tekstowym.

Tagowanie POS – tagowanie części mowy (ang. *part-of-speech*, *POS-tagging*), obliczeniowe metody oznaczania wyrazów częściami mowy (rzeczownik, czasownik, itd.).

Zob. T. Piotrowski, Ł. Grabowski, *Interpretacja danych frekwencyjnych z korpusów językowych: opis pewnych problemów (na kilku przykładach z życia wziętych)*, https://repo.uni.opole.pl/, dostęp: 09.05.2022 r.

traktuje dane jako obserwacje procesu probabilistycznego z ukrytymi zmiennymi (tematami).

Jedną z najstarszych praktyk OSINT jest analiza języka i sentymentu[28]. Wnioskowanie o psychologii przywództwa, intencjach polityki i spójności organizacyjnej przez badanie mowy i pisma jest podstawową praktyką historycznych wersji OSINT, umożliwiającą np. dyplomatom syntezę zdobywanych przez nich danych. Rzeczywiście, w okresie zimnej wojny wycinki z gazet z oświadczeniami przywódców, wycinki z czasopism naukowych były powszechnym, otwartym źródłem informacji wykorzystywanym w krajach po obu stronach trwającego wówczas konfliktu. Należy jednak zauważyć, że już od czasów I wojny światowej w środowiskach wywiadowczych popularność zaczęły zyskiwać językoznawstwo, antropologia, a także badanie danych przestrzennych, czego dowodem było utworzenie w tamtym czasie wyspecjalizowanych wydziałów na najlepszych uniwersytetach, kształcących specjalistów w tych specjalnościach[29].

W latach 60. XX wieku lingwistyka ilościowa stała się dziedziną popularną w wywiadzie ze źródeł otwartych, ale dopiero digitalizacja tekstów i popularyzacja metod tekstowych, jako źródeł danych w naukach społecznych, wywarły bezpośredni wpływ na rozwój lingwistycznej analizy OSINT. Masowa digitalizacja i standaryzacja plików tekstowych za pomocą komputerowych procesorów tekstu przyczyniły się do znaczących postępów w zbieraniu danych typu *open source*, takich jak kategoryzacja tekstu, grupowanie tekstu, wyodrębnianie jednostek i podsumowanie obliczeniowe.

Dzięki masowej digitalizacji literatury narodowe archiwa historyczne, teksty polityczne i pamiętniki zostały przekształcone do postaci cyfrowej, zapewniając językoznawcom i analitykom treści (dyskursu) niespotykany dotąd rozmiar danych i narzędzia do ich szybkiego przetwarzania. Narzędzia te okazały się szczególnie cenne w przypadku internetowej eksploracji tekstów umieszczanych na stronach internetowych, blogach i postach w mediach społecznościowych. Okazuje się, że obecnie przytłaczającą większość interakcji tekstowych na świecie można przeszukiwać, posortować i zmierzyć – niektóre z nich w czasie rzeczywistym.

Chociaż tekstowy OSINT można realizować za pomocą standardowego oprogramowania, takiego jak Python, R, MatLab i Ruby, to istnieją również tekstowe aplikacje opracowane specjalnie dla OSINT. Niektóre z nich, takie jak popularne WordStat, RapidMiner, KHCoder i NVivo, pozwalają użytkownikom wykrywać i wizualizować połączenia, wzorce i motywy działania w dużych ilościach tekstu.

[28] Sentyment to wydźwięk emocjonalny wypowiedzi. Analiza sentymentu, znana również jako AI emocji lub *opinion mining*, to mechanizm analizy tekstów online, gdzie oceniany jest ton emocjonalny, który teksty te niosą niezależnie od tego, czy są o zabarwieniu pozytywnym, negatywnym czy neutralnym.

[29] *The Oxford Handbook…*, *op.cit.*, s. 144.

Ponadto aplikacje do przetwarzania języka naturalnego oparte na statystycznym modelowaniu tematów, takie jak Latent Semantic Analysis/Indexing (LSA/I)[30] lub Latent Dirichlet Allocation (LDA)[31], ułatwiają katalogowanie, sortowanie i przetwarzanie dużych ilości danych tekstowych z mediów społecznościowych, umożliwiając analitykom OSINT wykrywanie wzorców zachowań i analizę sentymentu. Co więcej, wspomniana aplikacja do rozpoznawania i ekstrakcji jednostek (LSA/I) znacznie ułatwia katalogowanie, sortowanie i przetwarzanie dużych ilości danych tekstowych pochodzących z mediów społecznościowych, w celu przeprowadzenia ich analizy retrospektywnej lub w czasie rzeczywistym.

Kilka obiecujących zastosowań OSINT obejmuje również przewidywanie (wykrywanie) behawioralne. Problematyce tej poświęcone są m.in. praca Asghara (i innych) nad wykrywaniem wzorców zachowań pozwalających zmierzyć poziom radykalizacji w filmach z komentarzami zamieszczanymi na YouTube[32], a także przełomowa praca Hsinchun Chena na temat eksploracji tekstu w Dark Web[33], pozwalającej na wykrycie siatek ekstremistycznych funkcjonujących wewnątrz „ciemnej sieci".

Singh i inni poszli o krok dalej i zajęli się tweetami indyjskich dyplomatów, aby przeanalizować wzajemne relacje pomiędzy indyjską służbą zagraniczną a przywódcą kraju Narendrą Modim, dając jasny obraz indyjskiego kapitału dyplomatycznego i wsparcia dyplomatów tego kraju dla przywództwa Indii[34]. Z kolei

---

[30] Utajone indeksowanie semantyczne (Latent Semantic Indexing, LSI) lub inaczej: utajona analiza semantyczna (Latent Semantic Analysis, LSA) to metoda analizy tekstu oparta na uczeniu maszynowym, która uczy się na podstawie przykładowego tekstu, aby zidentyfikować „ukryte" koncepcje w wielu dokumentach. Na przykład, jeśli słowa: „artyleria", „pocisk" i „bombardowanie" często pojawiają się w wielu dokumentach, system indeksuje te słowa w tym samym kontekście semantycznym, jednocześnie oddzielając słowo: „pocisk" od dokumentów zawierających wyrażenia „plaża", „piasek" lub „krab". Metoda ta sprawdza się najlepiej w dużych ilościach tekstu, takich jak dokumenty archiwalne, akty prawne czy dokumenty sądowe.

[31] Utajona alokacja Dirichleta (Latent Dirichlet Allocation, LDA) to tekstowa metoda uczenia maszynowego podobna do LSI, chociaż LDA gromadzi słowa w modelu tematycznym samodzielnie, a nie w folderach określonych przez użytkownika. LDA sprawdza częstotliwość i relacje między słowami w tekście na podstawie tego, jak często są one razem używane i w jakim kontekście. LDA oparta jest na modelu statystycznym, który opisuje (hipotetyczny) proces losowy generujący kolejne słowa każdego dokumentu zgodnie z rozkładem tematów w dokumencie. Temat (ang. *topic*) w tym wypadku należy rozumieć jako rozkład prawdopodobieństwa słów z ustalonego słownika. Przykładowo, w temacie: genetyka często będą występować słowa związane z genetyką, w temacie: informatyka częściej będą występować słowa informatyczne.

[32] M.Z. Asghar i in., *Sentiment Analysis on YouTube: A Brief Survey*, „MAGNT Research Report" 2015, vol. 3(1).

[33] H. Chen, *Dark Web: Exploring and Data Mining the Dark Side of the Web*, „Integrated Series in Information Systems", Springer-Verlag, New York 2012, //www.springer.com/gp/book/9781461415565.

[34] V.K. Singh, D. Mahata, R. Adhikari, *Mining the Blogosphere from a Socio-Political Perspective*, w: *2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*, 2010, s. 365–370, https://doi.org/10.1109/CISIM.2010.5643634.

Mueller i Rauch wykorzystali eksplorację tekstu z gazet do prognozowania zbliżających się protestów i konfliktów, opracowując jasny model wykorzystywania dużych ilości tekstu jako podstawy prognozowania zachowań społecznych[35].

Metody wykorzystujące systemy informacji geograficznej (GIS) – teledetekcję

Podobnie jak analiza i badanie tekstów analiza kartograficzna (badanie map) należy do najstarszych metod wywiadu i analizy strategicznej. Metoda ta bazuje przede wszystkim na zmiennych geopolitycznych i geograficznych, a także na politycznym wpływie ukształtowania terenu na przebieg granic. Połączenie systemów informacji geograficznej, czyli GIS[36], i danych o lokalizacji opartych na internecie (meldunki, oznaczenia lokalizacji) pozwala analitykom wykorzystać w szerszym zakresie społeczną i przestrzenną dynamikę ludzkich zachowań, w tym mobilizację, masowe ruchy społeczne i konflikty. Dzięki dodatkowym zmiennym, takim jak wysokość, topografia terenu i jego nachylenie, zasoby naturalne, transport i infrastruktura, analitycy mogą analizować i mapować indywidualne i zbiorowe zachowania ludzi, tworząc ich wzorce za pomocą tzw. wywiadu geoprzestrzennego – GEOINT[37].

Do tego rodzaju analiz stworzono specjalne platformy GIS, np. ArcGis, QGis, ale do analiz można wykorzystać również inne platformy programistyczne, takie jak Python and R (a nawet Excel), które mają pakiety GIS lub rozszerzenia integrujące mapowanie, geostatystykę i analizę zbliżeniową. Poza tym do realizacji przedsięwzięć GEOINT przez zwykłych obywateli, pod warunkiem zastosowaniu dobrego zobrazowania, mogą być wykorzystane aplikacje Planet Labs, Terra Bella, BlackSky Global i XpressSAR.

W GEOINT istnieją dwa główne typy danych: wektorowe i rastrowe. Dane wektorowe to kombinacja zbioru wielokątów i współrzędnych w celu wyznaczenia

[35] H. Mueller, Ch. Rauh, *Reading Between the Lines: Prediction of Political Violence Using Newspaper Text*, „American Political Science Review" 2018, vol. 112, nr 2, https://doi.org/10.1017/S0003055417000570.

[36] GIS (ang. Geographic Information System) – system informacji geograficznej, system informacyjny służący do wprowadzania, gromadzenia, przetwarzania oraz wizualizacji danych geograficznych, którego jedną z funkcji jest wspomaganie procesu decyzyjnego. Każdy GIS składa się z: bazy danych geograficznych, sprzętu komputerowego, oprogramowania oraz twórców i użytkowników GIS. W przypadku gdy system informacji geograficznej gromadzi dane opracowane w formie mapy wielkoskalowej (tj. w skalach 1:5000 i większych), może być nazywany systemem informacji o terenie (ang. Land Information System, LIS).

[37] T.S. Bacastow, D. Bellafiore, *Redefining Geospatial Intelligence*, „American Intelligence Journal" 2009, vol. 27, nr 1.

określonej lokalizacji lub obszaru na mapie. Dane rastrowe obejmują zdjęcia, modele wysokościowe i rendery map[38] w celu przeprowadzenia analizy 3D.

Wraz z rosnącą popularnością GIS w internecie pojawia się coraz więcej baz danych geoprzestrzennych. Te zestawy danych są uzupełniane również przez dane z systemów LiDAR (Light Detection and Ranging), UAV, GPS i satelity, co zwiększa szczegółowość i rozmiar zestawów danych geograficznych. Niezależnie od techniki niektóre z najlepszych zastosowań GEOINT nie tylko dostarczają i wizualizują dane przestrzenne, ale także „opowiadają" historię polityki lub „widzą" strategiczną lukę tam, gdzie inne metody nie są w stanie jej dostrzec. Jednym z wcześniejszych przykładów uniwersyteckiego podejścia do GEOINT jest harwardzka inicjatywa humanitarna (Harvard Humanitarian Initiative). Założona w 1999 roku HHI nawiązała współpracę z organizacjami pozarządowymi, agencjami ONZ i organizacjami pomocy uchodźcom w celu mapowania kryzysów i konfliktów w Darfurze, Sudanie, Czadzie i Kongo, w ścisłej korelacji z zasobami naziemnymi. Z kolei podczas huraganu Katrina zarówno rząd USA, jak i analitycy pozarządowi wykorzystali wiele różnych metod GIS, zwiększając w ten sposób zakres i skuteczność pomocy i reagowania na tę katastrofę.

Godną uwagi, niepaństwową inicjatywą OSINT związaną z danymi geoprzestrzennymi jest narzędzie stworzone przez japońską firmę non-profit Ushahidi, która koncentruje się na monitorowaniu wyborów, nadzorowaniu pomocy w przypadku katastrof i koordynacji pomocy humanitarnej. Narzędzie to wykorzystane było już podczas akcji ratunkowych na Haiti, w Chile, Kenii i we Włoszech. Narzędzie Ushahidi, należące do kategorii GEOINT, tworzy mapę zwaną crowdmap[39], którą traktuje jako platformę danych o wydarzeniach kryzysowych. Crowdmap powstająca za pomocą tzw. crowdsourcingu[40], znalazła już zastosowanie w moni-

[38] Renderowanie – graficzne przedstawienie treści zapisanej cyfrowo w formie właściwej dla danego środowiska. Część programu komputerowego odpowiedzialna za renderowanie nazywana jest mechanizmem renderującym, silnikiem renderującym lub rendererem.

[39] Crowdmapping to podtyp crowdsourcingu, w którym gromadzenie danych wejściowych generowanych przez tłum, takich jak przechwycone komunikaty z telefonów komórkowych, w mediach społecznościowych, jest łączona z danymi geograficznymi w celu stworzenia możliwie najbardziej aktualnej mapy cyfrowej o takich wydarzeniach, jak wojny, kryzysy humanitarne, przestępczość, wybory czy klęski żywiołowe. Takie mapy tworzone są przez ludzi spotykających się za pośrednictwem internetu. Informacje są zwykle wysyłane do inicjatora lub inicjatorów stworzenia mapy drogą SMS-ową lub przez wypełnienie specjalnego formularza online, a następnie zobrazowane automatycznie na mapie w trybie online lub przez wybraną grupę. W 2010 roku firma Ushahidi stworzyła crowdmap – darmową platformę typu open source, dzięki której każdy może realizować projekty crowdmappingowe. Crowdmap to narzędzie, które umożliwia tworzenie online interaktywnych map lub wykresów przebiegu wydarzeń społecznych na podstawie danych zebranych z telefonów komórkowych, wiadomości mailowych i analizy przeglądanych stron internetowych.

[40] Crowdsourcing – proces, w którym organizacja (firma, instytucja publiczna, organizacja non-profit) przeprowadza outsourcing zadań wykonywanych tradycyjnie przez pracowników do

torowaniu wielu protestów na całym świecie, w tym do analizy dynamiki ruchów Occupy[41], protestów w Londynie w 2011 roku, a także wydarzeń kryzysu kenijskiego w latach 2007–2008. Nieco później firma Ushahidi stworzyła infrastrukturę techniczną i oprogramowanie do gromadzenia danych o zdarzeniach kryzysowych w oparciu o relacje świadków, które zostały wykorzystane np. do monitorowania wyborów we Włoszech i Indiach[42].

Metody oparte na teorii sieci

Grupy społeczne i relacje między tymi grupami, tworzące sieci, zawsze były ważne dla prowadzenia wywiadu ze źródeł otwartych, czyli OSINT. Powodem było zainteresowanie państwowych służb wywiadowczych takimi grupami, a także strukturami społecznymi, takimi jak: kierownictwa organizacji politycznych i gospodarczych, kręgi polityczno-decyzyjne państw czy też wewnętrzne struktury organizacji terrorystycznych.

Klasyczna teoria sieci opisująca grupy społeczne skupia się na powiązaniach między jednostkami (przyjaźnie, zasięganie porad itp.) oraz na formalnie ukształtowanych relacjach społecznych (sojusze, stosunki handlowe, wspólnota bezpieczeństwa). Znaczenie teorii sieciowej dla nauk społecznych, polityki i IR (Industrial Relations), polega na jej zdolności do konceptualizacji i prowadzenia analiz dotyczących wzajemnych związków na różnych (mikro, mezo i makro) poziomach procesów politycznych. Teoria ta koncentruje się na interakcjach między poziomami tych analiz, dążąc do określenia, w jaki sposób wspomniane interakcje prowadzą do określonych rozwiązań politycznych czy też zachowań społecznych[43]. Stosownie

niezidentyfikowanej, zwykle bardzo szerokiej grupy ludzi w formie open call (ang. *crowd* – tłum, *sourcing* – pozyskiwanie, zaopatrywanie się). Crowdsourcing umożliwia wszystkim użytkownikom internetu partycypację w zadaniach, które kiedyś były zarezerwowane dla wąskiej grupy specjalistów. Termin „crowdsourcing" został po raz pierwszy zdefiniowany i użyty przez dziennikarza magazynu „Wired" Jeffa Howe'a w artykule *Rise of Crowdsourcing* z 2006 r.

[41] Ruch Occupy był międzynarodowym populistycznym ruchem społeczno-politycznym, który wyrażał sprzeciw wobec nierówności społecznych i ekonomicznych oraz braku „prawdziwej demokracji" na całym świecie. Jego celem było przede wszystkim promowanie sprawiedliwości społecznej i ekonomicznej oraz różnych form demokracji. Ruch miał różne oblicza, ponieważ lokalne grupy często miały różne cele, ale jego główne obawy dotyczyły tego, że wielkie korporacje (i globalny system finansowy) kontrolują świat w sposób, który nieproporcjonalnie przynosi korzyści mniejszości, podważa demokrację i powoduje niestabilność. Pierwszy protest Occupy, który spotkał się z szerokim zainteresowaniem – Occupy Wall Street w nowojorskim Zuccotti Park rozpoczął się 17 września 2011 roku. Do 9 października protesty Occupy odbyły się w ponad 600 społecznościach w Stanach Zjednoczonych i w ponad 951 miastach w 82 krajach.

[42] S. Wheaton, *New Technology Generates Database on Spill Damage*, „The New York Times" 04.05.2010 r., sec. U.S., https://www.nytimes.com/2010/05/05/us/05brigade.html.

[43] *The Oxford Handbook*…, *op.cit.*, s. 26.

do tego teoria sieci zakłada, że relacje społeczne, a także naciski wewnętrzne i zewnętrzne na te relacje mają zdolność wpływania na przekonania i zachowania ludzi i całych społeczeństw. Badając te relacje, teoria ta umożliwia odtworzenie struktur pozornie złożonych interakcji między badanymi grupami społecznymi.

Powstało szereg aplikacji, takich jak Gephi, NetMiner i iGraph, ułatwiających pracę z większymi sieciami, mierząc je metodami ilościowymi za pomocą takich parametrów sieci społecznościowej, jak: betweenness centrality[44], homofilia[45] i centralność[46]. Umożliwia to np. w sieciach stworzonych dla ugrupowań ekstremistycznych i radykalnych łatwiejszą wizualizację i wyraźniejsze (w porównaniu z tradycyjnymi metodami[47]) określenie hierarchii i roli wpływowych osób w tych sieciach. Ponadto obliczeniowa analiza sieci rozszerza klasyczną teorię sieci na znacznie większe i bardziej złożone poziomy, wyznaczając nie tylko relacje między nimi, lecz także umożliwiając wykorzystanie sztucznej inteligencji, uczenia maszynowego i rozwiązań związanych z zastosowaniem sieci neuronowych do automatycznego generowania zmian w czasie rzeczywistym w tych relacjach.

Aktualnie jednym z najpopularniejszych zastosowań analizy sieciowej w cyfrowym OSINT jest analiza mediów społecznościowych, polegająca na śledzeniu aktywności i polubień w tych mediach oraz badaniu relacji między bardzo dużymi grupami uczestników social mediów. W porównaniu ze starszymi metodami sieciowa analiza mediów społecznościowych umożliwia skuteczniejsze wyjawienie hierarchii określonej grupy społecznościowej i funkcjonujących w niej influencerów[48].

---

[44] Betweenness centrality (centralność pośredniczości) – w teorii grafów centralność pośredniczości jest miarą centralności na wykresie opartym na najkrótszych ścieżkach. Miara ta dla wierzchołka w grafie jest frakcją najkrótszych ścieżek pomiędzy wszystkimi parami węzłów w grafie, które przechodzą przez ten węzeł. Może być interpretowana, w pewnym sensie, jako miara wpływu wierzchołka na rozprzestrzenianie się informacji w sieci, przyjmując, że do przepływu są wykorzystywane najkrótsze ścieżki.

[45] Homofilia sieciowa – opiera się na teorii sieci i zakłada, że węzeł ma większe prawdopodobieństwo przyłączenia się do węzła o cechach podobnych do siebie. Homofilia sieciowa jest bardzo dobrze widoczna w sieciach społecznościowych i zwierzęcych. Jest to cecha sieci, która często jest przyczyną przegrupowań lub „klastrów". Homofilia często determinuje szybkość, z jaką informacje są rozpowszechniane w sieci.

[46] Centralność (pomiędzy) – w analizie sieci centralność wyznacza najważniejsze węzły na grafie, w odniesieniu do liczby połączeń z innymi węzłami. W OSINT badania centralności sieci zwykle skupiają się na najważniejszych lub najlepiej połączonych członkach dużej grupy. W analizie sieci społecznościowych najważniejsze dane to te, które przyjmują status influencera.

[47] *The Oxford Handbook*…, *op.cit.*, s. 26.

[48] Influencer (od ang. *influence* – wpływ) – w świecie mediów społecznościowych osoba wpływowa, która dzięki swojemu zasięgowi jest w stanie oddziaływać na ludzi, z którymi nawiązuje trwałe relacje. Często tym terminem określa się twórców internetowych o znacznym rozgłosie, którzy mają znaczne grono odbiorców. Osoby tego rodzaju bywają wykorzystywane w kampaniach marketingowych, ponieważ potrafią umiejętnie wpływać na zachowania internautów. Influencerzy koncentrują się często na ustalonej tematyce. Publikują recenzje produktów lub artykuły informacyjne w zamian za możliwość wypróbowania tego towaru albo bonus finansowy ze strony partnera.

Metody oparte na kryminalistyce obrazowej

W miarę jak usługi sieci Wi-Fi i telefonii danych stały się szybsze i tańsze, komunikacja między ludźmi w internecie szybko ewoluowała od tekstowej do medialnej. Zwykle łatwiej jest wysłać wiadomość głosową na Whatsapp zamiast wiadomości tekstowej lub wysłać zdjęcie lub film, zamiast tworzyć długie zdania. Ta sama logika działa w sytuacjach zagrożeń i kryzysów. W sytuacjach stresowych ludzie mają tendencję do udostępniania zdjęć i filmów, aby udokumentować wydarzenie lub wezwać pomoc, zamiast wysyłać SMS-y i pisać długie wiadomości online. W tym celu, chociaż wciąż tweetujemy, udostępniamy teksty i blogujemy, coraz większa część naszej komunikacji cyfrowej (szczególnie podczas kryzysów) opiera się na mediach (głosowych, obrazowych). Faktycznie, badanie fotografii dla celów strategicznych lub komunikacji w sytuacjach kryzysowych nie jest niczym nowym i sięga końca XIX wieku. Jednak „wywiad obrazowy" (IMINT) jako powszechna praktyka, został wprowadzony po II wojnie światowej.

Dziś media wizualne można metodami OSINT analizować, interpretować i wykorzystywać do wydobywania kluczowych informacji np. z obszarów objętych konfliktami, protestami lub katastrofami, gdzie fizyczny dostęp jest ograniczony. Obrazy i filmy mogą być wykorzystywane do celów weryfikacji, oświadczeń, propagandy i kontrpropagandy na polu działań bojowych lub w epizodach kryzysowych. Mogą być również udostępniane jako dowód istniejących relacji, zainteresowań i możliwości. Ze względu na znaczenie tych mediów dla OSINT jest to również jeden z obszarów najbardziej narażonych na manipulacje i fałszerstwa. Obrazy i filmy mogą być fałszowane, a stare zdjęcia lub filmy udostępniane jako nowe. To z kolei, w sytuacjach kryzysowych, pozwala podmiotom państwowym i niepaństwowym wprowadzać w błąd, rozpraszać i zastraszać przeciwników lub rywali politycznych.

Badań nad obrazami i filmami wideo w internecie, w celu stworzenia sieci badań obrazowych OSINT, podjęło się kilka inicjatyw prywatnych. Najbardziej znaną z nich jest internetowa platforma śledcza Bellingcat. Jej słynne śledztwa internetowe polegające na analizie publikowanych w internecie zdjęć i filmów obejmują m.in.: ruchy wojsk rosyjskich w Syrii, syryjską broń chemiczną, a także zakres i dynamikę wykorzystania policji przeciw protestującym w wielu incydentach na świecie[49].

Innym przykładem prywatnej inicjatywy OSINT, wykorzystującej kryminalistykę obrazową jest Forensic Architecture – platforma akademicko-aktywistyczna

[49] P. Gutierrez, P. Torpey, *How Digital Detectives Say They Proved Ukraine Attacks Came from Russia*, „The Guardian" 17.02.2015 r., http://www.theguardian.com/world/2015/feb/17/ukraine-russia-crossborder-attacks-satellite-evidence.

z siedzibą na Uniwersytecie Londyńskim. Platforma ta wykorzystuje zdjęcia, filmy i zdjęcia lotnicze do rekonstrukcji słabo udokumentowanych incydentów, które mają znaczenie polityczne[50]. Zarówno Bellingcat, jak i Forensic Architecture mają na celu weryfikację wydarzeń poprzez metodyczne badanie mediów, a także łączenie rozproszonych materiałów wizualnych z różnych źródeł w celu stworzenia dowodów.

Początkowo postrzegane jako hobby entuzjastów inicjatywy OSINT z zakresu kryminalistyki medialnej stały się obecnie ważne, a niekiedy skuteczniejsze w porównaniu z państwowymi agencjami wywiadowczymi. Świadczą o tym przykłady Bellingcat i Forensic Architecture, które dostarczyły dowodów sądowych, a także danych dla raportów na temat naruszeń praw człowieka, tworzonych przez ONZ i niektóre państwa członkowskie tej organizacji[51].

OSINT z crowdsourcingu

Przy tak dużej liczbie publicznie dostępnych, krytycznych typów danych dość kuszące jest stwierdzenie, że „tajemnice się skończyły" lub że wkraczamy w „posttajny" porządek świata". Rzeczywiście, kiedy Sean P. Larkin w swoim artykule dla „Foreign Affaires" zapowiadał *age of transparency* (wiek transparentności), był przekonany, że powszechny dostęp do zdjęć satelitarnych, śledzenie za pomocą dronów, automatyczne raporty kryzysowe, dziennikarstwo obywatelskie i blogerzy funkcjonujący w otwartych mediach sprawią, że dotychczasowe sekrety nie będą miały znaczenia[52]. Larkin twierdził również, że ze względu na malejące koszty publicznie dostępnej inwigilacji wzrastają koszty utrzymania i ochrony tajemnic. Zdolność państw do tworzenia i utrzymywania ram bezpieczeństwa informacyjnego, a także własnej narracji podczas różnego rodzaju kryzysów, napięć dyplomatycznych i protestów została znacznie utrudniona przez technologię. Zwłaszcza od czasu odkrycia potęgi mediów społecznościowych i ich roli podczas ważnych wydarzeń społecznych i politycznych, kiedy państwa muszą konkurować z tymi nowymi źródłami informacji, np. w ramach tzw. SOCMINT (ang. SOCial Media INTelligence) – wywiadu z mediów społecznościowych. Poza tym zainteresowanie kryminalistyką obrazową oraz globalne, wzajemne powiązania prywatnych analityków spowodowały pojawienie się zjawiska nazywanego „raportowaniem obywatelskim", a co za tym idzie, powstaniem nowej kasty analityków, tworzących

[50] R. Moore, *Forensic Architecture: The Detail behind the Devilry*, „The Observer" 25.02.2018 r., sec. Art and Design, https://www.theguardian.com/artanddesign/2018/feb/25/forensic-architects-eyal-weizman.

[51] D. Collins, *A US Airstrike Which Killed 38 People Allegedly Hit a Peaceful Mosque in a Syrian Village*, „Business Insider" 18.04.2017 r., http://www.businessinsider.com/us-airstrike-allegedly-hit-a-peaceful-mosque-in-a-syrian-village-2017-4.

[52] S.P. Larkin, *The Age of Transparency*, „Foreign Affairs" 18.04.2016 r., https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency.

swego rodzaju sieci wywiadowcze[53], funkcjonujące w oparciu o wspomniany już wcześniej crowdsourcing.

W rzeczywistości jednak to amerykańska agencja DARPA jako pierwsza próbowała wykorzystać crowdsourcing do analizy danych wywiadowczych. Podczas cyfrowych ćwiczeń zorganizowanych w 2009 roku pod kryptonimem „Network Challenged"[54], próbowano stwierdzić, czy półautonomiczna sieć użytkowników, współpracująca za pośrednictwem narzędzi społecznościowych, mogłaby lepiej zarządzać wyzwaniami, przed którymi stoją państwowe wywiady realizujące zadania OSINT (takie jak generowanie danych o zdarzeniach, ich szybka weryfikacja czy pomiar nastrojów społecznych). Ćwiczenie wykazało, że „amatorzy" (czyli cywile, którzy mieli niewielkie lub żadne formalne przygotowanie w zakresie wywiadu i polityki planowania) byli zarówno użyteczni, jak i mało przydatni, w zależności od przyjętego punktu widzenia. Z jednej strony OSINT z crowdsourcingu był zdecydowanie szybszy, nie podlegał ograniczeniom biurokratycznym i restrykcjom politycznym. Z drugiej – większości entuzjastów OSINT brakowało odpowiedniego przygotowania wywiadowczego, co wpływało na to, że raporty dla decydentów miały charakter chaotyczny i niespójny. Innymi słowy, OSINT oparty na crowdsourcingu został uznany za dobry w kwestionowaniu narracji państwowych podczas ukierunkowanych incydentów (takich jak kryzysy), ale brakowało mu potencjału dla monitorowania i zbierania regularnych, codziennych danych internetowych dla tworzenia ocen rozwoju sytuacji i wysuwania sugestii politycznych[55].

Ze względów politycznych państwom trudno jest wykorzystać siłę crowdsourcingu zawartą w OSINT podczas wydarzeń kryzysowych. Powodem jest to, że większość cyfrowych narzędzi OSINT upowszechniła się po 2011 roku, czyli po wydarzeniach związanych z ruchami Occupy i arabskiej wiośnie, co spowodowało, że ogólna wymowa tej praktyki stała się antyhegemoniczna[56] i opozycyjna[57].

---

[53] Warto zwrócić uwagę, że niebezpieczeństwem w gromadzeniu i ocenie zebranych w ten sposób danych wywiadowczych jest w tym wypadku zwrot „podobnie myślących". „Myślący podobnie" analitycy mogą w imię własnych przekonań odrzucać niektóre scenariusze, biorąc pod uwagę tylko te, które odpowiadają ich poglądom politycznym lub społecznym (przyp. K.S.).

[54] M. Harris, *How A Lone Hacker Shredded the Myth of Crowdsourcing*, „WIRED" 02.09.2015 r., https://www.wired.com/2015/02/how-a-lone-hacker-shredded-the-myth-of-crowdsourcing/.

[55] L. Greenemeier, *DARPA Verigames Crowdsourced Formal Verification (CSFV) Project*, „Scientific American" 09.06.2015 r., https://www.scientificamerican.com/citizen-science/darpa-verigames-crowdsourced-formal-verification-csfv-project/.

[56] Antyhegemoniczny – zaprzeczenie słowa hegemoniczny, które pochodzi od słowa „hegemonia" i oznacza m.in. wojnę o hegemonię, tj. wojnę między dominującym w międzynarodowym systemie mocarstwem lub mocarstwami a rosnącym konkurentem lub konkurentami. Konflikt przyjmuje wymiar globalny i charakteryzuje się udziałem wszystkich większych i większości mniejszych państw w systemie.

[57] Z. Tufekci, *Twitter and Tear Gas. The Power and Fragility of Networked*, Yale University Press, New Haven 2019.

Ponadto większość wcześniejszych form crowdsourcingu OSINT skupiała się na kierowaniu protestującymi tłumami, organizowaniu logistyki protestów i omijaniu działań policji lub państwowych agencji wywiadowczych. W związku z tym powstała szeroka przepaść między państwowymi agencjami wywiadowczymi, które nie ufają OSINT z crowdsourcingu, a organizacjami stworzonymi przez indywidualnych analityków, które z kolei nie ufają wywiadom państwowym. Ta wzajemna nieufność uniemożliwiła jak dotąd stworzenie możliwego do zaakceptowania, wspólnego państwowego i społecznego modelu środowiska OSINT, opartego na mediach społecznościowych. Ponieważ taki wspólny model jest jak na razie trudny do osiągnięcia, działania wywiadów państwowych i działania organizacji OSINT tworzonych przez osoby prywatne wykorzystują w sytuacjach kryzysowych własne narzędzia zdobywania informacji i własne sieci do ich przekazywania.

W crowdsourcing zaangażowane są trzy grupy ludzi. Są to:

1) osoby gromadzące dane o zdarzeniach w terenie ich występowania;
2) kuratorzy danych cyfrowych[58] w terenie;
3) analitycy danych, którzy mogą być ulokowani poza terenem zdarzeń.

Jednym z najwcześniejszych przykładów crowdsourcingu jest zastosowanie platformy Ushahidi (nazwa w języku suahili oznacza „świadka") do monitorowania brutalnych wydarzeń związanych z wyborami w Kenii w latach 2007–2008. Po dokładnej analizie okazało się, że dokładność danych o zdarzeniach w Kenii, jakie zebrała ta platforma, była lepsza niż praca specjalistów wywiadu państwowego[59]. Ushahidi ze zmodernizowaną platformą mapową GeoCommons była również wykorzystana do pozyskania danych o wydarzeniach związanych z trzęsieniem ziemi na Haiti w 2010 roku, znacząco pomagając agencjom humanitarnym w ich wysiłkach na rzecz niesienia pomocy ofiarom kataklizmu. W kolejnych latach platforma Ushahidi współpracowała z Biurem Narodów Zjednoczonych ds. Koordynacji Pomocy Humanitarnej (OCHA), przy stworzeniu mapy kryzysowej Libii. Mapa ta przeznaczona była dla skuteczniejszego gromadzenia danych o obszarach dotkniętych wojną, które ze względu na trudności z dotarciem konwojów pomocowych drogą lądową wymagały zrzutów powietrznych. Przy okazji okazało się, że opracowane przez cywilów platformy humanitarne i mapy pomocowe OSINT mogą

[58] Kuratorstwo danych cyfrowych – selekcja, konserwacja, utrzymanie, gromadzenie i archiwizacja zasobów cyfrowych. Kurator wyznacza, utrzymuje i nadaje wartość repozytoriom danych cyfrowych, aby umożliwić wykorzystanie konkretnych danych zarówno obecnie, jak i w przyszłości. Zwykle zajmują się tym archiwiści, bibliotekarze, naukowcy, historycy i inni uczeni. Przedsiębiorstwa również zaczynają wykorzystywać kuratorstwo danych celem poprawy jakości informacji i danych w obrębie swoich procesów operacyjnych i strategicznych. Pomyślnie przeprowadzone pomoże ograniczyć utratę danych spowodowaną zanikaniem przestarzałych nośników cyfrowych.

[59] A. Giridharadas, *Ushahidi – Africa's Gift to Silicon Valley*, 13.03.2010 r., https://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html.

być wykorzystywane przez podmioty państwowe. Niektóre siły powietrzne NATO wykorzystały stworzoną przez Ushahidi mapę pomocy humanitarnej dla lokalizacji celów naziemnych i planowania bombardowań powietrznych[60].

Podsumowanie

Eksplozja popularności korzystania przez internautów z mediów społecznościowych i powszechnego umieszczania w nich najróżniejszych danych powoduje wiele problemów związanych z wiarygodnością tych danych. Dostępnych jest wiele narzędzi i technik eksploracji danych w internecie, a tradycyjne systemy monitorowania mediów osiągnęły taki poziom, że możliwe jest monitorowanie sytuacji lub zdarzenia będącego obiektem zainteresowania w czasie rzeczywistym. Wyzwaniem jest jednak ciągle podjęcie decyzji, w jakie raporty wierzyć, jak je indeksować i jak przetwarzać dane. Prywatne interesy pozwalają różnym grupom na wykorzystywanie zarówno mediów społecznościowych, jak i mediów tradycyjnych do celów propagandowych. Oprócz tego pod uwagę należy wziąć celową dezinformację stosowaną w ramach tzw. wojen informacyjnych. Tak więc wraz ze wzrostem łatwości publikowania coraz ważniejsze staje się zbieranie raportów ze wszystkich stron konfliktów oraz równoważenie wzajemnych roszczeń i pretensji.

Ogromna ilość możliwych do eksploracji danych pochodzi z IoT, bodynetu czy SCADA, tworzących wielkie zbiory danych. Poza tym w szybkim tempie postępuje cyfryzacja analogowych dotąd administracyjnych, bibliotecznych i innych zbiorów danych. Co kilka lat świat zwielokrotnia wysiłki na rzecz porzucenia dokumentów papierowych. Według amerykańskiej National Archives and Records Administration rząd federalny USA już zdigitalizował ponad 235 mln stron akt rządowych, a do 2024 roku zamierza osiągnąć poziom 500 mln stron. I chociaż digitalizacja dokumentów papierowych może pomóc agencjom rządowym zwiększyć efektywność, wydajność, poprawić komunikację i usprawnić usługi publiczne, większość danych nadal pozostanie nieustrukturyzowanych. Jest to obszar, gdzie wkracza NLP. Dzięki najnowszym postępom technologicznym komputery mogą teraz czytać, rozumieć i używać ludzkiego języka. Mogą nawet zmierzyć tzw. sentyment, śledząc określone teksty lub ton wypowiedzi, a także umożliwić agencjom rządowym rozpoznawanie wzorców zachowań społecznych, kategoryzować ważne tematy i analizować opinię publiczną.

Przeszukiwanie wielkich zbiorów danych za pomocą współczesnych narzędzi OSINT jest możliwe m.in. dzięki metodom pozyskiwania danych wywiadowczych

[60] I. Traynor, *Libya: Nato Bombing of Gaddafi Forces 'Relying on Information from Rebels'*, „The Guardian" 18.05.2011 r., sec. World News, https://www.theguardian.com/world/2011/may/18/libya-nato-bombing-benghazi-rebel-leaders.

w ogólnodostępnych zbiorach cyfrowych. Warto również zauważyć, że wyzwaniem dzisiaj nie jest już sam dostęp do informacji z open sources, ale ich tagowanie, indeksowanie, archiwizowanie i analiza. Wymaga to rozwoju baz wiedzy ogólnego przeznaczenia i baz dziedzinowych. Potrzebne są narzędzia wywiadowcze, które umożliwią analitykowi szybki dostęp do odpowiednich danych, a także dostęp do rankingu źródeł obejmujących zarówno fakty, jak i opinie.

Wraz z rozwojem nowych technologii informacyjnych zmieniło się podejście do kwestii ochrony ważnych informacji o charakterze niejawnym. Obowiązuje założenie, że to państwa odpowiadają zarówno za ochronę tego typu informacji, jak i ich pozyskiwanie przez wywiady u przeciwników politycznych. OSINT znacząco zmienił to założenie. Monopolistami w prowadzeniu wywiadu na wysokim poziomie nie są już największe państwa i potężne korporacje. Dziennikarze, organizacje pozarządowe i obywatele, mając dostęp do odpowiednich narzędzi informatycznych, zbierają, przetwarzają i rozpowszechniają informacje uznawane wcześniej za klasyfikowane. Urynkowienie wywiadu – sprzętu inwigilacyjnego, usług analitycznych w mediach społecznościowych i rewolucja programistyczna – doprowadziło do pojawienia się nowych źródeł informacji dostępnych międzynarodowej konkurencji wywiadowczej. Powszechny dostęp do komercyjnych zdjęć satelitarnych i zobrazowań wykonywanych przez drony, a także do platform analitycznych w mediach społecznościowych przyczynił się do pojawienia się globalnej kasty analityków OSINT z nieproporcjonalnym wpływem na politykę informacyjną. Dzisiejsi entuzjaści wywiadu o skromnym poziomie wiedzy technicznej, mający mniej niż podstawowe umiejętności programowania, ale za to dysponujący „wnikliwym okiem", niezbędnym do eksploracji medialnych danych cyfrowych, mogą stać się częścią globalnej sieci OSINT opartej na przykład na crowdsourcingu.

Bibliografia

Literatura

Appel E.J., *Cybervetting: Internet Searches for Vetting, Investigations, and Open-Source Intelligence*, Second Edition, CRC Press 2014.

Asghar M.Z. i in., *Sentiment Analysis on YouTube: A Brief Survey*, „MAGNT Research Report" 2015, vol. 3(1).

Bacastow T.S., Bellafiore D., *Redefining Geospatial Intelligence*, „American Intelligence Journal" 2009, vol. 27, nr 1.

Dover R., Goodman M., Hillebrand C., *Routledge Companion to Intelligence Studies*, Routledge 2015.

Dulles A., *The Craft of Intelligence: America's Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*, Guilford 2016.

Hulnick A.S., *Keeping Us Safe: Secret Intelligence and Homeland Security*, Praeger Publishers, Westport, CT, 2004.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Wydział Dziennikarstwa i Nauk Politycznych, Uniwersytet Warszawski, Warszawa 2015.

The Oxford Handbook of National Security Intelligence, L.K. Johnson (red.), Oxford University Press 2012.

Tufekci Z., *Twitter and Tear Gas. The Power and Fragility of Networked*, Yale University Press, New Haven 2019.

Netografia

Brzeziński D., *Top modeling*, http://www.cs.put.poznan.pl/alabijak/emd/11_Topic_modeling.pdf.

Chen H., *Dark Web: Exploring and Data Mining the Dark Side of the Web*, „Integrated Series in Information Systems", Springer-Verlag, New York 2012, https://www.springer.com/gp/book/9781461415565.

Collins D., *A US Airstrike Which Killed 38 People Allegedly Hit a Peaceful Mosque in a Syrian Village*, „Business Insider" 18.04.2017 r., http://www.businessinsider.com/us-airstrike-allegedly-hit-a-peaceful-mosque-in-a-syrian-village-2017-4.

Digital Activism Survey Report 2009, https://www.othersidegroup.com/2009/07/digital-activism-survey-results/.

Giridharadas A., *Ushahidi – Africa's Gift to Silicon Valley*, 13.03.2010 r., https://www.nytimes.com/2010/03/14/weekinreview/14giridharadas.html.

Greenemeier L., *DARPA Verigames Crowdsourced Formal Verification (CSFV) Project*, „Scientific American" 09.06.2015 r., https://www.scientificamerican.com/citizen-science/darpa-verigames-crowdsourced-formal-verification-csfv-project/.

Gutierrez P., Torpey P., *How Digital Detectives Say They Proved Ukraine Attacks Came from Russia*, „The Guardian" 17.02.2015 r., http://www.theguardian.com/world/2015/feb/17/ukraine-russia-crossborder-attacks-satellite-evidence.

Harris M., *How A Lone Hacker Shredded the Myth of Crowdsourcing*, „WIRED" 02.09.2015 r., https://www.wired.com/2015/02/how-a-lone-hacker-shredded-the-myth-of-crowdsourcing/.

Larkin S.P., *The Age of Transparency*, „Foreign Affairs" 18.04.2016 r., https://www.foreignaffairs.com/articles/world/2016-04-18/age-transparency.

Moore R., *Forensic Architecture: The Detail behind the Devilry*, „The Observer" 25.02.2018 r., sec. Art and Design, https://www.theguardian.com/artanddesign/2018/feb/25/forensic-architects-eyal-weizman.

Mueller H., Rauh Ch., *Reading Between the Lines: Prediction of Political Violence Using Newspaper Text*, „American Political Science Review" 2018, vol. 112, nr 2, https://doi.org/10.1017/S0003055417000570.

*NATO Open Source Intelligence Reade*r, 2002, https://cyberwar.nl/d/NATO%20OSINT%20Reader%20FINAL%20Oct2002.pdf.

Piotrowski T., Grabowski Ł., *Interpretacja danych frekwencyjnych z korpusów językowych: opis pewnych problemów (na kilku przykładach z życia wziętych)*, https://repo.uni.opole.pl/.

Singh V.K., Mahata D., Adhikari R., *Mining the Blogosphere from a Socio-Political Perspective*, w: *2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM)*, 2010, https://doi.org/10.1109/CISIM.2010.5643634.

Tongur S., Engwall M., *The Business Model Dilemma of Technology Shifts*, „Technovation" 2014, vol. 34, nr 9, https://doi.org/10.1016/j.technovation.2014.02.006.

Traynor I., *Libya: Nato Bombing of Gaddafi Forces 'Relying on Information from Rebels'*, „The Guardian" 18.05.2011 r., sec. World news, https://www.theguardian.com/world/2011/may/18/libya-nato-bombing-benghazi-rebel-leaders.

Ünver A., *Digital Open Source Intelligence and International Security: A Primer*, http://edam.org.tr/en/digital-open-source-intelligence-and-international-security-a-primer/.

Wheaton S., *New Technology Generates Database on Spill Damage*, „The New York Times" 04.05.2010 r., sec. U.S., https://www.nytimes.com/2010/05/05/us/05brigade.html.

Streszczenie

Działalność polegająca na zdobywaniu informacji ze źródeł jawnych i ogólnie dostępnych w polskiej literaturze często nazywana jest białym wywiadem. Za granicą zwykle używa się akronimu OSINT (ang. Open Source INTelligence), którego rozwinięcie można przetłumaczyć jako „wywiad ze źródeł otwartych". Rozwój technologii cyfrowych i pojawienie się w telekomunikacji wielu nowych rozwiązań i źródeł danych doprowadziły do powstania ogromnych repozytoriów danych cyfrowych. Najpopularniejsze metody pozyskiwania danych wywiadowczych w ogólnodostępnych zbiorach cyfrowych to: metody językowe i tekstowe; metody wykorzystujące systemy informacji geograficznej (GIS) – teledetekcję; metody oparte na teorii sieci; metody wykorzystujące kryminalistykę wizualną.

Summary

The activity consisting in obtaining information from open and generally available sources in Polish literature is often called white intelligence. Abroad, the acronym OSINT (Open Source INTelligence) is usually used, the extension of which can be translated as „open source intelligence". The development of digital technologies and the emergence of many new solutions and data sources in telecommunications have led to the creation of huge digital data repositories. The most popular methods of obtaining intelligence data in publicly available digital collections are: language and text methods; methods using geographic information systems (GIS) – remote sensing; methods based on network theory; methods using visual forensics.

Słowa kluczowe

Wywiad ze źródeł otwartych, bazy danych, dane wywiadowcze.

Keywords

Open source intelligence, databases, intelligence.

Krzysztof Surdyk – dr, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie.

Aleksandra Miler-Zawodniak
Marcin Zawodniak

KONCEPCJE SYSTEMU BEZPIECZEŃSTWA NARODOWEGO W DOKUMENTACH STRATEGICZNYCH W LATACH 2000–2020

Wstęp

Rozwijanie i utrzymywanie sprawnego systemu bezpieczeństwa narodowego jest głównym elementem polityki bezpieczeństwa każdego państwa. System bezpieczeństwa musi elastycznie dostosowywać się do zmian zachodzących w otoczeniu, aby w każdej sytuacji osiągnąć zakładane cele. Analiza dokumentów strategicznych obowiązujących w Polsce w ciągu ostatnich 20 lat pozwala dostrzec różne koncepcje i podejścia do systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej (SBN RP).

Strategia bezpieczeństwa Rzeczypospolitej Polskiej z 2000 roku

Strategia bezpieczeństwa Rzeczypospolitej Polskiej przyjęta 4 stycznia 2000 roku odnosiła się do różnych dziedzin bezpieczeństwa; jej zasadnicze treści dotyczyły systemu obronności[1], który do przeciwdziałania zagrożeniom integrować miał cały militarny i niemilitarny potencjał państwa[2]. Można wnioskować, że poszerzanie systemu obronności o aspekty pozamilitarne wskazuje na potrzebę rozumienia i postrzegania problematyki bezpieczeństwa szerzej niż wymiar militarny.

---

[1] System obronności obejmuje podsystemy: kierowania obronnością (organy kierowania obronnością); militarny (Siły Zbrojne RP); pozamilitarny (pozamilitarne ogniwa obronne). Strategia bezpieczeństwa Rzeczypospolitej Polskiej z 2000 roku, pkt 4.4.

[2] Poza problematyką bezpieczeństwa militarnego system obronności zawierał dodatkowe misje, które obejmowały m.in.: ochronę środowiska naturalnego; bezpieczeństwo energetyki jądrowej; ochronę ludności i majątku narodowego przed skutkami oddziaływań kryzysowych i wojennych. Szerzej zob. W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, AON, Warszawa 2011, s. 282–283.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 2003 roku

Dokument ten nie ujmuje *explicite* problematyki SBN RP. Jednak jego treść pozwala określić, choć jedynie w formie przypuszczeń, elementy tworzące taki system. Elementami składowymi niezdefiniowanego SBN RP mogłyby być:

- podsystem kierowania, składający się z „wszystkich instytucji państwowych, organów władzy administracji państwowej". Jego zadaniem byłoby zapewnienie „harmonijnego współdziałania […], odpowiedniego dostosowania ich metod pracy do nowych wyzwań w dziedzinie bezpieczeństwa"[3];
- podsystem obronny – w dokumencie został określony jako system obronny państwa (SOP), odpowiedzialny za: wykrywanie zagrożeń (określonych w Strategii); kierowanie przygotowaniami obronnymi w czasie pokoju; reagowanie na zagrożenia kryzysowe; obronę państwa i udział we wspólnej; sojuszniczej obronie[4];
- podsystemy wzmocnienia – gospodarka, wywiad, obrona cywilna, służby specjalne, policja, straż graniczna, straż pożarna[5].

Strategia bezpieczeństwa narodowego RP z 2007 roku

Strategia ta podejmuje już problematykę SBN RP, określając go jako „wszystkie odpowiedzialne za bezpieczeństwo w świetle Konstytucji RP i właściwych ustaw organy oraz instytucje należące do władz ustawodawczych, wykonawczych i sądowniczych [...], ważnymi jego elementami są siły zbrojne oraz służby i instytucje rządowe zobowiązane do zapobiegania i przeciwdziałania zagrożeniom zewnętrznym, zapewnienia bezpieczeństwa publicznego, prowadzenia działań ratowniczych oraz ochrony ludności i mienia […], a także […] władze samorządowe oraz inne podmioty prawne, w tym przedsiębiorcy tworzący potencjał przemysłowo-obronny"[6].

Strategia nie określała wprost misji i celów SBN RP, ale jej treść umożliwia ich pośrednie wyinterpretowanie. Mając na uwadze, że strategia z 2007 roku przyjmuje, jako punkt wyjścia, interesy narodowe oraz cele strategiczne państwa, można założyć, że misja SBN RP wynika z treści nadrzędnego celu strategicznego RP, natomiast jego cele są pochodną określonych w tej strategii celów strategicznych. Stwierdzić zatem można, że misją SBN RP byłoby „zapewnienie korzystnych

[3] Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 2003 roku, rozdział II.
[4] Zob. W. Kitler, *Bezpieczeństwo narodowe RP…*, *op.cit.*, s. 285.
[5] Szerzej zob. *ibidem*.
[6] Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2007, s. 21.

i bezpiecznych warunków realizacji interesów narodowych poprzez eliminację zewnętrznych i wewnętrznych zagrożeń, redukowanie ryzyka oraz odpowiednie oszacowanie podejmowanych wyzwań i umiejętne wykorzystywanie pojawiających się szans”[7]. Analogicznie rozpatrując główne cele strategiczne zawarte w Strategii, można wskazać cele SBN RP[8]:

- zapewnienie niepodległości i nienaruszalności terytorialnej oraz suwerenności RP;
- zdolność obrony interesów narodowych;
- ochrona: wolności, praw człowieka i obywatela, duchowego i materialnego dziedzictwa narodowego, środowiska naturalnego;
- stworzenie warunków rozwoju cywilizacyjnego i gospodarczego;
- zapewnienie możliwości aktywnego kształtowania stosunków w otoczeniu międzynarodowym oraz promowanie wizerunku wiarygodnego uczestnika stosunków międzynarodowych, a także realizacji zobowiązań sojuszniczych.

Struktura SBN RP przedstawiona w tej Strategii zbudowana jest z dwóch zasadniczych elementów: podsystemu kierowania bezpieczeństwem narodowym oraz podsystemów wykonawczych. Podsystem kierowania tworzą organy władzy publicznej i kierownicy jednostek organizacyjnych wykonujących zadania związane z bezpieczeństwem narodowym oraz organy dowodzenia Sił Zbrojnych RP. Zasadniczym zadaniem podsystemu kierowania było „zapewnienie ciągłości podejmowania decyzji i działań w celu utrzymania” bezpieczeństwa narodowego[9].

Podsystemy wykonawcze „tworzą siły i środki pozostające we właściwościach ministrów kierujących działami administracji rządowej, centralnych organów administracji rządowej, wojewodów, organów samorządu terytorialnego oraz innych podmiotów odpowiedzialnych za realizację ustawowo określonych zadań w zakresie bezpieczeństwa narodowego”[10]. Jako podstawowe zadania tych podsystemów wskazano: wczesne wykrywanie i zapobieganie zagrożeniom bezpieczeństwa kraju, a w razie ich wystąpienia – przeciwdziałanie negatywnym następstwom[11].

---

[7] *Ibidem*, s. 5.

[8] Por. *ibidem*, s. 5–6.

[9] „Realizuje on ponadto przedsięwzięcia związane z monitorowaniem źródeł, rodzajów, kierunków i skali zagrożeń; zapobieganiem powstawaniu zagrożeń bezpieczeństwa narodowego na terytorium Rzeczypospolitej Polskiej oraz poza jej granicami; zapobieganiem skutkom tych zagrożeń oraz ich usuwaniem, a także kierowaniem obroną narodową” – szerzej zob. W. Kitler, *Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe*, Wydawnictwo Adam Marszałek, Toruń 2018, s. 225.

[10] Strategia bezpieczeństwa narodowego RP, 2007, s. 23.

[11] Zob. *ibidem*.

Struktury podsystemów wykonawczych stanowiły poszczególne działy administracji rządowej, a ich szczegółowe zadania realizowane na rzecz SBN RP wynikały z ich obszarów odpowiedzialności kompetencyjnej[12].

W 2009 roku ukazała się Strategia obronności Rzeczypospolitej Polskiej, która była strategią sektorową do Strategii bezpieczeństwa narodowego RP z 2007 roku. Określono w niej zadania i kształt systemu obronnego państwa.

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022

Główny obszar zainteresowania Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022[13] (SRSBN RP) z 2013 roku ukierunkowany był na bezpieczeństwo zewnętrzne i militarne[14]. Z jej zakresu tematycznego wyłączone zostały obszary, które obejmują inne dziedziny funkcjonowania państwa[15]. Dokument definiuje system bezpieczeństwa narodowego jako „całość sił, środków oraz zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa, odpowiednio do tych zadań zorganizowana, utrzymywana i przygotowywana, w którym wyróżnia się podsystem kierowania i szereg podsystemów wykonawczych”[16].

Jako misję SBN RP wskazano zagwarantowanie szybkiego i sprawnego działania w każdych warunkach i w reakcji na wszelkiego typu zagrożenia oraz kry-

[12] Strategia z 2007 roku do podsystemów wykonawczych zalicza: sprawy zagraniczne, obronę narodową, służby specjalne, administrację publiczną i sprawy wewnętrzne, informatyzację i telekomunikację, sprawiedliwość, gospodarkę, gospodarkę morską, budżet i finanse publiczne, Skarb Państwa, transport, budownictwo, gospodarkę przestrzenną i mieszkaniową, rolnictwo, rozwój wsi i rynki rolne, rozwój regionalny, pracę, zabezpieczenie społeczne i sprawy rodziny, zdrowie, naukę i szkolnictwo wyższe, oświatę i wychowanie, kulturę i ochronę dziedzictwa narodowego, środowisko. Szerzej zob. Strategia bezpieczeństwa narodowego RP, 2007, s. 23–36.

[13] Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022 została przyjęta uchwałą nr 67 Rady Ministrów z 9 kwietnia 2013 r. (M.P. poz. 377). Jej wprowadzenie wycofało jednocześnie Strategię obronności Rzeczypospolitej Polskiej z 2009 r. Jest ona jednym z dziewięciu dokumentów zawierających zintegrowane strategie rozwoju kraju. Struktura ta stanowi próbę powiązania budowy zintegrowanego systemu bezpieczeństwa narodowego z planowaniem rozwoju społeczno-gospodarczego kraju. Dokonano w niej diagnozy systemu bezpieczeństwa narodowego oraz przedstawiono wyzwania i wizję rozwoju systemu bezpieczeństwa narodowego. Szerzej zob. http://www.nowastrategia.org.pl/analiza-krytyczna-srsbn/, dostęp: 02.01.2021 r.

[14] Zob. Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022, s. 4.

[15] Pozostałe strategie to: Strategia innowacyjności i efektywności gospodarki; Strategia rozwoju kapitału ludzkiego; Strategia rozwoju transportu; Bezpieczeństwo energetyczne i środowisko; Sprawne państwo; Strategia rozwoju kapitału społecznego; Krajowa strategia rozwoju regionalnego 2010–2020: Regiony, miasta, obszary wiejskie; Strategia zrównoważonego rozwoju wsi, rolnictwa i rybactwa. Zob. *Strategia rozwoju kraju 2020,* Ministerstwo Rozwoju Regionalnego, Warszawa 2012, s. 5, https://rpo2007-2013.slaskie.pl/zalaczniki/2014/01/17/1389965536.pdf, dostęp: 02.01.2021 r.

[16] Strategia rozwoju systemu..., s. 3.

zysy[17]. Za cel SBN RP uznano „odpowiednie przygotowanie i wykorzystanie sił oraz środków będących w dyspozycji państwa do przeciwdziałania zagrożeniom godzącym w przetrwanie narodu i państwa, integralność terytorialną, niezależność polityczną i suwerenność, sprawne funkcjonowanie instytucji państwa oraz rozwój społeczno-gospodarczy"[18].

Struktura SBN RP składa się z:

- podsystemu kierowania – w jego skład wchodzą „organy władzy publicznej i kierownicy jednostek organizacyjnych, którzy wykonują zadania związane z bezpieczeństwem narodowym oraz organy dowodzenia Sił Zbrojnych RP"[19].
- podsystemów wykonawczych – są to „siły i środki pozostające we właściwościach ministrów […], centralnych organów administracji rządowej, wojewodów, organów samorządu terytorialnego oraz innych […], odpowiedzialnych za realizację […] zadań w zakresie bezpieczeństwa narodowego"[20]. Wyróżnić należy trzy zasadnicze podsystemy: sprawy zagraniczne, obronność (Siły Zbrojne RP, struktury administracyjne, struktury gospodarcze) oraz służby specjalne[21];
- systemów wsparcia bezpieczeństwa, które uzupełniają podsystemy wykonawcze – są to: „ochrona infrastruktury krytycznej […], system rezerw strategicznych […], szereg uzupełniających, szczegółowych systemów operacyjnych (np.: system ochrony granicy państwowej, system przeciwpowodziowy, system ochrony danych osobowych i informacji niejawnych)[22].

Strategia bezpieczeństwa narodowego RP z 2014 roku

Strategia ta wskazuje, że SBN RP „obejmuje siły, środki i zasoby przeznaczone przez państwo do realizacji zadań w tym obszarze, odpowiednio zorganizowane, utrzymywane i przygotowywane"[23]. Podobnie jak w przypadku Strategii z 2007 roku misja i cel SBN RP nie zostały wskazane wprost. Odwołując się do interesów narodowych[24], misją SBN RP byłoby „dysponowanie skutecznym potencjałem bezpieczeństwa, zapewniając gotowość i zdolność do zapobiegania zagro-

[17] *Ibidem*.
[18] *Ibidem*, s. 13.
[19] Szerzej zob. W. Kitler, *Organizacja bezpieczeństwa…*, *op.cit*., s. 204.
[20] Zob. *ibidem*, s. 210.
[21] Wiodącą rolę wśród podsystemów wykonawczych w realizacji celów strategii pełnić będzie dyplomacja oraz Siły Zbrojne RP. Szerzej zob. *ibidem*, s. 210–211.
[22] Strategia rozwoju systemu..., s. 14.
[23] Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, 2014, s. 13.
[24] Misja i cel SBN RP w jednoznaczny sposób była określona w wydanej w 2013 roku Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022.

żeniom, utrzymanie silnej pozycji Polski na arenie międzynarodowej, zapewnienie ochrony obywatelom oraz zapewnienie trwałego i zrównoważonego rozwoju”[25]. W pośredni sposób można również wskazać cele SBN RP[26]:

- utrzymywanie i demonstrowanie gotowości zintegrowanego SBN do wykorzystywania szans, podejmowania wyzwań, redukowania ryzyka i przeciwdziałania zagrożeniom;
- doskonalenie zintegrowanego SBN, a zwłaszcza jego elementów kierowania, w tym zapewnienie niezbędnych zasobów i zdolności;
- rozwój potencjału obronnego i ochronnego adekwatnego do potrzeb i możliwości państwa oraz zwiększenie jego interoperacyjności w NATO i UE;
- wzmocnienie gotowości i zdolności NATO do kolektywnej obrony oraz spójności działań UE w dziedzinie bezpieczeństwa (budowanie silnej pozycji Polski w obu tych organizacjach);
- rozwijanie bliskiej współpracy ze wszystkimi sąsiadami oraz budowanie partnerskich relacji z innymi państwami, w tym służących zapobieganiu i rozwiązywaniu konfliktów i kryzysów międzynarodowych;
- promowanie na arenie międzynarodowej zasad prawa międzynarodowego oraz uniwersalnych wartości, takich jak: demokracja, prawa człowieka i wolności obywatelskie;
- zapewnienie bezpieczeństwa powszechnego poprzez doskonalenie krajowego systemu ratowniczo-gaśniczego oraz systemu monitorowania, powiadamiania ostrzegania o zagrożeniach i likwidowania skutków klęsk żywiołowych oraz katastrof, a także wdrożenie rozwiązań prawnych i organizacyjnych w zakresie systemu ochrony ludności oraz obrony cywilnej;
- doskonalenie i rozwój krajowego systemu zarządzania kryzysowego dla zapewnienia jego wewnętrznej spójności i integralności oraz umożliwienia niezakłóconej współpracy w ramach systemów zarządzania kryzysowego organizacji międzynarodowych, których polska jest członkiem;
- ochrona granic Polski, stanowiących zewnętrzną granicę UE;
- przeciwdziałanie przestępczości zorganizowanej, w tym gospodarczej;
- ochrona porządku publicznego;
- udoskonalenie rozwiązań systemowych dla przeciwdziałania i zwalczania terroryzmu i proliferacji broni masowego rażenia;
- zapewnienie bezpiecznego funkcjonowania Polski w cyberprzestrzeni;
- zapewnienie bezpiecznych warunków rozwoju kapitału ludzkiego i społecznego oraz innowacyjności, efektywności i konkurencyjności gospodarki, a także stabilności finansowej państwa;

[25] Por. Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, 2014, s. 10–11.
[26] *Ibidem*, s. 11–12.

- zapewnienie bezpieczeństwa energetycznego i bezpieczeństwa klimatycznego oraz ochrony środowiska, różnorodności biologicznej i zasobów naturalnych, w szczególności zasobów wodnych, a także kształtowanie zagospodarowania przestrzennego kraju w sposób zwiększający odporność na różnorakie zagrożenia, w szczególności militarne, naturalne i technologiczne;
- zapewnienie bezpieczeństwa żywnościowego;
- prowadzenie efektywnej polityki rodzinnej oraz dostosowanie polityki migracyjnej do nowych wyzwań;
- pogłębianie świadomości społecznej w sferze bezpieczeństwa oraz zwiększanie kompetencji obywateli pozwalających na właściwe reagowanie w sytuacjach kryzysowych.

Strategia z 2014 roku określa strukturę systemu bezpieczeństwa narodowego RP, która obejmuje:

- podsystem kierowania, w skład którego wchodzą: „organy władzy publicznej i kierownicy jednostek organizacyjnych, wykonujący zadania związane z bezpieczeństwem narodowym, wraz z organami doradczymi i aparatem administracyjnym oraz procedurami funkcjonowania i stosowną infrastrukturą”[27];
- podsystemy wykonawcze, które stanowią „siły i środki przewidziane do realizacji zadań w obszarze bezpieczeństwa narodowego, pozostające w dyspozycji organów kierowania bezpieczeństwem”[28]. Dokonano ich podziału na podsystemy operacyjne (podsystem obronny[29] i podsystemy ochronne[30]) oraz podsystemy wsparcia (społeczne[31] i gospodarcze[32]). Wskazano, że podsystemy operacyjne przeznaczone są do wykorzysty-

[27] Dodano także, że w skład podsystemu kierowania SBN RP wchodzi zarządzanie kryzysowe. Zob. *ibidem*, s. 13.

[28] *Ibidem*.

[29] Do podsystemu obronnego zaliczono: dyplomację, Siły Zbrojne RP oraz służby specjalne i przemysłowy potencjał obronny. Szerzej zob. *ibidem*, s. 45–47.

[30] Do podsystemów ochronnych zaliczono: wymiar sprawiedliwości, służby specjalne, instytucje przeciwdziałania i zwalczania terroryzmu i ekstremizmu, instytucje właściwe do spraw cyberbezpieczeństwa, instytucje ochrony informacji niejawnych, instytucje ochrony infrastruktury krytycznej, służby porządku publicznego, służby bezpieczeństwa powszechnego (ratownictwo i ochrona ludności), służby graniczne, służby ochrony najważniejszych organów władzy i administracji publicznej, inne podsystemy ochronne. Szerzej zob. *ibidem*, s. 47–52.

[31] Do podsystemów społecznych zaliczono: system ochrony dziedzictwa narodowego, instytucje edukacji dla bezpieczeństwa, media w systemie bezpieczeństwa narodowego oraz przeciwdziałanie zagrożeniom demograficznym i bezpieczeństwo socjalne. Szerzej zob. *ibidem*, s. 52–54.

[32] Do podsystemów gospodarczych zaliczono: instytucje bezpieczeństwa finansowego, podmioty bezpieczeństwa energetycznego, system rezerw strategicznych, bezpieczeństwo żywnościowe oraz podmioty ochrony środowiska naturalnego i jednostki naukowe. Szerzej zob. *ibidem*, s. 54–56.

wania szans, podejmowania wyzwań, redukowania ryzyk i przeciwdziałania zagrożeniom o charakterze polityczno-militarnym i pozamilitarnym. Z kolei podsystemy społeczne i gospodarcze zasilają je odpowiednimi zdolnościami i zasobami[33].

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 12 maja 2020 roku

Strategia nie definiuje SBN RP, ale jej postanowienia pozwalają wnioskować, że system stanowią: kierownicy działów administracji rządowej, kierownicy urzędów centralnych, wojewodowie, organy samorządu terytorialnego[34] oraz inne siły i środki wykonujące zadania wynikające z osiągania celów strategicznych i interesów narodowych w dziedzinie bezpieczeństwa[35].

Strategia również nie określa wprost misji i celów SBN RP. Uwzględniając interesy narodowe, można pośrednio je wskazać. Misją SBN RP byłoby: „zapewnienie bezpieczeństwa państwa i obywateli, kształtowanie porządku międzynarodowego gwarantującego Polsce bezpieczny rozwój, umacnianie tożsamości narodowej i strzeżenie dziedzictwa narodowego, jak również zapewnienie warunków do trwałego i zrównoważonego rozwoju społecznego i gospodarczego oraz ochrony środowiska naturalnego”[36]. Celów SBN RP obejmują:

- zapewnienie zintegrowanego zarządzania bezpieczeństwem narodowym, w tym kierowania obroną państwa;
- zapewnienie zdolności do szybkiej adaptacji do nowych wyzwań i zagrożeń oraz do identyfikacji szans;
- podniesienie odporności państwa na zagrożenia (w tym hybrydowe), poprzez tworzenie systemu obrony powszechnej;
- wzmocnienie zdolności operacyjnych Sił Zbrojnych RP do odstraszania i obrony przed zagrożeniami bezpieczeństwa, ze szczególnym uwzględnieniem podniesienia poziomu mobilności i modernizacji technicznej;
- podniesienie poziomu odporności na cyberzagrożenia;
- zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym oraz prywatnym;

[33] W strategii podkreślono, że sektor społeczny i gospodarczy oprócz pełnienia funkcji zaplecza sił zbrojnych i innych służb mundurowych jest również aktywnym wytwórcą wartości dodanej w dziedzinie bezpieczeństwa narodowego. Szerzej zob. W. Kitler, *Organizacja bezpieczeństwa…*, *op.cit.*, s. 230.

[34] Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2020, s. 37.

[35] *Ibidem*, s. 11.

[36] *Ibidem*.

- wzmocnienie zdolności Sojuszu Północnoatlantyckiego i Unii Europejskiej do zapewniania bezpieczeństwa Polski oraz całego obszaru euroatlantyckiego;
- rozwinięcie współpracy w formule bilateralnej, regionalnej oraz w wymiarze globalnym na rzecz wzmocnienia pozycji Polski jako istotnego elementu systemu bezpieczeństwa międzynarodowego;
- wzmocnienie tożsamości narodowej, zakorzenionej w chrześcijańskim dziedzictwie i uniwersalnych wartościach;
- wzmacnianie pozytywnego wizerunku RP oraz jej atrakcyjności kulturowej i gospodarczej;
- poprawa warunków do ochrony i rozwoju rodziny;
- skoordynowanie polityki migracyjnej z polityką gospodarczą, społeczną i polityką bezpieczeństwa;
- wzmocnienie bezpieczeństwa zdrowotnego, ekonomicznego oraz ekologicznego;
- zapewnienie bezpieczeństwa energetycznego państwa, opartego o tradycyjne źródła energii, poprzez tworzenie warunków do rozwoju ich alternatyw;
- zagospodarowanie kapitału ludzkiego oraz potencjału naukowego i technologicznego do rozwoju gospodarczego kraju.

Podsumowanie

Analizy rozpatrywanych dokumentów strategicznych wskazują wzajemnie powiązane i skoordynowane elementy (podsystemy) kierowania i wykonawcze, których działania wynikają z misji i celów strategicznych. W rozpatrywanym okresie podejmowane były również rozważania teoretyczne, których przedmiotem była m.in. struktura SBN. Najczęściej poglądy teoretyczne w zakresie koncepcji systemu bezpieczeństwa narodowego rozróżniają podsystem kierowania wraz z różnymi rozwiązaniami w zakresie podsystemów (elementów) wykonawczych. Można je ująć w dwóch grupach

Wariant 1:

- nadrzędny podsystem kierowania (przede wszystkim władza wykonawcza – prezydent i administracja publiczna)[37];

[37] Działanie systemu kierowania SBN należy traktować jako specyficzny przejaw kierowania określany zarządzaniem – tj. decydowanie o zachowaniach innych, dysponowanie zasobami, planowanie, organizowanie, monitorowanie i kontrolowanie przedsięwzięć. Atrybutem zarządzania w administracji publicznej jest posiadanie przez zarządzającego władzy, której źródłem jest prawo do dysponowania zasobami wykonawczymi. Dodatkową rolą jest koordynacja działań wszystkich elementów systemu.

- podsystemy wykonawcze:
  - ochronno-obronny – inaczej interwencyjny, mający na celu przygotowanie zapobieganie i reagowanie na sytuacje kryzysowe oraz militarne;
  - społeczny – jego celem jest przygotowanie zasobów ludzkich, społeczeństwa, jego morale i patriotyzmu;
  - gospodarczy – odpowiedzialny za przygotowanie i utrzymywanie materialnych i finansowych podstaw bezpieczeństwa.

Wariant 2:

- naczelny podsystem kierowania bezpieczeństwem narodowym;
- podsystemy wykonawcze, składające się z:
  - podsystemu obronnego;
  - zbioru (wielu odrębnych) podsystemów ochronnych[38];
  - zbioru podsystemów społecznych[39];
  - zbioru podsystemów gospodarczych[40].

Przedstawione rozwiązania mogą również występować w układzie hierarchicznym zgodnie z ustrojem terytorialnym państwa, tworząc wojewódzki, powiatowy oraz gminny system bezpieczeństwa.

Niezależnie od rozpatrywanych wariantów, warunkowanych cechami podsystemów wykonawczych, kształt podsystemu kierowania SBN wynika z obowiązującego systemu prawnego. Aktualny kształt podsystemu kierowania w SBN RP charakteryzuje się podziałem swoich wewnętrznych elementów organizacyjnych na podmioty: decyzyjne, opiniodawczo-doradcze oraz sztabowe. Prezydent RP i Rada Ministrów jako organy władzy wykonawczej pełnią funkcję decydentów politycznych w podsystemie kierowania. Organami doradczymi (opiniodawczo-doradczymi) są: Rada Bezpieczeństwa Narodowego[41] (dla prezydenta RP) oraz Komitet Rady Ministrów do spraw Bezpieczeństwa Narodowego i spraw Obronnych[42] (dla Rady Ministrów). Z kolei organami sztabowymi są: Biuro Bezpieczeństwa Narodo-

Zarządzanie cechuje się funkcją egzekutywy w całym systemie bezpieczeństwa narodowego (czyli władzą bezpośrednio zarządzającą sprawami państwa).

[38] Przykładowo, podsystem ochrony państwa i porządku konstytucyjnego, podsystem ochrony granicy państwowej, podsystem ochrony infrastruktury krytycznej, podsystem bezpieczeństwa publicznego, podsystem ochrony danych osobowych, podsystem ochrony środowiska naturalnego. Szerzej zob. W. Kitler, *Organizacja bezpieczeństwa…*, *op.cit.*, s. 239.

[39] Przykładowo, podsystem edukacji na rzecz bezpieczeństwa, podsystem nauki i szkolnictwa wyższego, podsystem ochrony dziedzictwa narodowego. Szerzej zob. *ibidem*, s. 239–240.

[40] Przykładowo, podsystem rezerw strategicznych, podsystem bezpieczeństwa finansowego państwa, podsystem ochrony zdrowia, przemysł obronny. Szerzej zob. *ibidem*, s. 240.

[41] Organem doradczym Prezydenta Rzeczypospolitej w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa jest Rada Bezpieczeństwa Narodowego. Zob. art. 135 Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku, Dz.U. Nr 78, poz. 483 ze zm.

[42] Ustanowiony zarządzeniem nr 162 Prezesa Rady Ministrów z 9 października 2020 r. w sprawie Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego i spraw Obronnych. Stanowi organ

wego (na rzecz prezydenta RP) oraz Rządowe Centrum Bezpieczeństwa (na rzecz Rady Ministrów).

W pełni zintegrowany, spójny i uporządkowany system bezpieczeństwa narodowego stanowi podstawę do osiągania celów strategicznych państwa oraz jego interesów narodowych. Dynamika zagrożeń i wyzwań, które niejednokrotnie determinują konieczność wprowadzania zmian w SBN, wskazuje na konieczność przyjmowania różnych koncepcji budowy i funkcjonowania SBN. Ogólny kształt systemu powinien mieć jednak charakter stały ze względu na kompleksowy wymiar bezpieczeństwa oraz konieczność zaangażowania wszystkich obszarów funkcjonowania państwa.

Bibliografia

Akty prawne i dokumenty

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku, Dz.U. Nr 78, poz. 483 ze zm.

Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022", M.P. poz. 377.

Zarządzenie nr 162 Prezesa Rady Ministrów z 9 października 2020 r. w sprawie Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego i spraw Obronnych, M.P. poz. 918.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej z 2003 roku.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2007.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2014, https://www.bbn.gov.pl/ftp/SBN%20RP.pdf.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.

Strategia rozwoju kraju 2020, Ministerstwo Rozwoju Regionalnego, Warszawa 2012.

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczpospolitej Polskiej 2022.

Literatura

Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, AON, Warszawa 2011.

Kitler W., *Organizacja bezpieczeństwa narodowego Rzeczypospolitej Polskiej. Aspekty ustrojowe, prawno-administracyjne i systemowe*, Wydawnictwo Adam Marszałek, Toruń 2018.

Netografia

Http://www.nowastrategia.org.pl/analiza-krytyczna-srsbn/.

Https://rpo2007-2013.slaskie.pl/zalaczniki/2014/01/17/1389965536.pdf.

doradczy Rady Ministrów, rozpatruje i przedkłada jej koncepcje rozwiązań w obszarze bezpieczeństwa narodowego w ujęciu ogólnopaństwowym.

Streszczenie

Kształtowanie koncepcji systemu bezpieczeństwa narodowego RP na przestrzeni ostatnich 20 lat miało swoje odzwierciedlenie w dokumentach strategicznych, które w większym lub mniejszym stopniu określały charakterystykę oraz elementy składowe tego systemu. Analiza strategii bezpieczeństwa obowiązujących w latach 2000–2020 pozwala zauważyć różne podejście do postrzegania systemu bezpieczeństwa narodowego RP. Jego strukturalny charakter ewoluował od aspektu obronności, aż do struktury i obszarów zawierających niemal wszystkie dziedziny funkcjonowania państwa. Pozwala to wyszczególnić jego zasadnicze elementy składowe, którymi są podsystem kierowania i podsystemy wykonawcze. Niezależnie od przyjmowanych koncepcji misja systemu bezpieczeństwa narodowego RP sprowadzała się do zapewnienia korzystnych i bezpiecznych warunków do realizacji interesów narodowych, a jego celem było właściwe przygotowanie i wykorzystanie sił oraz środków będących w dyspozycji państwa do przeciwdziałania zagrożeniom. Struktura system bezpieczeństwa narodowego RP obejmuje całość sił, środków oraz zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa.

Summary

The concept development of the National Security System of the Republic of Poland over the past 20 years has been reflected in strategic documents. Its characteristics and structure has been determined in different scope. The security strategies' analysis shows a different approach to the perception of the National Security System of the Republic of Poland. It gives the possibility to sum up that its structural nature has evolved from the military defence aspects to the structure containing almost all of the state's functioning areas. This allows for the specification of its basic components, which are the control subsystem and the executive subsystems, which perform tasks in the area of national security. The mission of the National Security System of the Republic of Poland is to ensure the favourable and safe conditions for the implementation of national interests. Therefore the main aim of the National Security System is to prepare in a proper manner and use all tools and resources in order to provide the national security and counteract the threats. The National Security System of the Republic of Poland is the entirety of means and resources allocated by the state to perform tasks in the field of security.

Słowa kluczowe

Bezpieczeństwo, bezpieczeństwo narodowe, system bezpieczeństwa narodowego RP, podsystem kierowania, podsystemy wykonawcze, podsystem obronny, podsystemy ochronne, podsystemy wsparcia.

Keywords

Security, national security, the National Security System of the Republic of Poland, control subsystem, executive subsystems, defense subsystem, protection subsystems, support subsystems.

Aleksandra Miler-Zawodniak – dr, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie, ORCID: 0000-0002-0325-4474.
Marcin Zawodniak – dr, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie, ORCID: 0000-0002-5737-4850.

Kazimierz Banasiak

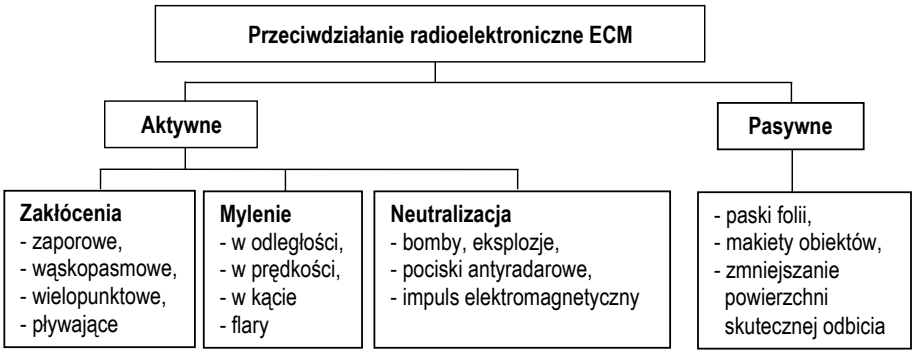
WYBRANE ASPEKTY PRZETWARZANIA POMIARÓW SYGNAŁÓW RADAROWYCH W ZAKRESIE BEZPIECZEŃSTWA ELEKTROMAGNETYCZNEGO

Wprowadzenie

Jednym z komponentów, istotnym dla zapewnienia bezpieczeństwa działań wojsk jest walka radioelektroniczna [1, 3, 4]. Wysoko zautomatyzowane urządzenia i systemy są już od wielu lat integralną częścią wyposażenia samolotów lub okrętów. Walka radioelektroniczna (ang. WRE, EW – Electronic Warfare) obejmuje:

- przeciwdziałanie radioelektroniczne (ang. ECM, Electronic Counter Measures);
- wsparcie radioelektroniczne (ang. ESM, Electronic Warfare Support Measures);
- obronę radioelektroniczną (ang. EPM, Electronic Protective Measures).

Zakres przeciwdziałania radioelektronicznego przedstawiono na rys. 1.



Rys. 1. Metody realizacji przedsięwzięć z zakresu przeciwdziałania radioelektronicznego
Źródło: opracowanie własne.

Cele przeciwdziałania radioelektronicznego ECM realizowane są przez:

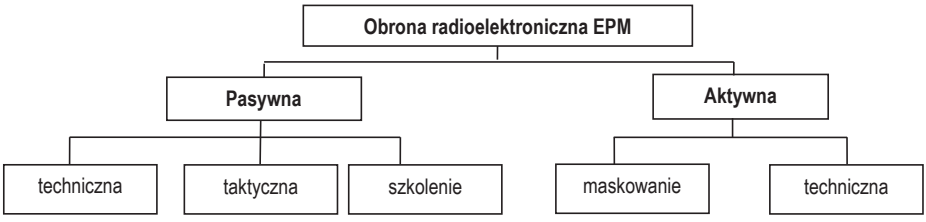
- wytworzenie zakłóceń (czynnych i biernych);
- zmianę właściwości odbijających ochranianego obiektu lub otaczającego go tła, zmianę właściwości ośrodka, w którym rozchodzą się fale elektromagnetyczne.

Rezultatem tych działań jest tło maskujące lub fałszywe zobrazowanie celów na ekranach radarów.

Wsparcie radioelektroniczne obejmuje działania związane z poszukiwaniem, przechwytem i identyfikacją emisji elektromagnetycznych oraz lokalizacją ich źródeł emisji. Głównym zadaniem ESM jest wykorzystanie efektów pracy urządzeń elektronicznych przeciwnika, np. radarów, w celu dostarczenia w czasie rzeczywistym informacji o wykryciu zagrożenia bezpieczeństwa, ostrzeżenia i obrony wojsk własnych [1, 3, 4]. Na polu walki ESM dostarcza przetworzone dane pomiarowe do:

- ostrzegania przed zagrożeniem bezpieczeństwa oraz do identyfikacji zamiaru przeciwnika;
- opracowania i zmiany rozkazu bojowego (ang. Electronic Order of Battle);
- tworzenia i modyfikowania bazy danych (BD);
- selekcji informacji i wspierania dowódcy obrony radioelektronicznej.

Obrona radioelektroniczna obejmuje działania podejmowane w celu efektywnego użycia widma elektromagnetycznego przez siły własne (rys. 2) i zapobieżenie wykorzystania tego widma przez systemy wsparcia i przeciwdziałania przeciwnika [1, 4].



Rys. 2. Diagram podziału w obronie radioelektronicznej

Źródło: opracowanie własne.

W nomenklaturze NATO używane jest również pojęcie kontrprzeciwdziałania radioelektronicznego (ang. ECCM, Electronic Counter-Counter Measuers). Głównymi zadaniami ECCM jest:

- zredukowanie prawdopodobieństwa przechwytu emisji i sygnałów;
- zabezpieczenie przed wykorzystaniem treści przesyłanych informacji;
- zwiększenie odporności na zakłócenia.

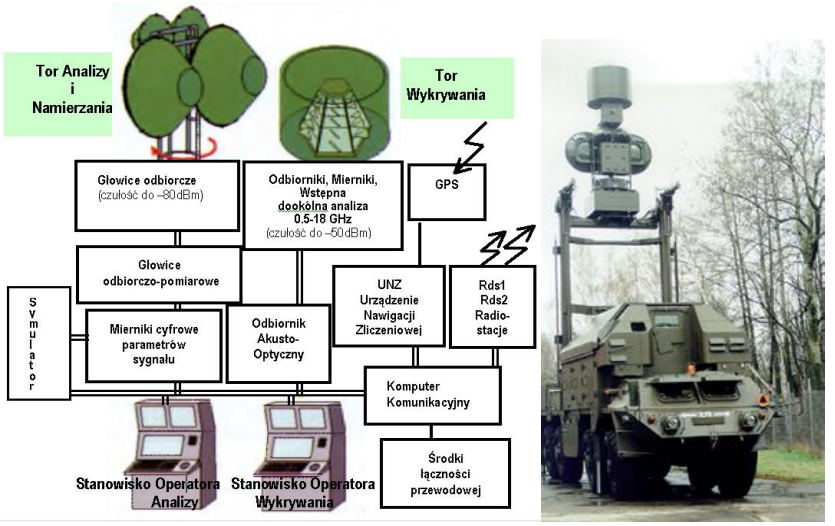
Do walki radioelektronicznej zaliczyć należy także tzw. wywiad sygnałowy (ang. SIGINT, Signal Intelligence), który dostarcza informacji zarówno technicznych, jak i operacyjnych dotyczących przeciwnika oraz informacji uzyskanych z wywiadu radiowego (ang. COMINT, Communications Inteligence) i elektronicznego (ang. ELINT, Electronic Intelligence).

Głównym zadaniem SIGINT jest zdobywanie informacji o przeciwniku w celu wsparcia rozpoznania radioelektronicznego (RRE) i innych operacji. Zadania SIGINT oraz ELINT realizowane są zarówno w czasie pokoju, jak i wojny. Cechują się dłuższym czasem przeznaczonym na analizę i opracowanie uzyskanych danych z racji większej rozległości analizy. SIGINT spełnia podobne zadania jak ESM, jednak są tu istotne różnice w ramach czasowych przeznaczonych na realizację działań oraz ze względu na to, że SIGINT koordynowany jest na poziomie strategicznym.

Przedstawione rozważania dotyczą wybranych aspektów algorytmizacji przetwarzania pomiarów w urządzeniu rozpoznawczym (UR) klasy ESM o wysokim stopniu automatyzacji przetwarzania. UR typu ESM wykorzystują do wykrywania sygnałów impulsowych, generowanych przez różne źródła emisji (ZE), kanał szerokopasmowy z kierunkowymi lub dookólnymi antenami. Przykład pierwszego tego typu, dużego, mobilnego urządzenia rozpoznawczego MUR 20, klasy ELINT/ESM, opracowanego przez Wojskową Akademię Techniczną i Przemysłowy Instytut Telekomunikacji przedstawiono na rys. 3. Urządzenie jest przeznaczone do pracy indywidualnej i systemowej zapewniającej lokalizację wykrywanych źródeł. MUR 20 to inaczej stacja rozpoznania systemów radiolokacyjnych. Jest ona przeznaczona do:

- zautomatyzowanego wykrywania sygnałów impulsowych źródeł emisji, wspierających systemy uzbrojenia w strefie taktycznej w paśmie częstotliwości 0,5–18 GHz (z opcją do 40 GHz);
- automatycznego, monoimpulsowego pomiaru następujących parametrów impulsów:
  - częstotliwości nośnej,
  - czasu przyjścia impulsu,
  - amplitudy średniej impulsu,
  - czasu trwania impulsu,
  - okresu powtarzania (częstotliwości powtarzania);
- standaryzacji informacji pomiarowej do postaci tzw. wektora pomiarowego (WP), przyporządkowanego do każdego, kolejnego, odebranego impulsu;
- przetwarzanie informacji pomiarowej zawartej w ciągu WP;
- automatycznego rozpoznawania wykrytych sygnałów i źródeł ich emisji (ZE);

- zautomatyzowanego określania kierunku (namierzania) na pracujące źródła emisji;
- śledzenia w częstotliwości źródeł emisji wykrytych w paśmie 0,5–18 GHz;
- gromadzenia wyników rozpoznania i danych pomiarowych,
- przekazywania łączem cyfrowym lub fonicznym informacji z rozpoznania.



Rys. 3. System ELINT/ESM MUR 20 – schemat blokowy i widok urządzenia

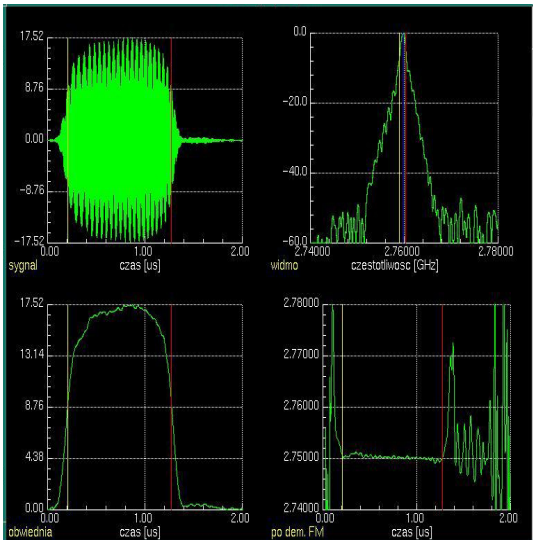
Źródło: opracowanie własne.

W zależności od częstotliwości, pasma, warunków propagacji i miejsca pomiarów możliwy jest wtedy odbiór sygnałów pojedynczych ZE [6, 7] lub jednoczesny odbiór sygnałów wielu ZE [1, 2, 6, 7, 8, 9, 10]. Opracowanie MUR 20 zaowocowało dalszymi wdrożeniami innych, krajowych rozwiązań technicznych.

W rozpoznawaniu jednym z ważnych parametrów jest okres powtarzania impulsów (ang. Pulse Repetition Interval, PRI). Wynika to z podatności pomiarowej, wysokiej dokładności [1, 2] oraz wartości informacyjnej tego parametru. Jedną z jego cech informacyjnych jest występowanie okresowości (cykliczności) zmian wartości PRI [1, 2, 7, 8, 9, 10]. Jednak wykrycie cykliczności bywa utrudnione z uwagi na różnorodne zakłócenia występujące w procesie odbiorczym i pomiarowym [1, 2]. W artykule przedstawiona zostanie idea autorskiego algorytmu określonego mianem algorytmu sekwencyjnego wykrywania cyklu (ASWC) zmian PRI oraz wyniki badań ilustrujące możliwości automatycznego wykrywania cykliczności w warunkach intensywnych zakłóceń.

Zakres przetwarzania deskryptorów ciągu impulsów

Realizowany w UR proces pomiarowy pozwala na przyporządkowanie każdemu impulsowi sygnału sondującego wektora pomiarowego WP (1) jego parametrów czasowych i częstotliwościowych. Na rys. 4 przedstawiono interpretację graficzną parametrów impulsu radarowego. W kolumnie 1 rysunku, w części górnej widoczna jest postać radiowa impulsu, w części dolnej – obwiednia impulsu. Impuls poddawany jest próbkowaniu i cyfryzacji. Na jej podstawie wyznaczane są: czas przyjścia impulsu, czas jego trwania i amplituda impulsu. Obecnie są to dokładności nanosekundowe. W części prawej widoczne są parametry częstotliwościowe. Wykres na rysunku górnym pozwala na wyznaczenie wartości średniej, minimalnej i maksymalnej częstotliwości nośnej. Rysunek dolny pokazuje wewnątrzimpulsowe zmiany częstotliwości (tu częstotliwość ma stałą wartość).



Rys. 4. Impuls radaru i jego parametry czasowe i częstotliwościowe
Źródło: opracowanie własne.

W literaturze WP określany jest również mianem deskryptora impulsu PDW (ang. Pulse Descriptor Words) lub PDV (ang. Pulse Descriptor Vector) [2, 6, 7, 8, 9, 10]. Jego szczegółowa struktura zależy od możliwości pomiarowych konkretnego UR, ale zwykle zawiera takie parametry, jak:

$$\text{WP (PDW)} = \begin{cases} \text{– czas przyjścia impulsu (TOA, time of arrival),} \\ \text{– czas trwania impulsu (PW, PD, pulse width, pulse duration),} \\ \text{– amplituda impulsu (A, amplitude),} \\ \text{– częstotliwość (RF, radio frequency),} \\ \text{– kąt odbioru (AOA, angle of arrival).} \end{cases} \quad (1)$$

W tabeli 1 przedstawiono fragment niezakłóconego ciągu WP sygnału radaru o zmianach PRI typu stagger prosty z czterema wartościami PRI powtarzanymi cyklicznie co Tc = 3,840[ms].

Tabela 1. Fragment jednorodnego ciągu wektorów pomiarowych

$Tc=\sum_{i=1}^{4} TOAi \approx 3.840ms$, Kc=4

Nr	TOA[s]	TOA_{i+1}-TOA_i[ms]	Amp	PW[μs]	Fmin	Fsr[MHz]	Fmax
0	1,0613409	1061,3409	141,0	0,700	2795,863	2807,415	2807,824
1	1,0621698	0,8289	154,0	0,700	2795,863	2808,140	2808,020
2	1,0633461	**1,1763**	176,0	0,900	2796,059	2808,181	2808,216
3	1,0642212	0,8751	200,0	0,900	2796,059	2808,547	2808,716
4	1,0651813	0,9601	212,0	0,900	2796,059	2808,239	2808,316
5	1,0660102	0,8289	232,0	0,900	2796,059	2808,377	2808,520
6	1,0671863	**1,1761**	235,0	0,900	2795,863	2808,273	2808,412
7	1,0680614	0,8751	246,0	1,000	2796,059	2808,510	2808,612
8	1,0690215	0,9601	243,0	1,000	2796,059	2808,303	2808,420
9	1,0698504	0,8289	246,0	0,900	2796,059	2808,181	2808,220
10	1,0710267	**1,1763**	246,0	1,100	2796,059	2807,123	2808,222
11	1,0719016	0,8749	248,0	1,000	2796,059	2808,278	2808,824
12	1,0728617	0,9601	248,0	0,900	2795,275	2807,927	2808,216
13	1,0736906	0,8289	244,0	1,000	2796,059	2808,118	2808,216
14	1,0748667	**1,1761**	252,0	0,900	2795,275	2807,743	2807,824

Źródło: opracowanie własne.

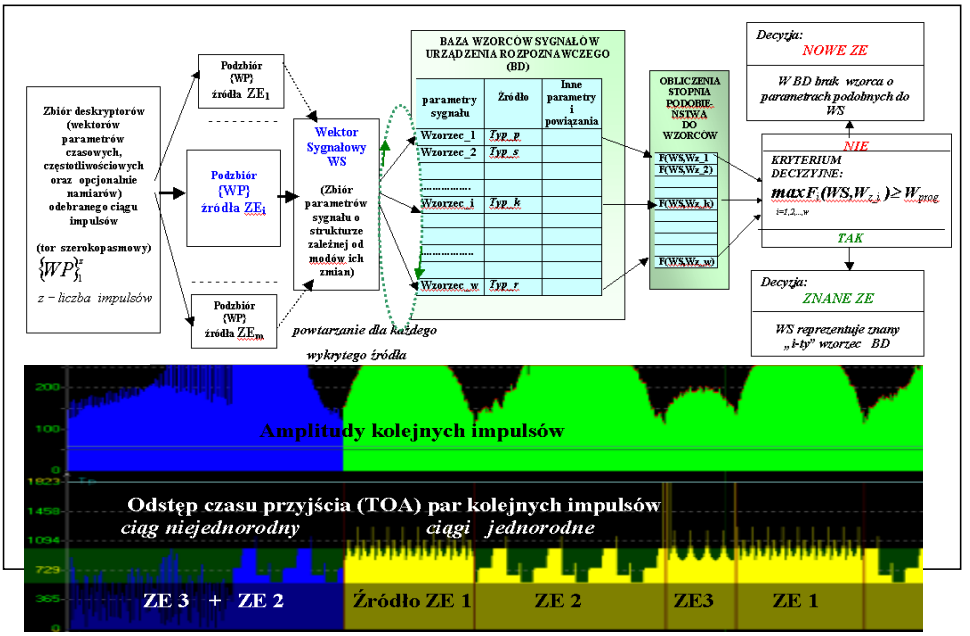
Rozpoznawanie pojedynczego ZE wymaga realizacji następujących etapów (rys. 5):

1) skojarzenia odbieranych ciągów WP z poszczególnymi ZE;
2) określenia odpowiadającego danemu ZE tzw. wektora sygnałowego (WS);
3) porównywania WS z wzorcami bazy danych (BD) systemu rozpoznania;
4) podjęciu decyzji o wykryciu sygnału nowego ZE lub potwierdzeniu pracy znanego.

Proces kojarzenia odbieranych ciągów z poszczególnymi ZE jest określany mianem sortowania sygnałów (signal sorting) lub rozplatania (deinterleaving) [2, 6, 7, 8]. Według jednej z pierwszych prac [1] dotyczącej tej problematyki rozplatanie (deinterleaving pulse train) jest rozumiane jako proces określania liczby ZE i przyporządkowania im ciągów impulsów (deskryptorów) w przypadku, gdy ciągi impulsów poszczególnych ZE są w dużym stopniu „zmieszane", np. tak jak to po-

kazano na rys. 5, dla pierwszej paczki (grupy) impulsów strumienia danych wejściowych (kolor niebieski).

Przedstawiony na rysunku strumień danych jest reprezentowany amplitudami kolejnych impulsów i różnicami czasów przyjścia kolejnych par impulsów (DTOA, Differences TOA). W przypadku braku zakłóceń są to wartości PRI. Ciągi PDW wielu paczek impulsów skojarzone z pojedynczym ZE pozwalają na określenie znacznie szerszej charakterystyki sygnału tego ZE (Interpulse Signal Analysis).



Gdzie: z – liczba wzorców sygnałów w bazie danych,

r – liczba źródeł emisji reprezentowana liczbą „w" wzorców (w ^{3} r),

$F_i(WS,W_{z\_i})$ – wartość miary podobieństwa między zbiorem parametrów WS a i-tym wzorcem BD.

Rys. 5. Etapy przetwarzania pomiarów w urządzeniu rozpoznawczym oraz przykład wejściowego strumienia danych

Źródło: opracowanie własne.

Graficzna prezentacja pomiarów jest często stosowana, ponieważ dla operatora lub analityka prostsza jest interpretacja obrazów (rys. 5) i ich podobieństwa niż szukanie podobieństwa w kolumnach liczb (tabela 1). W wyniku analizy międzyimpulsowej na podstawie wielu paczek impulsów zostają określane parametry tzw. wektora sygnałowego WS (2) (Emiter Deskryptor Vector, EDV) [6].

Ogólna struktura wektora sygnałowego WS jest następująca:

$$\mathrm{WS} = \langle \{D_{PRI}\}, \{D_{R}\}, \{I\} \rangle \qquad (2)$$

gdzie: $\{D_{PRI}\}$ – zbiór parametrów (deskryptor) okresu powtarzania impulsów,

$\{D_{RF}\}$ – zbiór parametrów (deskryptor) częstotliwości nośnej,

{I} – inne parametry sygnału (np. czasu trwania impulsu, parametry i sposób skanowania, polaryzacja, kąt odbioru AOA).

Parametry WS są w dalszym etapie porównywane ze znanymi wzorcami bazy danych (BD) w celu wyznaczenia wzorca o maksymalnej wartości miary oceniającej zgodność parametrów WS i wzorców BD (rys. 5). Dla ustalonej postaci kryterium porównania oraz zasobów BD jakość rozpoznania zależy głównie od liczby uwzględnianych w WS parametrów, dokładności ich estymacji i wagi przy rozpoznawaniu radaru.

Szczegółowa struktura deskryptora powinna uwzględniać najbardziej dystynktywne cechy sygnału sondującego i powinna być dopasowana do sposobu zmian parametrów czasowych i częstotliwościowych sygnału. Należy podkreślić, że poprawne określenie deskryptora D_{PRI} ułatwia określenia deskryptora parametrów częstotliwościowych D_{RF} – szczególnie w zakresie określenia kolejności zmian wartości częstotliwości RF, co w efekcie wpływa na poprawność rozpoznania.

Zakres przetwarzania danych w ciągu PDW sygnału od pojedynczego ZE zależy od złożoności zmian parametrów PRI i RF (rys. 6) w sygnale. Sposób przetwarzania oraz algorytmy powinny zapewnić identyfikację modu (sposobu) zmian parametru oraz dostosować strukturę WS tak, żeby możliwe było reprezentowanie zmian parametrów (rys. 7a, 7b, 8), jeśli jego wartość jest:

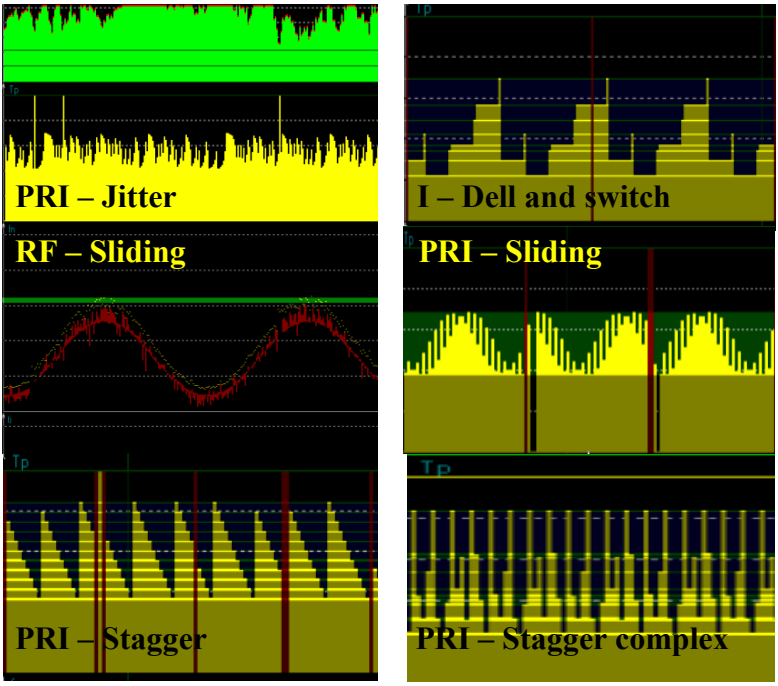
- stała (constant);
- fluktuująca (jitter);
- zmieniana z dyskretem czasu (dwell and switch) – zmiany o charakterze skokowym;
- zmieniana w sposób płynny (sliding) – zmiany liniowym lub nieliniowym);
- zmieniana przemiennie (stagger) – ustalona liczba wartości w określonym porządku;
- losowa (random) – duża liczba dyskretnych wartości powtarzalnych (lub nie) w długim cyklu;
- fluktuująca (w pewnym zakresie, zmiany ciągłe lub dyskretne, jitter).

W niektórych z wymienionych rodzajów zmian PRI można jeszcze wyróżnić podklasy. Złożoność zmian PRI z jednej strony komplikuje proces analizy wyników pomiarów i stawia przed algorytmami wymóg adaptacji w stosunku do aktualnej sytuacji pomiarowej, z drugiej – potencjalnie pozwala na zwiększenie rozróżnialności sygnałów, a w efekcie także typów a nawet egzemplarzy sprzętu. W najprostszym przypadku dla rozpoznania radaru na podstawie ciągu PDW można wyznaczyć tylko statystyczne wartości PRI i RF. Jednak przy dużej liczbie wzorców BD wynik rozpoznania może być niejednoznaczny, bo różne radary mogą

mieć podobne parametry, a różnią się np. tylko kolejnością występowania wartości PRI (RF), a uwzględnienie tego w WS zwiększa możliwość rozróżniania egzemplarzy sprzętu.

Z przedstawionych rozważań wynika, że dla wykorzystania cech sygnałów sondujących algorytmy przetwarzające ciągi PDW powinny zapewniać:

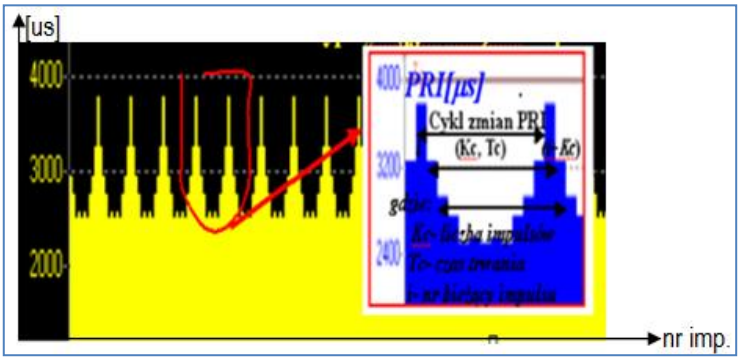
- wykrywanie w ciągu PDW faktu istnienia cyklu zmian PRI;
- określenie parametrów (Kc, Tc) tego cyklu.



Rys. 6. Przykładowe mody zmian parametrów PRI i częstotliwościowych w ciągach impulsów
Źródło: opracowanie własne.

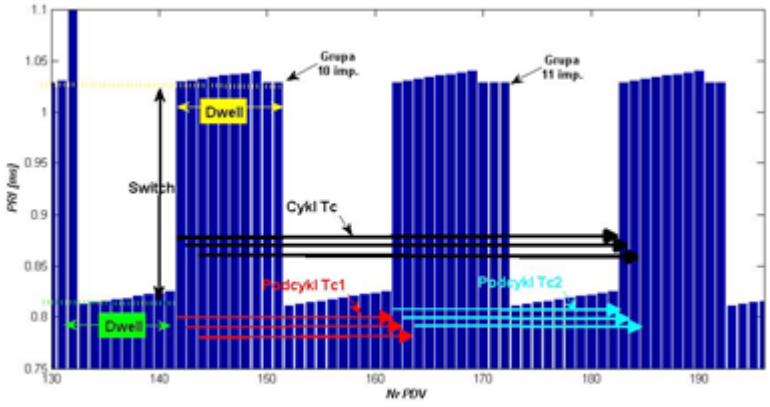
Przez pojęcie cyklu zmian PRI (stagger frame) rozumiane jest okresowe powtarzanie się w sygnale sekwencji wielu różnych wartości PRI (level staggered). Parametrami cyklu są: okres – Tc oraz jego długość Kc, określająca liczbę wartości PRI w cyklu, które nie muszą być różne. Interpretację cyklu PRI w niezakłóconym ciągu impulsów z przemiennym, złożonym PRI (stagger complex) o parametrach Kc = 12, Tc ≈ 34.200 ms i różnych 6 wartościach PRI_1, PRI_2,…, PRI_6 pokazano na rys. 7a. Ogólna struktura cyklu nie odzwierciedla pełnej zawartości informacyjnej. Niektóre z wartości PRI mogą występować w cyklu wielokrotnie. Mogą występować na różnych, kolejnych pozycjach, mogą też występować jedno- lub wielokrot-

nie. Dlatego długość cyklu Kc nie może być utożsamiana z liczbą wartości PRI. Tego rodzaju cykle są określane jako złożone (np. stagger complex).



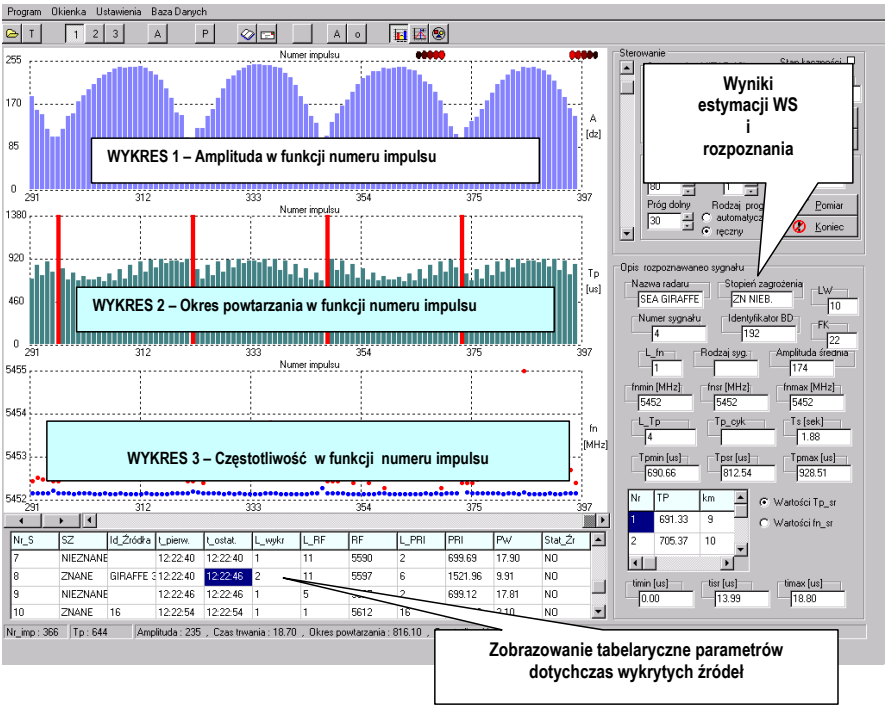
Rys. 7a. Interpretacja cyklu PRI w ciągu impulsów sygnału typu stagger complex
Źródło: opracowanie własne.

Przykład długiego (41 wartości PRI) cyklu o zmianach typu dwell and switch przedstawiono na rys. 7b. Tu występują grupy wartości PRI liczące 10, 11 lub 12. Dodatkowo występują podcykle. Dlatego w przedstawianym przykładzie cykl jest długi i zawiera 41 wartości PRI, a jego czas Tc to około 36.0 [ms].



Rys. 7b. Interpretacja cyklu PRI w ciągu ze zmianami PRI typu dwell and switch
Źródło: opracowanie własne.

Praktycznie estymowane parametry czasowe i częstotliwościowe są w urządzeniach rozpoznawania prezentowane za pomocą interfejsów graficznych (ekranowych). Przykład przedstawiono na rys. 8. Użyte oznaczenie Tp (czas powtarzania impulsów) odpowiada oznaczeniu PRI obecnie stosowanemu.



Rys. 8. Przykład zobrazowania ciągu WP, estymacji parametrów sygnału oraz wyniku rozpoznania
Źródło: opracowanie własne.

Zakłócenia procesu akwizycji pomiarów

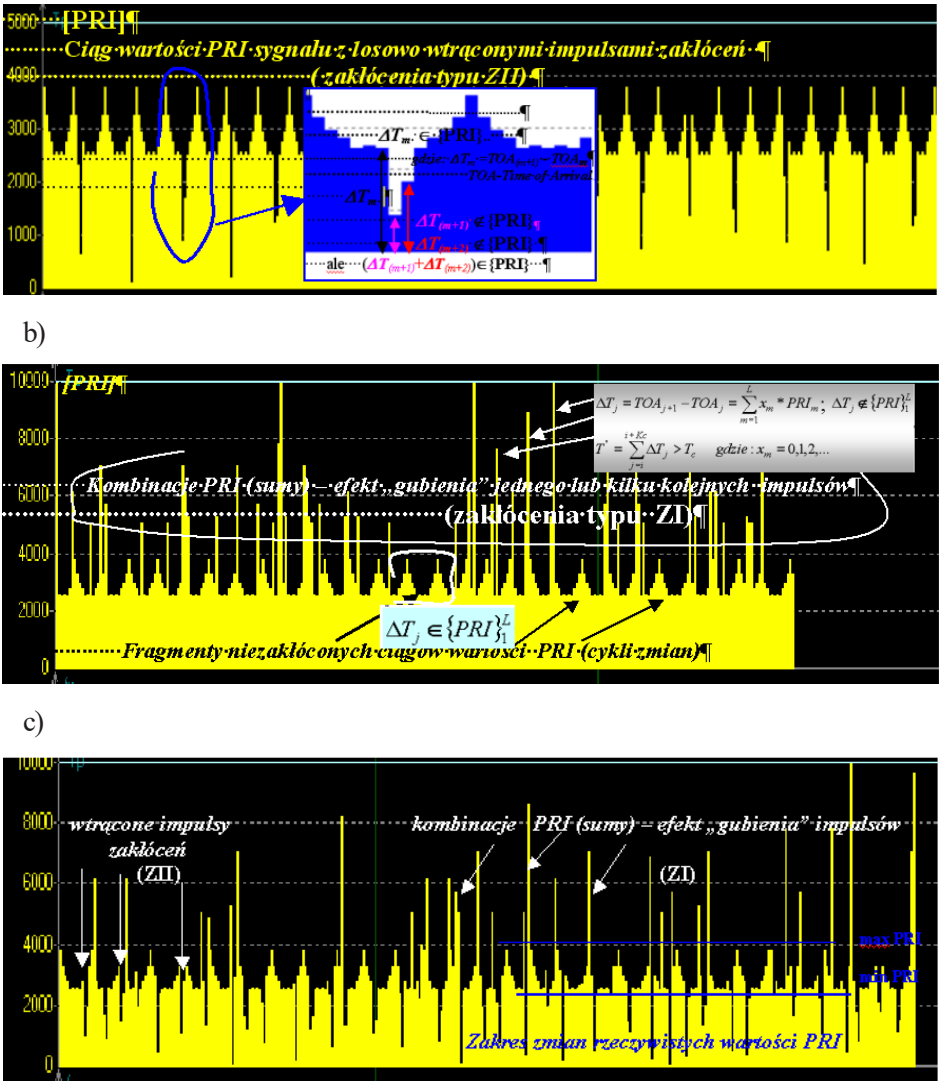
W praktyce automatyczne wykrycie cyklu PRI jest utrudnione ze względu na zakłócenia w odbiorze sygnałów i przy pomiarze PDW ich impulsów. Zakłócenia [1, 2, 3] wynikają z:

- odbioru sygnałów odbitych (wielodrogowość) (ang. multi path);
- relacji między wartością energii impulsów i progami wykrywania;
- zmian częstotliwości sygnału (ang. frequency agile);
- błędów rozplatania całkowicie wymieszanych ciągów impulsów różnych ZE.

Na rys. 9 przedstawiono interpretację symulowanych zakłóceń w odniesieniu do cyklicznego ciągu (350 impulsów) sygnału rzeczywistego przedstawionego wcześniej na rys. 7a.

Efekty zakłóceń widoczne na rys. 9b mogą być rozpatrywane jako „gubienie" (missing) impulsów, określane dalej, jako zakłócenia typu ZI.

a)



b)

c)

Rys. 9. Interpretacja zakłóceń w analizowanych ciągach impulsów
Źródło: opracowanie własne.

Wówczas odstęp między czasami przyjścia kolejnych, odebranych impulsów (Differences TOA) nie odpowiada wartości PRI, gdyż jest sumą (kombinacją liniową) dwu lub więcej wartości PRI. W procesie odbiorczym mogą wystąpić również przypadkowe impulsy zakłóceń (np. atmosferycznych czy też z pracy urządzeń sąsiednich). Ich efekty mogą być też interpretowane jako widoczne na rys. 9a „wtrącenia" impulsów – dalej określane, jako zakłócenia ZII. Powodują one zwykle

przypadkowe „dzielenie" rzeczywistych wartości PRI najczęściej na dwie wartości, których suma jest wartością PRI.

Z przedstawionych na rys. 10 wykresów widać, że znacznie pogorszyły się warunki pozwalające na identyfikację cyklu oraz poprawne określenie zbioru wartości PRI. Szczególnie jest to widoczne w przypadku intensywnych zakłóceń ZI na rys. 10b oraz w przypadku jednoczesnego występowania zakłóceń ZI i ZII (rys. 10c), gdzie wydaje się, że wykrycie cykliczności jest niemożliwe.

Identyfikacja zakłóceń i wartości PRI w ciągach impulsów

Dla ciągu WP (r = 1, 2, ..., z, z – liczba PDW) można określić różnice czasów przyjścia dla różnych par impulsów odległych o zadaną liczbę całkowitą „k" impulsów. Wówczas zostanie określony zbiór {ΔTj(k)} odstępów czasu między impulsami (TOA Differences Histogram) o elementach:

$$\Delta Tj(k) = \Delta Tr,s = TOAs - TOAr \qquad (3)$$

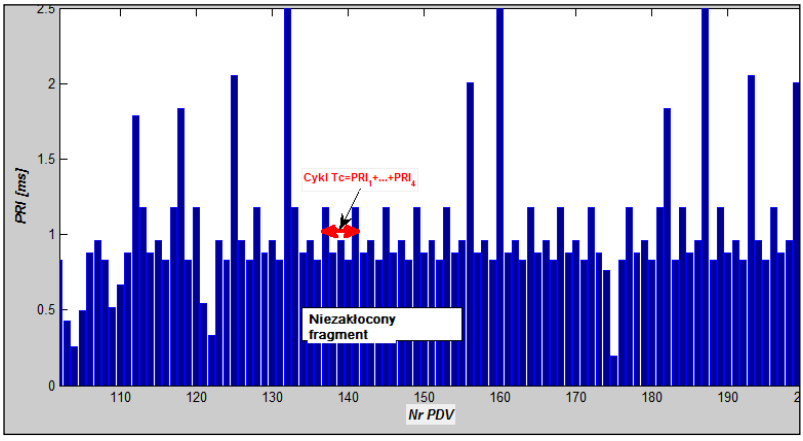
gdzie: TOA – czas przyjścia impulsów o numerach s i r,

r = 1, 2, 3, ..., (z−k), s = (r + k),

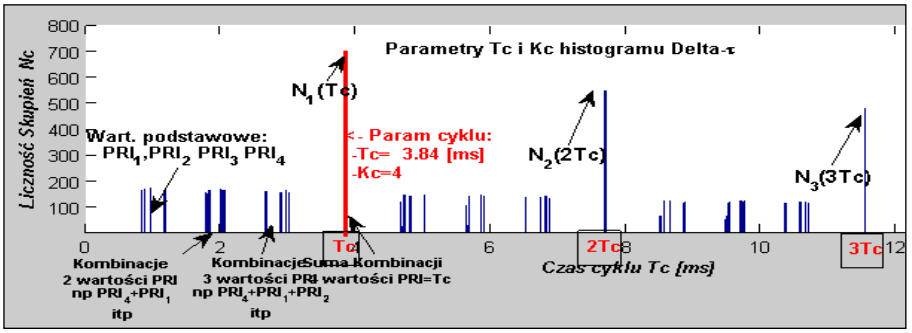
z – liczba PDW, $j \in [1, 2, 3, ..., (z-k)]$.

Dla ustalonej wartości „k" jest on też określany jako SDIF (Sequential Difference Histogram) [2, 6]. Może też być interpretowany jako wiersz macierzy Delta-τ [1] odległości czasowej impulsów. Dla zadanej wartości „k" liczba odstępów $\Delta Tr,s$ wyniesie (z−k). Przykład histogramu Delta-τ dla fragmentu niezakłóconego ciągu impulsów około 700 impulsów ze zmianami PRI typu stagger z rys. 10a pokazano na rysunku 10b. Niezakłócony fragment takiego ciągu WP przedstawiono w tabeli 1.

a)



b)



Rys. 10. Fragment parametrów ciągu impulsów z zmianami typu stagger oraz struktura i interpretacja histogramu Delta-τ. dla długiego ciągu impulsów o krótkim cyklu Kc = 4 i Tc ≈ 3.840 ms

Źródło: opracowanie własne.

W tabeli 2 przedstawiono zbiory skupień (3) dla zakłóconego intensywnie ciągu z rys. 10c. Kolumny 2 i 3 to parametry skupień dla k = 1 (między kolejnymi impulsami), natomiast zbiory skupień w kolumnach 5 i 6 to parametry skupień dla k = 2 (czyli między co drugimi impulsami). Analiza relacji wartości średnich skupień d_i^k i ich liczności n_i^k umożliwia:

- identyfikację skupień, które są wartościami zbioru {PRI};
- identyfikację występowania zakłóceń i ich rodzaju (wynika to z relacji niebieskich i czerwonych);

Wartości PRI to w pierwszej kolejności wartości występujące tylko w kolumnie 2 (zielone), ponadto jeśli w ciągu pomiarowym dla k = 1 i k = 2 są zbliżone wartość skupień ($d_i^{k=1} \approx d_j^{k=2}$) w kolumnie 2 i 5, to jeśli liczność skupienia dla k = 1 (w kolumnie 2) jest dominująca (relacje czerwone), to oznacza, że są obecne zakłócenia ZII, a wartość $d_i^{k=1}$ jest również wartością PRI (tzn. $d_i^{k=1} \in \{PRI\}$). Istotę takiej analizy, realizowanej automatycznie, przedstawiono w tabeli 2.

Przykładowo w kolumnie 2, wiersz 2 tabeli odstęp między impulsami wynosi 2,5110 ms, a częstość jego występowania w ciągu to 44 razy. Najbardziej zbliżony do niego jest odstęp w kolumnie 5 w wierszu 11, ale jego częstość wynosi tylko 5. Korzystając z relacji logicznych, ustalamy, że 2,5110 ms to wartość PRI i jednocześnie wiemy, że w sygnale były zakłócenia typu ZII i stąd się wzięła wartość 2,5110 ms w kolumnie 6, jako odstęp między niekolejnymi impulsami (tzn. dla k = 2). Taka automatyczna analiza pozwala w sposób pewny odfiltrować zbiór wartość PRI, tak jak to pokazano w kolumnie 4.

Tabela 2. Przykład zbiorów skupień (dla ciągu impulsów z rys. 9c) oraz interpretacja relacji między skupieniami przy identyfikacji rodzaju zakłóceń oraz zbioru wartości PRI

	dla k=1			**dla k=2**		
	Skupienia odstępów między kolejnymi impulsami (k=1) $\Delta Ti = TOA\ i_{i+1} - TOA\ i$	*Liczności skupień*		*Skupienia odstępów między niekolejnymi impulsami (k=2)* $\Delta Ti = TOAi_{+2} - TOA\ i$	*Liczności skupień*	
	$\mathbf{d_i^{k=1}}$ *[ms]*	$\mathbf{n_i^k}$		$\mathbf{d_i^k}$ *[ms]*	$\mathbf{n_i^k}$	
1	**2.5500**	45	PRI_1	5.0490	39	→ZI=True
2	**2.5110**	44	PRI_2	5.0610	37	→ZI=True
3	**3.2455**	40	PRI_3	5.2730	34	
4	**2.7620**	39	PRI_4	6.1680	33	
5	**2.9225**	37	PRI_5	7.0326	27	→ZI=True
6	**2.4990**	22	PRI_6	5.6845	26	→ZI=True
7	**3.7870**	18	PRI_7	8.9303	9	
8	6.1682	9	*Kombinacja PRI*	2.7620	8	→ZII=True
9	7.0328	8	-II-	9.9554	7	→ZII=True
10	5.6853	8	-II-	2.9222	6	
11	5.0612	7	-II-	2.5110	5	→ZII=True
12	5.0490	6	-II-	7.5600	5	
…	…	…		…	…	
Łącznie 93 skupienia				***Łącznie 103 skupienia***		

Źródło: opracowanie własne.

Z kolei znajomość rodzaju zakłóceń i wartości PRI daje możliwość wykrycia cyklu. Podstawą jest tu sekwencyjne badanie skupień dla impulsów, między którymi liczba różnych odstępów wynika z zadawanego k = 3, 4, 5, …, itd. Znając rodzaj zakłóceń na każdym etapie k-tym badane są relacje ilościowe i powiązanie skupień (3) ze zbiorami {PRI}.

Wykrywanie cykliczności zmian PRI w ciągach impulsów

Metoda wykorzystująca histogram Delta-τ

Do wyznaczania cykliczności zmian PRI najprostszym rozwiązaniem jest algorytm wykorzystujący pełny, wspomniany histogram Delta-τ. Otrzymane wówczas skupienia (3) reprezentują wszystkie kombinacje odstępów czasu między impulsami. Wówczas, jeżeli w ciągu występuje cykl, to jego długość Tc określa najbardziej liczne skupienie j* (prążek – przykład rys. 10b), tzn.:

$$T_c = d_{j*} \qquad (4)$$

gdzie:

j^* – numer skupienia dla którego osiągnięto $n_{j*} = n_i$, $i = 1, 2, \ldots, m$;

m – ilość skupień otrzymana dla liczby $0{,}5(z^2 - z)$ skupianych odstępów $\Delta Tr,s$ ($r, s = 1, 2, \ldots, z$, $s > r$).

Znając Tc, można w wyniku dalszej analizy wyznaczyć Kc. Wadą tej metody jest:

- bardzo duża liczba obliczeń i zajętość pamięci (złożoność kwadratowa algorytmu $O(z) = z^2$);
- brak możliwości bezpośredniego wyznaczenia Kc;
- skupienie najliczniejsze nie zawsze odpowiada wartość Tc ze względu na zakłócenia, rozdzielczość skupiania i występowanie prążków subharmonicznych.

Metoda wykorzystująca histogram SDIF

Innym sposobem może być etapowe (sekwencyjne) skupianie odstępów czasu między impulsami według (3) dla wszystkich wartości „k" (k = 1, 2, 3, ... (z−k) (difference level). Wówczas jest złożoność liniowa algorytmu proporcjonalna do z (liczby impulsów). Wynikiem są wówczas zbiory skupień (podobne jak w tabeli 2) dla każdego etapu „k". Po zrealizowaniu wszystkich etapów można wyznaczyć parametry (Tc, Kc). Wartość Tc jest określona przez wartość d_{j*} o największej liczności skupienia z wszystkich etapów (maksymalny prążek). Metoda wymaga pamiętania dużych zbiorów.

Algorytm sekwencyjnego wykrywania cyklu i wyniki badań

Sekwencyjny algorytm wykrywania cykliczności SAWC bazuje na zasadzie SDIF. Główna różnica polega na ograniczeniu liczby etapów poszukiwania do liczby określającej długość cyklu (tzn. k = Kc). Nie ma też konieczności pamiętania dużych zbiorów danych. Ograniczenie zakresu górnego poszukiwania wymaga, by na każdym etapie podjąć decyzję o wykryciu cyklu i zakończeniu poszukiwania lub o kontynuacji. Wymaga to zdefiniowania wskaźnika W(Tc, k), wykrycia cyklu dla danego etapu k. Takie wskaźniki zostały zdefiniowane i omówione szerzej w [8, 10]. Ocena wykrycia powinna dotyczyć wartości Tc, gdyż wartość Kc będzie zgodna z numerem „k" bieżącego etapu. Obliczając wartość wskaźnika i porównując ją z progiem (wartość około 0.9), można rozstrzygnąć o dalszym przebiegu obliczeń. Wskaźnik wykrycia cyklu (5) bazuje na informacji zawartej w zbiorach skupień (3) z każdego etapu „k" i relacjach tych zbiorów ze zbiorami PRI oraz ich kombinacjami.

Wykrycie cyklu (5) w niezakłóconym ciągu impulsów nie nastręcza trudności (jedno skupienie j^*, określona wysoka liczność $n_{j*}{}^k$). W przypadku występowania zakłóceń zbiory nie mają tych własności. Tak więc własności ciągu niezakłóconego mogą być przyjęte jako punkt odniesienia. Dla takich sytuacji zdefiniowano wskaźnik skojarzenia (6) skupień W_{sk} [8, 10]. Należy również nadmienić, że na bieżącym

etapie rozważań dysponujemy informacją o wariancie zakłóceń (ZI, ZII) w analizowanym ciągu – stąd też w procesie decyzyjnym wiadomo, jakich własności należy oczekiwać. Na przykład, jeżeli zidentyfikowano w ciągu tylko zakłócenia ZI, to etap „k", na którym liczność pierwszego skupienia nie jest największa, to parametr k nie wyznacza długości cyklu Kc i poszukiwania należy kontynuować.

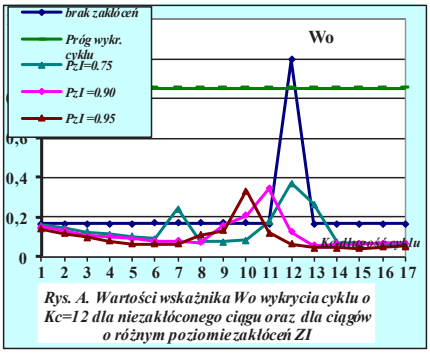
Podstawowym ciągiem badanym był ciąg z rys. 7a – zawierający 350 impulsów o parametrach cyklu: Kc = 12 i Tc = 34,268 ms. Taki niezakłócony ciąg generuje w histogramie Delta-T najwyższy prążek odpowiadający skupieniu o wartości Tc = 34,268 ms i liczności 338 odstępów czasu (bo 350 – Kc = 338). Na wykresach wyników badań, zamieszczonych na rys. 10a, 10b, ten prążek powoduje, że wartości wskaźników wykrycia cyklu W_0(Tc, Kc = 12) przyjmują wartości maksymalne równe 1,0 (kolor granatowy). Wskaźnik Wo to najogólniej iloraz liczności skupienia dominującego n_{j*}^k dla *k*-tego etapu podzielonej przez liczbę możliwych odstępów między impulsami badanego ciągu:

$$Wo(Tc= d_{j*}, k) = \max n_{j*}^k / (z - k) \qquad (5)$$

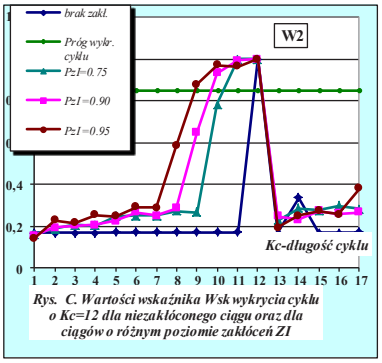
Inne warianty badań wskaźnika W_0(Tc, Kc = 12) uzyskiwano, zakłócając losowo (równomiernie) dane pomiarowe z wariantu podstawowego ciągu. Poziom zakłóceń np.: PzI = 0.75 (z rys. 10a) jest rozumiany jako utrata 75% liczność skupienia maksymalnego uzyskiwanego w sygnale niezakłóconym, czyli zamiast 338 było tylko 85 wartości tworzących skupienie dominujące. W podobny sposób wygląda to przy bardzo silnych zakłóceniach PzI = 0,90 i 0,95. Ze wzrostem poziomu zakłóceń wartość wskaźnika Wo(Tc, k) gwałtownie spada i jest mniejsza niż 0,4. Zauważalne jest też wykrywanie cyklu o poprawnej wartości Tc i mniejszej wartości Kc, np. Kc = 11. Podobnie wyglądają wyniki w przypadku występowania tylko zakłóceń ZII oraz zakłóceń mieszanych ZI i ZII (wykres na rys. 10b). Tym wariantom badań odpowiadają zobrazowania pomiarów na rys. 9a i 9c. Zmodyfikowany algorytm ASWC ze wskaźnikiem Wsk(Tc, k = Kc) daje dla identycznych sytuacji pomiarowych wyniki znacznie bardziej stabilne (rys. 10c i 10d) przekraczające próg 0,85–0,9. Istota modyfikacji polega na dołączaniu do skupienia najliczniejszego na etapie *k*-tym sumy liczności skupień d_i różniących się $d_i - d_{j*} \in \{PRI\}$ o jedną ze zidentyfikowanych wcześniej wartości okresu powtarzania ze zbioru {PRI}:

$$Wsk(Tc= d_{j*}, k) = (\max n_{j*}^k + \Sigma n_i^k) / (z - k), \text{ gdzie: } n_i^k > 0 \text{ jeśli } d_i^k \in \{PRI\} \qquad (6)$$

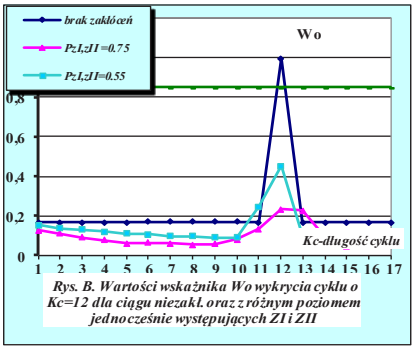
Stąd (6) wynika wysoka wartość oraz stabilność Wsk, widoczne na rys. 10c i 10d.



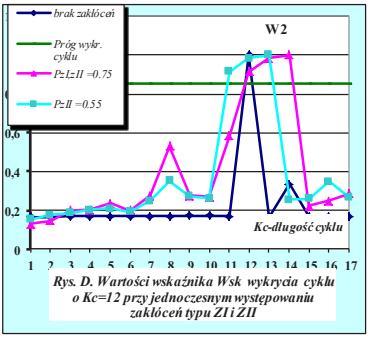
Rys. A. Wartości wskaźnika Wo wykrycia cyklu o Kc=12 dla niezakłóconego ciągu oraz dla ciągów o różnym poziomie zakłóceń ZI



Rys. C. Wartości wskaźnika Wsk wykrycia cyklu o Kc=12 dla niezakłóconego ciągu oraz dla ciągów o różnym poziomie zakłóceń ZI



Rys. B. Wartości wskaźnika Wo wykrycia cyklu o Kc=12 dla ciągu niezakł. oraz z różnym poziomem jednocześnie występujących ZI i ZII



Rys. D. Wartości wskaźnika Wsk wykrycia cyklu o Kc=12 przy jednoczesnym występowaniu zakłóceń typu ZI i ZII

Uwaga. W celu poprawienia widzialności zmian obliczanych wartości wskaźników na wykresach punkty połączono liniami.

Rys. 10. Porównanie wartości wskaźników Wo i Wsk wykrywania długości Kc cyklu i Tc dla sygnału niezakłóconego oraz różnych wariantów i stopnia jego zakłócania
Źródło: opracowanie własne.

Podsumowanie

Z przedstawionych wyników dla wskaźnika Wo (rys. 10a, 10b) widać, że:

- wartości wskaźnika Wo są niestabilne – szybko maleją ze wzrostem ZI;
- ma on podobne własności przy występowaniu tylko zakłóceń ZII;
- jego wartości ulegają obniżeniu przy łącznym występowaniu ZI i ZII;
- przy mniejszym poziomie zakłóceń przyjmuje on maksymalną wartość dla etapu k = Kc, jednak wartości Wo są bardzo małe i szybko maleją ze wzrostem zakłóceń;
- niestabilny charakter wyklucza stosowanie Wo do automatycznego wykrywania cyklu.

Wartości wskaźnika skojarzenia skupień W_{sk}, dla identycznych wariantów ciągów jak w przypadku Wo, przedstawiono na rys. 10c i 10d. Z przedstawionych wykresów wynika, że:

- wartości wskaźnika W_{sk} przyjmują wartość maksymalną dla etapu k = Kc, i wartość ta bliska jest wartości maksymalnej (tzn. 1,0);
- ze wzrostem zakłóceń ZI wskaźnik W_{sk} przyjmuje również wysokie wartości dla etapów k < 12, ale należy tu zaznaczyć, że w obliczeniach, aby uwidocznić różnice, celowo nie wykorzystywano wszystkich możliwości algorytmu AWSC [8, 10]. Jej uwzględnienie spowodowałaby, że wartość wskaźnika byłaby przyjmowana jako $W_{sk} = 0$, gdyż dla ZI = True i etapów k = 8÷11 skupienie najbardziej liczne nie jest skupieniem pierwszym (o j* = 1);
- jego wartości ulegają niewielkiemu obniżeniu przy łącznym występowaniu ZI i ZII.

Badania potwierdzają, że wskaźnik W_{sk} wykrycia cyklu ma wszystkie oczekiwane cechy, które pozwalają na jego stosowanie w algorytmach automatycznego określania parametrów PRI.

Analiza algorytmu ASWC pozwala na wyspecyfikowanie następujących cech:

- wysoka niezawodność wykrywania cyklu w warunkach zakłóceń;
- pozwala na wykrywanie cykli o złożonych strukturach PRI;
- wysoka dokładność wyznaczenia parametrów PRI;
- oszczędność ze względu na zajętość pamięci.

Zasadnicze, bardziej czasochłonne operacje wynikają z sortowania zbioru odstępów w celu przyspieszenia ich grupowania, ale sortowane zbiory nie są zbiorami licznymi. Pesymistyczna, szacowana, złożoność obliczeniowa Q(z, Kc) przy wykrywaniu cyklu o długości Kc w ciągu „z" impulsów i stosowaniu algorytmu sortowania Quicksort wynosi około 0,5 Kc (z^2 +3z).

Literatura

[1] Paradowski L., Szutkowski F., *Problemy rozpoznania i przeciwdziałania radioelektronicznego*, WAT, Warszawa 1986.

[2] Wiley R.G., *Electronic Intelligence: The Analysis of Radar Signals*, Artech House 1995.

[3] Adamy D., *EW 102. A First Course in Electronic Warfare*, Artech House, Boston–London 2004.

[4] *Walka radioelektroniczna w radiolokacji*, WAT, Warszawa 2019.

[5] Shahhoseini H.S., Naseri A., Naderi M., *A new matrix method for pulse train identification: Implementing by systolic array*, w: *2002 11th European Signal Processing Conference*, 183–187.

[6] Banasiak K., *Monitorowanie pracy radarów*, Konferencja Naukowa „Urządzenia i systemy radioelektroniczne", Soczewka 21.09–23.09.2005 r.

[7] Banasiak K., Pieniężny A., *Radar pulse repetitive patterns detection*, 11th International Radar Symposium (IRS 2010), 16.06–18.06.2010 r., Vilnius, Litwa.

[8] Banasiak K., *Automatyzacja przetwarzania pomiarów w rozpoznawaniu sygnałów impulsowych*, „Przegląd Elektrotechniczny" 2013, nr 9a, s. 12–19.

[9] Banasiak K., *Wykrywanie sygnałów impulsowych w złożonych warunkach ich akwizycji*, „Pomiary – Automatyka – Kontrola" 2014, nr 9, s. 722–725.

[10] Banasiak K., *Zastosowanie metod histogramowych w analizie sygnałów o długich cyklach okresu powtarzania impulsów*, „Przegląd Elektrotechniczny" 2016, nr 1, s. 29–33.

Streszczenie

Bezpieczeństwo elektromagnetyczne Sił Zbrojnych RP zapewniają m.in. urządzenia i systemy elektronicznego wywiadu sygnałowego, które są zaliczane do urządzeń walki radioelektronicznej – WRE (ang. Electronic Warfare) i spełniają funkcje urządzeń ELINT (ang. Electronic Intelligence) lub ESM (ang. Electronic Warfare Support Measures). Walka radioelektroniczna WRE jest zamierzonym działaniem zmierzającym do wykorzystania widma elektromagnetycznego i obejmuje: przechwyt i identyfikację emisji elektromagnetycznych, użycie energii elektromagnetycznej do zmniejszenia skuteczności lub uniemożliwienia użycia tego widma przez przeciwnika oraz zapewnienie efektywnego wykorzystania widma elektromagnetycznego przez siły własne. Z definicji WRE wynika, że w czasie pokoju jej zadaniem jest zdobywanie informacji o środkach radioelektronicznych potencjalnych przeciwników.

Jednym z istotnych parametrów w rozpoznaniu jest okres powtarzania impulsów PRI (ang. Pulse Repetition Interval). Sygnały radarowe charakteryzuje duża złożoność zmian PRI, co w efekcie zapewnia jego dużą przydatność informacyjną. W artykule przedstawiono istotę autorskiego algorytmu sekwencyjnego wykrywania cyklu o małej złożoności obliczeniowej. Przedstawiono również przykładowe wyniki badań potwierdzające jego wysoką skuteczność.

Summary

The electromagnetic safety of the Polish Armed Forces is ensured, among others, by: devices and systems of electronic signal intelligence, which are classified as radio-electronic warfare devices – WRE (Electronic Warfare) and fulfill the functions of ELINT (Electronic Intelligence) or ESM (Electronic Warfare Support Measures) devices. EW electronic warfare is a deliberate action aimed at the use of the electromagnetic spectrum and includes: interception and identification of electromagnetic emissions, the use of electromagnetic energy to reduce the effectiveness or prevent the use of this spectrum by the enemy, and ensuring the effective use of the electromagnetic spectrum by own forces. From the definition of EW it

follows that in peacetime its task is to obtain information about the radio-electronic means of potential opponents.

One of the important parameters in diagnosis is the PRI (Pulse Repetition Interval) period. Radar signals are characterized by high complexity of PRI changes, which in turn ensures its high information usefulness. The article presents the essence of the proprietary sequential cycle detection algorithm with low computational complexity. Examples of test results confirming its high effectiveness were also presented.

Słowa kluczowe

Walka elektroniczna, radar.

Keywords

Electronic warfare, radar.

Kazimierz Banasiak – dr inż., Instytut Radioelektroniki Wydziału Elektroniki Wojskowej Akademii Technicznej w Warszawie.

Andrzej Wilk

ARMAND HAMMER – POSTAĆ Z PODRĘCZNIKÓW BIZNESU

Armand Hammer (1898–1990) był człowiekiem niezwykłym. Łączył w sobie umiejętności wielkiego przedsiębiorcy, zręczność właściwą wybitnym dyplomatom i szczodrość filantropa wspierającego medycynę, edukację i sztukę. Miał niezwykły dar zjednywania ludzi i udowadniania im swej użyteczności. Do tych ludzi przez kilka dekad należeli kolejni amerykańscy prezydenci i przywódcy Komunistycznej Partii Związku Radzieckiego. Hammer był dla nich pośrednikiem i doradcą proponującym sposoby osiągania porozumienia.

Julius Hammer pochodził z rodziny żydowskiej mieszkającej w Odessie. Po przyjeździe do Nowego Jorku był aktywnym lekarzem i właścicielem dobrze prosperującej firmy farmaceutycznej. 21 maja 1898 roku urodził się jego syn Armand. Julius Hammer był jednym z założycieli Komunistycznej Partii Stanów Zjednoczonych. Stąd też był znany Włodzimierzowi Leninowi i innym politykom bolszewickim.

Kontynuując tradycję rodzinną, Armand Hammer studiował medycynę w Columbia University. Jeszcze jako student stał się milionerem. Było to w czasie prohibicji. W firmie ojca uruchomił produkcję syropu na kaszel zawierającego alkohol i ekstrakt z imbiru. Było to zgrabne obejście prohibicyjnych zakazów.

Po ukończeniu studiów młody Hammer udał się do radzieckiej Rosji, aby sprawdzić się jako lekarz przy zwalczaniu chorób epidemicznych. Na Kremlu został przyjęty przez Lenina, który doradzał mu zajęcie się biznesem służącym przezwyciężaniu izolacji gospodarczej Rosji, stosowanej przez państwa zachodnie. Zwiedzając Moskwę, młody Amerykanin zauważył w sklepach ogromne ilości skór zwierząt upolowanych przez syberyjskich myśliwych, a także liczne szlachetne kamienie znalezione w górach Uralu. Nikt tego nie kupował. Tymczasem głodująca Rosja była zainteresowana zakupem amerykańskiej pszenicy.

Armand Hammer w podręcznikach biznesu uznawany jest za pomysłowego organizatora wielkich transakcji wymiennych (barterowych)[1]. Nie była to prosta wymiana towaru za towar. Skóry należało sprzedać zainteresowanym firmom

[1] R.W. Griffin, R.J. Ebert, *Business*, Prentice Hall, Eaglewood, New Jersey 1991, s. 699.

futrzarskim. Kamienie szlachetne musiały trafić do producentów wyrobów jubilerskich. Uzyskane z tych transakcji pieniądze musiały być skierowane do firm eksportujących amerykańską pszenicę. Młody lekarz potrafił poradzić sobie z tymi kwestiami i uzyskać dla siebie godziwą prowizję.

Ołówki Hammera

Ogłoszona przez Lenina w 1921 roku nowa polityka ekonomiczna (NEP) miała na celu m.in. przyciągnięcie zachodnich przedsiębiorców i zainteresowanie ich uzyskaniem koncesji w różnych sektorach gospodarki. Przedsiębiorcy ci byli jednak bardzo ostrożni albo nastawieni na uzyskanie jednostronnych, czasami wręcz eksploatatorskich korzyści. Uzyskanie koncesji okazało się trudne i długotrwałe. Potrzebny był dobry, konstruktywny przykład. Hammer przy poparciu Lenina uzyskał koncesję na wydobywanie azbestu w górach Uralu. Lenin w liście do Stalina określił tę koncesję jako „małą ścieżkę do amerykańskiego świata biznesu" i podkreślił: „musimy na wszelkie sposoby wykorzystać tą ścieżkę"[2]. Robotnicy pracujący przy wydobywaniu azbestu nie mieli odzieży ochronnej. Hammer sprowadził z USA ubrania pochodzące z zapasów wojskowych.

Kiedy w wielu krajach powstały radzieckie przedstawicielstwa handlowe, a w 1925 roku wprowadzono państwowy monopol handlu zagranicznego, Hammer utracił możliwość funkcjonowania jako pośrednik. Dostrzegł jednak nowe możliwości prowadzenia działalności gospodarczej. Powszechna kampania walki z analfabetyzmem oznaczała ogromny popyt na ołówki. Masowa ich produkcja była możliwa w fabryce wyposażonej w odpowiednie maszyny i urządzenia. Hammer sprowadził je z Niemiec. Również z Niemiec przybyli do Moskwy specjaliści-technicy zapewniający właściwą obsługę i konserwację tych maszyn i urządzeń. Byli to ludzie, którzy stracili pracę i nie mieli szans na jej uzyskanie w niemieckich fabrykach. Solidarność właścicieli fabryk oznaczała, że pracownik będący w konflikcie z jednym fabrykantem nie mógł liczyć na pracę w innej fabryce. Stąd też decyzje o podjęciu pracy w Moskwie.

Hammerowskie ołówki używane były przez dziesiątki milionów mieszkańców Związku Radzieckiego. Pewna ilość ołówków była eksportowana do Chin.

Powrót do Ameryki

W początkach pobytu w Moskwie Hammer zawarł z władzami radzieckimi porozumienie przewidujące, że wyjeżdżając z ZSRR, będzie uprawniony do zabrania

[2] L. Fischer, *The Life of Lenin*, N.Y., Evanson and London 1964, s. 606.

ze sobą wszystkiego, co stanowiło jego mienie osobiste. W trakcie ośmioletniego pobytu w Moskwie Hammer nabył wiele dzieł sztuki i precjozów pochodzących z carskiego dworu. Po powrocie do Stanów Zjednoczonych wiele z tych kosztowności zostało sprzedanych na kiermaszach. Wielki zbiór dzieł sztuki umieścił Hammer w Los Angeles w ufundowanym przez siebie muzeum, którego koszt wyniósł 30 mln dolarów.

Decyzję o powrocie Hammer podjął wtedy, gdy Stalin stał się faktycznym dyktatorem. Bliskim znajomym Hammera był Lew Trocki, który został odsunięty od władzy, a ludzie, którzy mieli z nim kontakt, znaleźli się w kręgu podejrzanych o „trockizm". Hammer brał też pod uwagę stalinowską kampanię podejrzliwości wobec cudzoziemców. Posiadanie amerykańskiego obywatelstwa narażało na podejrzenie o szpiegostwo. Takie podejrzenie – według stalinowskiego prawa – oznaczało możliwość skazania na wieloletnie więzienie. Należy podkreślić, że podstawą skazania bywało nie tylko szpiegostwo, ale podejrzenie o szpiegostwo.

Po zakończeniu prohibicji, w 1933 roku Hammer włączył się do produkcji whisky, do której produkcji potrzebna była duża ilość drewnianych beczek. Hammer importował ze Związku Radzieckiego drewno na klepki. Była to bodaj jedyna forma kontaktu ze stalinowskim mocarstwem[3].

Naftowa „siostra" nr 8

W życiu Hammera nie brakło problemów osobistych. Były dwa rozwody i oskarżenie syna o zabójstwo. Jednakże syn został uniewinniony, a trzecie małżeństwo okazało się szczęśliwe.

W 1955 roku Hammerowie przenieśli się z Nowego Jorku do Los Angeles. Wybitny biznesmen myślał o emeryturze. Nie wiedział, że jest przed nim wielka przyszłość. W autobiografii pisał, że gdyby w szklanej kuli zobaczył swą przyszłość, to roześmiałby się tak głośno, że kula rozprysłaby się na drobne kawałki.

Dwa lata później Hammer zainwestował 100 tys. dolarów w wiercenia dokonywane przez podupadłą firmę naftową Occidental Petroleum (Oxy), której wartość netto oceniano na 34 tys. dolarów. Wiercenia okazały się skuteczne. Hammer wykupił firmę i stał się jej prezesem. Wkrótce potem Oxy dokonało pomyślnych wierceń na polach gazowych w Kalifornii. Następne były pola naftowe w Kolumbii, na Morzu Północnym i w Libii. W tym ostatnim przypadku, po latach, za rządów Kaddafiego, pola naftowe zostały znacjonalizowane.

W 1960 roku roczny dochód Occidental Petroleum wyniósł 650 mln dolarów, a dziesięć lat później – ponad 2 mld. Koncern stał się ósmą wielką firmą naftową,

[3] G.W. Griffin, R.J. Ebert, *Business*, *op.cit.*, s. 699.

obok tzw. siedmiu sióstr – Texico, British Petroleum (BP), Shell, Exxon (Esso), Gulf, Mobil i Socal (Chevron). Amerykański ambasador David Newsom z dyplomatycznym umiarem zauważył: „Można bezpiecznie powiedzieć, że wejście Occidental na scenę nie było ciepło przyjęte przez wszystkie pozostałe przedsiębiorstwa”[4]. Kontakty pomiędzy szefami wszystkich korporacji naftowych były jednak konieczne. Hammer telefonował do nich z Kalifornii, nie biorąc pod uwagę różnicy czasu, czyli faktu, że budził ich o północy.

Kapitalista ukochany przez Kreml

Po śmierci Stalina Hammer odnowił kontakty z radzieckimi przywódcami. Rozmawiał z Chruszczowem, Breżniewem, Czernienką i Gorbaczowem. Po swych dziewięćdziesiątych urodzinach w 1988 roku był jedynym zachodnim biznesmenem zaproszonym do Moskwy w charakterze obserwatora spotkania pomiędzy Michaiłem Gorbaczowem a Ronaldem Reaganem. Podróżował własnym odrzutowcem OxyOne (Boeing 727), który był jedynym prywatnym samolotem uprawnionym do przekraczania granicy ZSRR.

Również w roku 1988 sędziwy jubilat doprowadził do zawarcia porozumienia Oxy z rządem radzieckim w sprawie wybudowania wielkich zakładów petrochemicznych za 6 mld dolarów[5]. W projekcie tym uczestniczyli partnerzy włoscy i japońscy.

W latach 1977–1984 Armand Hammer był wiceprzewodniczącym Amerykańsko-Radzieckiej Rady Handlowo-Gospodarczej (U.S.-U.S.S.R. Trade and & Economic Council).

W 1979 roku w trakcie pobytu w USA wielkiego chińskiego przywódcy i reformatora Denga Xiaopinga Hammer spotkał się z nim w Teksasie. Rezultatem tego spotkania był kontrakt pomiędzy Oxy i chińskim przemysłem węgla kamiennego na sumę około 750 mln dolarów.

Działalność publiczna

Sporo czasu i pieniędzy poświęcił Hammer badaniom medycznym. W roku 1981 prezydent Reagan mianował go członkiem trzyosobowego panelu mobilizującego środki na walkę z rakiem. W latach 1984–1989 Hammer był przewodniczącym panelu. W tym charakterze zainaugurował zgromadzenie w ciągu roku miliarda dolarów.

[4] A. Sampson, *The Seven Sisters*, New York 1979, s. 251.
[5] G.W. Griffin, R.J. Ebert, *Business*, *op.cit.*, s. 699.

W 1982 roku w Montezuma (stan Nowy Meksyk) rozpoczęła działalność uczelnia o nazwie Armand Hammer World College of the American West – uczelnia dwuletnia przygotowująca nastoletnich cudzoziemców z kilkudziesięciu krajów do studiów na czołowych uniwersytetach amerykańskich. Większość z nich otrzymywała stypendia pełne lub częściowe. Wspieranie edukacji poprzez inicjatywy i dotacje uczyniło Hammera popularnym w amerykańskich środowiskach akademickich. 25 uniwersytetów nadało mu stopień doktora honoris causa.

W szerokim kręgu zainteresowań Hammera była również hodowla koni rasowych. To zainteresowanie sprawiło, że bywał on na aukcjach w Janowie Podlaskim.

Hammer z troską obserwował sytuację w Afganistanie i usiłował podejmować działania służące przywróceniu pokoju w tym państwie. Po radzieckiej interwencji w 1979 roku zachodni przywódcy zawiesili kontakty z Leonidem Breżniewem. Prezydent Francji Valery Giscard d'Estaing w rozmowie z Hammerem wyraził pogląd, że istnieje potrzeba i możliwość nakłonienia Breżniewa do wycofania radzieckich wojsk z Afganistanu. W grę jednak nie wchodziło zaproszenie go do Paryża ani też wizyta prezydenta Francji w Moskwie. Hammer zadeklarował wówczas gotowość rozmowy z Edwardem Gierkiem i zasugerowania mu, aby zaprosił sekretarza generalnego KPZR i prezydenta Francji do Warszawy. Edward Gierek mówił o swej rozmowie z Hammerem: „W czasie spotkania ze znanym przemysłowcem amerykańskim, Hammerem, które miało miejsce w Warszawie, uzgodniłem, że wykorzystam swe specjalne stosunki z prezydentem Francji, jak i dobre z Breżniewem, dla próby zorganizowania takiego spotkania”[6].

Wydana w 1987 roku autobiografia Hammera była międzynarodowym bestsellerem. Jednakże zawierała ona istotną omyłkę. Hammer napisał, że do spotkania nie doszło, gdyż Gierek stracił władzę. W rzeczywistości spotkanie w Warszawie miało miejsce 19 kwietnia 1980 roku, a Gierek utracił władzę we wrześniu tegoż roku. Kiedy zauważyłem tę omyłkę, napisałem o niej do Hammera, sugerując korektę w następnym wydaniu jego interesującej autobiografii. Na ten list po pewnym czasie otrzymałem odpowiedź. Hammer usprawiedliwił zwłokę w udzieleniu odpowiedzi pilnymi obowiązkami, wyraził zadowolenie z powodu pozytywnej opinii o autobiografii i stwierdził, że ceni uwagę na temat Gierka.

Który system jest bardziej wydajny?

Armand Hammer zapytany, który system gospodarowania jest wydajniejszy: amerykański czy radziecki, odpowiedział, że amerykański, ponieważ stawia on ludziom wyższe wymagania. Istotnie, tak było. Z jednej strony, przeciętni Amery-

[6] J. Rolicki, *Edward Gierek: przerwana dekada*, Fakt, Warszawa 1990, s. 113.

kanie pozostawali i pozostają pod groźbą bicza bezrobocia i widma bezdomności. Z drugiej strony oddziałuje na nich opowieść o drodze od pucybuta do milionera. Opowieść ta dla niewielu jest zapowiedzią fortuny. Dla bardzo wielu jest ona mirażem mającym jednak siłę motywującą, większą aniżeli perspektywa uzyskania orderu Bohatera Pracy Socjalistycznej. Armand Hammer znał doskonale realia społeczne i ekonomiczne zarówno Stanów Zjednoczonych, jak i Związku Radzieckiego.

Po dziewięćdziesiątych urodzinach Hammer był wielokrotnie pytany, kiedy wybierze się na emeryturę. Odpowiadał, że decyzję w tej sprawie uzależnia od wzrostu wartości akcji Oxy i od ukończenia setnego roku życia. Rak szpiku kostnego spowodował, że do emerytury nie doczekał.

Bibliografia

Fischer L., *The Life of Lenin*, N.Y., Evanson and London 1964.

Griffin R.W., Ebert R.J., *Business*, Prentice Hall, Eaglewood, New Jersey 1991.

Rolicki J., *Edward Gierek: przerwana dekada*, Fakt, Warszawa 1990.

Sampson A., *The Seven Sisters*, New York 1979.

Andrzej Wilk – dr inż., Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie.