Grzegorz Klein

Akademia im. Jakuba z Paradyża
w Gorzowie Wielkopolskim

11/2019

Bezpieczeństwo informacyjne RP w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej – perspektywa teoretyczna

W drugiej dekadzie XXI wieku nastąpiła intensyfikacja działań Federacji Rosyjskiej zagrażających bezpieczeństwu informacyjnemu innych państw. Szczególnie udokumentowaną egzemplifikacją takich działań była wymierzona w Ukrainę rosyjska aktywność w przestrzeni informacyjnej podczas przygotowywania oraz realizowania „operacji krymskiej”[50]. Katalog zarówno potwierdzonych, jak i domniemanych działań Federacji Rosyjskiej wymierzonych w bezpieczeństwo informacyjne państw Europy Środkowej i Wschodniej czyni zasadnym badania nad polskim bezpieczeństwem informacyjnym w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej.

Zasadność ta jest umacniana dzięki wnioskom, jakie można sformułować na podstawie analizy literatury przedmiotu. Z analizy tej wynika, że jakkolwiek w ostatnich latach tematyka bezpieczeństwa informacyjnego jest przedmiotem refleksji badaczy, to w badaniach tych dominują aspekty praktyczne. Tym samym prowadzone badania częstokroć koncentrują się na szukaniu odpowiedzi na pytania: jak zapewniać bezpieczeństwo informacyjne? Jak ograniczać bądź zwalczać zagrożenia w przestrzeni informacyjnej? Są to kwestie ważne zarówno dla teorii, jak i dla praktyki, niemniej można przyjąć, że są to zagadnienia wtórne – przede wszystkim należy określić, czym jest bezpieczeństwo informacyjne.

Temu właśnie poświęcony jest niniejszy artykuł, będący rekapitulacją badań, w ramach których sformułowano następujący problem badawczy: w jaki sposób identyfikować bezpieczeństwo informacyjne Polski w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej? Przyjęto przy tym hipotezę, zgodnie z którą bezpieczeństwo informacyjne Polski w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej można identyfikować w sposób interdyscyplinarny, łączący podejścia właściwe dla komunikowania społecznego oraz nauk o bezpieczeństwie.

Rozpatrywanie bezpieczeństwa informacyjnego przez pryzmat nauk o bezpieczeństwie jest w polskim piśmiennictwie utrwalonym podejściem. Nie można tego powiedzieć o korzystaniu z dorobku komunikowania społecznego przy badaniu tej tematyki. Przyjęcie takiej percepcji oznacza, że w badaniach nad bezpieczeństwem informacyjnym przedmiotem zainteresowania jest nie tylko kanał przesyłania treści (informacji), ale również treść (informacja). Ważne jest zatem m.in. to jak treść powstaje, co w sobie zawiera i jakie powoduje reakcje. W perspektywie komunikowania społecznego treść jest co najmniej równie ważna jak kanał – wobec braku pierwszego elementu, drugi traci swoje znaczenie.

W celu weryfikacji przyjętej hipotezy badania zostały podzielone na dwa etapy, którym odpowiadają dwie części niniejszego artykułu. W pierwszej z nich dokonano rekapitulacji obecnych w polskim piśmiennictwie analiz sposobów definiowania bezpieczeństwa informacyjnego. Określono dzięki temu dominujące w literaturze przedmiotu podejście w zakresie określania jego istoty.

---

[50] Działania te były przedmiotem zarówno polskich, jak i międzynarodowych analiz, por.: J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, „Punkt widzenia” Warszawa 2014, nr 42; S. Samadashvili, *Muzzling the Bear. Strategic Defence for Russia's Undeclared War on Europe*, Bruksela, 2015; K. Geers, *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn 2015.

Druga część badań to refleksja nad bezpieczeństwem informacyjnym w percepcji komunikowania społecznego. Szczególną uwagę poświęcono treści jako kategorii bezpieczeństwa informacyjnego, wykazując użyteczność przyjętej perspektywy w procesie identyfikacji bezpieczeństwa informacyjnego Polski w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej.

Celem badań było pogłębienie wiedzy na temat identyfikowania istoty bezpieczeństwa informacyjnego w sposób interdyscyplinarny, przez pryzmat komunikowania społecznego i nauk o bezpieczeństwie. Jednocześnie celem badań nie było projektowanie nowej, kolejnej w polskim piśmiennictwie definicji bezpieczeństwa informacyjnego. Celem badań nie była również refleksja nad praktycznymi zagadnieniami, związanymi np. ze sposobami zapewnienia bezpieczeństwa informacyjnego – rozważania dotyczące użyteczności rozpatrywanej percepcji bezpieczeństwa informacyjnego służą wykazaniu tego, czym to bezpieczeństwo jest, jaka jest jego istota.

Sposoby definiowania bezpieczeństwa informacyjnego w polskim piśmiennictwie

Druga dekada XXI wieku to nie tylko wspomniana na początku artykułu intensyfikacja działań Federacji Rosyjskiej w przestrzeni informacyjnej, ale również wzrost zainteresowania tematyką bezpieczeństwa informacyjnego wśród polskich badaczy. W literaturze przedmiotu przedstawione są wyniki badań prowadzonych za pomocą analizy danych z Biblioteki Narodowej. Badania dotyczyły bezpieczeństwa informacyjnego w polskim piśmiennictwie naukowym w latach 2002-2017. Wynika z nich, że w latach 2002-2009 zarejestrowano w Katalogach Biblioteki Narodowej 51 rekordów dotyczących tego obszaru, natomiast w latach 2010-2017 tych rekordów było 428, w tym 214 w latach 2016-2017[51].

W badaniach tych wyodrębniono również konteksty, w jakich prowadzono badania nad bezpieczeństwem informacyjnym. Wydzielono 15 następujących kategorii: „komponent bezpieczeństwa narodowego, komponent kultury bezpieczeństwa, komponent kultury informacyjnej, komponent ekologii informacji, bezpieczeństwo w dobie globalizacji i społeczeństwa informacyjnego, element międzynarodowej i lokalnej polityki informacyjnej, cel polityki bezpieczeństwa informacyjnego, przedmiot technologii informatyczno-komunikacyjnych (infrastruktura teleinformatyczna – obsługa i eksploatacja), równoznacznik bezpieczeństwa informacji i ochrony danych, proces zarządzania bezpieczeństwem informacji (organizacja audytu informacji), obszar wpływu manipulacji medialnej przez środki masowego przekazu, wyznacznik organizacji i jej kultury organizacyjnej, przedmiot walki konkurencyjnej i biznesowej (gospodarka elektroniczna), element walki informacyjnej (przedmiot wojny informacyjnej, cyberwojny), część edukacji dla bezpieczeństwa”[52].

Wielość kontekstów w jakich analizowane jest bezpieczeństwo informacyjne oznacza różnorodność w sposobach jego definiowania. Niekiedy rozważania nad istotą bezpieczeństwa informacyjnego określane są mianem chaosu, który dodatkowo zwiększa upowszechnianie pojęć błędnych, czy też nieaktualnych. Dostrzega się przy tym częstą praktykę zawężania tego zagadnienia do tematów związanych z ochroną informacji niejawnych oraz cyberprzestrzenią[53]. Również w badaniach dotyczących bezpieczeństwa informacyjnego w polskim piśmiennictwie

[51] H. Batorowska, *Bezpieczeństwo informacyjne w dyskursie naukowym - kierunki badań* [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków 2017, s. 9. Można zakładać, że szczególna intensywność piśmiennicza w latach 2016-2017 związana była nie tylko z wymierzoną w Ukrainę agresją rosyjską, ale również z takimi wydarzeniami budzącymi zainteresowanie w kontekście bezpieczeństwa informacyjnego, jak referendum w sprawie brexitu, czy też wybory prezydenckie w USA.

[52] *Ibidem*, s. 12.

[53] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce-Warszawa 2016, s. 42.

skonstatowano, że można mówić o prymacie technicznej (technologicznej) i cybernetycznej perspektywy rozważań nad bezpieczeństwem informacyjnym[54].

Perspektywa oznaczająca „dominację technicznych i proceduralnych aspektów bezpieczeństwa informacyjnego" prowadzi do postrzegania tego obszaru jako bezpieczeństwa informatycznego. Zaznacza się przy tym, że takie podejście może oznaczać marginalizowanie znaczenia człowieka (przyjmując przy tym, że jest to najczęściej najsłabsze ogniwo systemów bezpieczeństwa) oraz kultury bezpieczeństwa[55].

Przykłady definiowania bezpieczeństwa informacyjnego przedstawiono w poniższej tabeli. Zdecydowano się na układ tabelaryczny w celu czytelnego wyodrębnienia elementów potencjalnie ważnych w kontekście komunikowania społecznego (lub wykazania ich braku). Przyjęto, że elementy te związane są z treścią (informacją), zwłaszcza z jej kreowaniem, a nie służącym do jej przesyłania kanałem oraz zapewnianiem bezpieczeństwa kanału.

Tabela 1. Wybrane definicje bezpieczeństwa informacyjnego z wyróżnionymi elementami ważnymi w kontekście komunikowania społecznego

Definicje bezpieczeństwa informacyjnego	Elementy ważne w kontekście komunikowania społecznego
„Zbiór działań, metod, procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem" [P. Potejko].	Brak potencjalnie użytecznych elementów w kontekście komunikowania społecznego.
„Wszelkiego rodzaju wysiłki, służące ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów)" [M. Madej].	Użytecznym elementem jest wskazanie na własne akcje dezinformacyjne.
„Obejmuje wszystkie procesy technologiczne – od pozyskiwania, poprzez transmisję, przetwarzanie, do przechowywania informacji w systemach informacyjnych, stanowiąc kompleks przedsięwzięć zapewniający bezpieczeństwo środowiska informacyjnego" [J. Janczak, A. Nowak].	Brak potencjalnie użytecznych elementów w kontekście komunikowania społecznego.
„Stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego" [E. Nowak, M. Nowak].	Użytecznym elementem jest powiązanie zagadnienia ze społeczeństwem informacyjnym.

[54] H. Batorowska, *Bezpieczeństwo informacyjne…, op. cit.,* s. 14.

[55] M. Cieślarczyk, *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce-Warszawa 2016, s. 48; A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych" 29/2013, s. 453.

„Możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą" [L.F. Korzeniowski].	Brak potencjalnie użytecznych elementów w kontekście komunikowania społecznego.
„Proces i stan, w ramach których zapewniania jest swoboda dostępu, gromadzenia, przetwarzania i przepływu wysokiej jakości informacji (osiąganej przez merytoryczną selekcję) połączone z racjonalnym, prawnym i zwyczajowym wyodrębnianiem kategorii podlegających ochronie bądź reglamentacji, ze względu na bezpieczeństwo podmiotów, których one dotyczą" [W. Fehler].	Użytecznym elementem jest merytoryczna selekcja informacji.

Źródło: opracowanie własne na podstawie: A. Polończyk, *Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa* [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków 2017, s. 80-81; P. Potejko, *Bezpieczeństwo informacyjne* [w:] *Bezpieczeństwo państwa*, Warszawa 2009, s. 194; M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego* [w:] *Bezpieczeństwo teleinformatyczne państwa*, Warszawa, s. 18-19; J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, s. 17; E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103; L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 147; W. Fehler, *O pojęciu…*, *op. cit.,* s. 29-30; A. Żebrowski, *Bezpieczeństwo informacyjne...*, *op. cit.,* s. 452-453.

Podobnie jak w przypadku definicji ujętych w powyższej tabeli, również w ujęciach bezpieczeństwa informacyjnego przedstawionych w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* oraz w *Białej Księdze Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* brakuje właściwej dla komunikowania społecznego percepcji tego zagadnienia. Przyjęta perspektywa jest związana z ochroną informacji niejawnych oraz bezpieczeństwem systemów teleinformatycznych[56].

Aspektów ważnych z perspektywy komunikowania społecznego nie uwzględniono również w ogłoszonym 24.07.2015 r. przez Biuro Bezpieczeństwa Narodowego projekcie (wersja finalna nie została przedstawiona) *Doktryny Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej*. W projekcie tym przyjęto, że „bezpieczeństwo informacyjne – wraz z jego integralną częścią, jaką jest cyberbezpieczeństwo – jest jednym z najbardziej wrażliwych obszarów bezpieczeństwa narodowego i międzynarodowego, mającym charakter transsektorowy i wpływającym na efektywność funkcjonowania całego systemu bezpieczeństwa"[57]. Ponadto w projekcie tym zdefiniowano bezpieczeństwo informacyjne państwa, przyjmując, że jest to „transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizacje takich zadań jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa

[56] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014, pkt. 85; Biała Księga *Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 171-172.

[57] *Projekt Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej*, Warszawa 2015, s. 3, za: https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf (09.04.2020).

informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego”[58].

Powyższe dwie definicje, czy też raczej z racji ostatecznego nieopublikowania *Doktryny*, propozycje definicji, również są mocno powiązane z cyberbezpieczeństwem. W przypadku drugiej z nich uwagę zwraca właściwe dla nauk o bezpieczeństwie postrzeganie rzeczywistości w kategoriach stanu i procesu. Wartościowe w kontekście dalszych rozważań jest również rozróżnienie działań defensywnych i ofensywnych.

Cechy bezpieczeństwa informacyjnego w pespektywie komunikowania społecznego

Na początku niniejszej pracy założono, że w perspektywie komunikowania społecznego treść jest co najmniej równie ważna jak kanał, ponieważ wobec braku pierwszego elementu, drugi traci swoje znaczenie. Założenie, że treść i kanał to osobne kategorie jest utrwalonym podejściem w badaniach prowadzonych w obszarze komunikowania społecznego. Podział taki jest obecny m.in. w uznawanym za „kanoniczny” modelu H. Lasswella, w ramach którego wyróżniono nadawcę, komunikat (treść), kanał, odbiorcę oraz efekt[59]. W naukach o bezpieczeństwie niektórzy badacze stosują korespondujący podział w rozważaniach nad informacją, dzieląc ją na warstwę humanistyczną (wymiar subiektywny) i fizykalną (wymiar obiektywny)[60] – można przyjąć, że pierwszej z nich odpowiada treść, drugiej kanał.

Jak wynika z przedstawionej w poprzedniej części analizy sposobów definiowania bezpieczeństwa informacyjnego, podział na treść i kanał nie jest upowszechniony wśród badaczy tego obszaru. O tym, że wprowadzenie właściwego dla komunikowania społecznego podziału może być wartościowe w procesie rozważań nad bezpieczeństwem informacyjnym mogą świadczyć problemy dotyczące *fake newsów*, dezinformacji i korespondujących zjawisk.

Terminy te są definiowane na różne sposoby. Stosuje się zarówno podejście, w ramach którego zaznaczane są różnice pomiędzy nimi (np. w zakresie odróżniania *fake newsów*, postprawdy, propagandy i populizmu)[61], jak i przyjmuje się sposób definiowania zbiorczego, jak np. w przypadku propagandy i dezinformacji w projekcie Doktryny Bezpieczeństwa Informacyjnego[62]. Niektórzy badacze przyjmują, że stosowanie *fake news* ma na celu „wywołanie określonych emocji i nastawienia do danej sprawy”[63], w innej percepcji jest to środek umożliwiający osiągnięcie celu, który ma wymiar finansowy: „strony [internetowe] zawierające *fake news* tworzone są głównie w celach zarobkowych”[64].

Niezależnie od tego, jak te zjawiska są definiowane i jaka towarzyszy im typologia, są to zagrożenia istniejące w przestrzeni informacyjnej. Przyjęcie technicznej (cybernetycznej) percepcji bezpieczeństwa informacyjnego, zatem skupienie uwagi na kanale i pominięcie lub marginalizowanie treści, może utrudnić zwalczanie tej grupy zagrożeń. Posiadanie jedynie zdolności do rozwijania kanałów przesyłania informacji oraz do zapewniania tym kanałom bezpieczeństwa nie uchroni danego podmiotu przed stanowiącymi realne bądź potencjalne zagrożenie informacjami rozpowszechnianymi za ich pośrednictwem. Do tego potrzebna jest zdolność danego podmiotu do identyfikowania i umiejętnego zwalczania treści fałszywych.

---

[58] *Ibidem.*

[59] W. Głodowski, *Komunikowanie interpersonalne*, Warszawa 2001, s. 17.

[60] P. Sienkiewicz, H. Świeboda, E. Szczepaniuk, *Informacyjny wymiar bezpieczeństwa państwa* [w:] *Teoretyczne podstawy bezpieczeństwa informacyjnego państwa. Praca naukowo-badawcza*, Warszawa 2013, s. 15.

[61] M. Waszak, *Postprawda i fake news czy weryfikacja treści i źródeł informacji?* „Refleksje” 16/2017, s. 175.

[62] *Projekt Bezpieczeństwa Informacyjnego…, op. cit.,* s. 4.

[63] *Fake news z perspektywy polskich dziennikarzy*, „Public Dialog”, 2017, s. 6, za: http://publicdialog.home.pl/www_logotomia/wp-content/uploads/2018/07/Raport_Badanie-fake-news-23-05-2017.pdf (09.04.2020).

[64] B. Łódzki, *Fake news – dezinformacja w mediach internetowych i formy jej zwalczania w przestrzeni międzynarodowej*, „Polityka i Społeczeństwo” 4(15)/2017, s. 22.

Tożsama konstatacja towarzyszy rozważaniom nad polityką historyczną rozpatrywaną w kontekście bezpieczeństwa informacyjnego. Sprzężenie polityki historycznej z mediami masowymi może prowadzić zarówno do szans (np. w zakresie kreowania polskiego *soft power*), jak i do zagrożeń w obszarze bezpieczeństwa informacyjnego. Przykładem takich zagrożeń mogą być pojawiające się pod koniec 2019 r. i na początku 2020 r. próby obarczenia Polski współodpowiedzialnością za wybuch II wojny światowej oraz Holokaust. Były to działania stanowiące zagrożenie nie tylko w zakresie bezpieczeństwa informacyjnego. Obecne w przestrzeni informacyjnej zagrożenia mogły negatywnie oddziaływać na wizerunek Polski na płaszczyźnie międzynarodowej oraz stanowiły potencjalne zagrożenie intensyfikacji wewnątrzkrajowych konfliktów politycznych (dotyczących tego, czy reakcja polskich władz była właściwa, czy też nie). Ponownie nie sposób uznać, żeby techniczna (cybernetyczna) percepcja bezpieczeństwa informacyjnego wystarczyła do zapobiegania, diagnozowania oraz zwalczania tego typu zagrożeń pojawiających się w przestrzeni informacyjnej.

Formułowane względem Polski przez W. Putina oskarżenia dotyczące zagadnień historycznych są elementem właściwego dla obecnych władz Federacji Rosyjskiej relatywizowania historii, czy też – używając publicystycznego określenia – pisania jej na nowo. Można zatem zakładać, że takie wymierzone w Polskę działania rosyjskich elit politycznych będą również pojawiać się w przyszłości[65]. Oznacza to, że samo rozwijanie zdolności do technicznego zapewniania bezpieczeństwa informacyjnego (np. w zakresie zwalczania tzw. trolli w nowych mediach) jest działaniem niewystarczającym.

Jak zauważono powyżej, zagrożenia w przestrzeni informacyjnej mogą oddziaływać negatywnie na wizerunek Polski. Negatywne oddziaływanie na płaszczyźnie wizerunkowej może dotyczyć nie tylko państwa jako całości, ale również poszczególnych instytucji, w tym instytucji zapewniających bezpieczeństwo. Dla takich instytucji jak np. wojsko, wizerunek jest elementem użytecznym w zakresie wspomagania działań, takich jak rekrutacja, modernizacja, sytuacje kryzysowe, walka informacyjna, czy też komunikowanie strategiczne[66]. Zagrożenia wizerunkowe mogą zatem utrudnić realizację działań ważnych dla bezpieczeństwa państwa. Zagrożenia te mogą powstawać za sprawą np. rozpowszechnianej w przestrzeni informacyjnej dezinformacji dotyczącej działań poszczególnych instytucji, upolitycznienia ich wizerunku (np. wojska jako całości lub Wojsk Obrony Terytorialnej), czy też prób wykazania niekompetencji. W takich sytuacjach ponownie należy uznać, że postrzeganie bezpieczeństwa informacyjnego przez pryzmat techniczny (cybernetyczny) nie uchroni przed takimi zagrożeniami – aby im przeciwdziałać potrzebne są działania związane z treścią, nie tylko z kanałami jej przesyłania.

Ostatni postulat koresponduje z istotą komunikowania oraz procesualnym postrzeganiem bezpieczeństwa. W przypadku komunikowania przyjmuje się, że jest to proces ciągły[67], przy określaniu istoty bezpieczeństwa zwraca się uwagę na to, że jest to zarówno stan, jak i proces. Procesualny wymiar bezpieczeństwa oznacza m.in. aktywność danego podmiotu w zakresie dążenia do pożądanego stanu bezpieczeństwa – postrzega się w ten sposób np. bezpieczeństwo narodowe[68], czy też bezpieczeństwo militarne[69].

---

[65] Założenie to bazuje nie tylko na dotychczasowym wykorzystywaniu przez Federację Rosyjską polityki historycznej do ataków na inne państwa, ale też np. na analizie zmian koncepcji nauczania historii w rosyjskich szkołach średnich. Zmiany te mogą prowadzić do utrwalenia wśród rosyjskiego społeczeństwa imperialnego postrzegania własnej historii i upowszechnienia tendencji do obarczania innych państw odpowiedzialnością za to, co było w historii złe, por. D. Moskwa, *„Putinowska" wizja przeszłości. Nowa koncepcja nauczania historii w świetle polityki historycznej Federacji Rosyjskiej*, „Historia i Polityka" 11(18)/2014.

[66] Por. G. Klein, *Kształtowanie wizerunku Wojska Polskiego jako instytucji zapewniającej bezpieczeństwo*, Warszawa 2019.

[67] B. Dobek-Ostrowska, *Podstawy komunikowania społecznego*, Wrocław 1999, s. 14-15.

[68] W. Kitler, *Bezpieczeństwo Narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011, s. 30.

[69] R. Szpyra, *Bezpieczeństwo militarne państwa*, Warszawa 2012, s. 97.

Przyjęcie perspektywy bezpieczeństwa informacyjnego jako stanu i procesu oznacza m.in. możliwość postrzegania kreowania własnych komunikatów (treści) w kategoriach ciągłej aktywności. Oznacza również percepcję tego obszaru nie tylko w kategoriach defensywnych (obrony przed zagrożeniami), ale także w wymiarze ofensywnym. Umożliwia to projektowanie i realizowanie własnych działań, np. w zakresie dezinformacji. Aktywność w obszarze bezpieczeństwa informacyjnego to również możliwości kreacyjne, m.in. w zakresie kreowania wizerunku państwa oraz kształtowania polskiego *soft power*, np. poprzez promowanie własnej polityki historycznej.

Wnioski

Badania zrekapitulowane w niniejszym artykule doprowadziły do pozytywnej weryfikacji przyjętej hipotezy badawczej, zgodnie z którą bezpieczeństwo informacyjne Polski w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej można identyfikować w sposób interdyscyplinarny, łączący podejścia właściwe dla komunikowania społecznego oraz nauk o bezpieczeństwie. W polskim piśmiennictwie dominuje postrzeganie bezpieczeństwa informacyjnego przez pryzmat aspektów technicznych (cybernetycznych). Oznacza to skupienie uwagi badaczy na kanałach służących do przesyłania treści (informacji), przy jednoczesnym pomijaniu bądź marginalizowaniu treści. Przyjmując perspektywę interdyscyplinarną, uwzględniającą komunikowanie społeczne można prowadzić badania w tym obszarze uwzględniając obydwa elementy.

W artykule podjęto próbę wykazania użyteczności takiej percepcji badanego obszaru, przede wszystkim w kontekście wschodnioeuropejskich zagrożeń w przestrzeni informacyjnej (*fake newsy*, dezinformacja, manipulowanie historią *etc*.). Podjęto również próbę wykazania szans związanych z taką percepcją badanego obszaru, m.in. w zakresie własnych działań kreacyjnych (związanych np. z *soft power*) i ofensywnych (np. dezinformacja). Zapobieganie wymienionym zagrożeniom i ich zwalczanie, jak również wykorzystywanie przedstawionych szans jest procesem możliwym do zrealizowania wówczas, kiedy treść jest postrzegana jako kategoria bezpieczeństwa informacyjnego równie ważna, jak kanały przesyłania komunikatów.

Streszczenie:

Celem artykułu jest analiza bezpieczeństwa informacyjnego w Polsce. Autor opisuje definicje bezpieczeństwa informacyjnego z wyróżnionymi elementami ważnymi w kontekście komunikowania społecznego oraz cechy bezpieczeństwa informacyjnego w ujęciu teoretycznym.

Słowa kluczowe:

Bezpieczeństwo informacyjne, półprawda, populizm,

Keywords:

Security of information, fake news, populism

Bibliografia:

1. Batorowska H., *Bezpieczeństwo informacyjne w dyskursie naukowym - kierunki badań* [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków 2017.
2. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013.
3. Cieślarczyk M., *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce-Warszawa 2016.
4. Darczewska J., *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku*, „Punkt widzenia" 2014, nr 42, Warszawa.
5. Dobek-Ostrowska B., *Podstawy komunikowania społecznego*, Wrocław 1999.
6. *Fake news z perspektywy polskich dziennikarzy* „Public Dialog" 2017, za: http://publicdialog.home.pl/www_logotomia/wp-content/uploads/2018/07/Raport_Badanie-fake-news-23-05-2017.pdf.
7. Fehler W., *O pojęciu bezpieczeństwa informacyjnego* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce-Warszawa 2016.
8. Geers K., *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn 2015.
9. Głodowski W., *Komunikowanie interpersonalne*, Warszawa 2001;
10. Janczak J. Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013.
11. Kitler W., *Bezpieczeństwo Narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Warszawa 2011.
12. Klein G., *Kształtowanie wizerunku Wojska Polskiego jako instytucji zapewniającej bezpieczeństwo*, Warszawa 2019.
13. Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, Warszawa 2012.
14. Łódzki B., *Fake news – dezinformacja w mediach internetowych i formy jej zwalczania w przestrzeni międzynarodowej*, „Polityka i Społeczeństwo" 4(15)/2017.
15. Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego* [w:] *Bezpieczeństwo teleinformatyczne państwa*, Warszawa.
16. Moskwa D., *„Putinowska" wizja przeszłości. Nowa koncepcja nauczania historii w świetle polityki historycznej Federacji Rosyjskiej*, „Historia i Polityka" 11(18)/2014.
17. Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.
18. Polończyk A., *Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa* [w:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, Kraków 2017.
19. Potejko P., *Bezpieczeństwo informacyjne* [w:] *Bezpieczeństwo państwa*, Warszawa 2009.
20. *Projekt Bezpieczeństwa Informacyjnego Rzeczypospolitej Polskiej*, Warszawa 2015, za: https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.
21. Samadashvili S., *Muzzling the Bear. Strategic Defence for Russia's Undeclared War on Europe*, Bruksela, 2015.
22. Sienkiewicz P., Świeboda H., Szczepaniuk E., *Informacyjny wymiar bezpieczeństwa państwa* [w:] *Teoretyczne podstawy bezpieczeństwa informacyjnego państwa. Praca naukowo-badawcza*, Warszawa 2013.
23. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2014.
24. Szpyra R., *Bezpieczeństwo militarne państwa*, Warszawa 2012;

25. Waszak M., *Postprawda i fake news czy weryfikacja treści i źródeł informacji?* „Refleksje” 16/2017.
26. Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki Kolegium Analiz Ekonomicznych” 29/2013.