

JOLANTA SALA

Wydział Zarządzania
Powiślańska Szkoła Wyższa

HALINA TAŃSKA

Wydział Matematyki i Informatyki
Uniwersytet Warmińsko-Mazurski w Olsztynie

Spółeczno-gospodarcze bezpieczeństwo informacyjne w kontekście zatrucia informacyjnego

1. Wstęp

Aktualnie w obszarze geopolitycznym Polski bardzo realne stały się wszelkie analizy bezpieczeństwa. Przeprowadzenie takiej analizy, podobnie jak analizy ryzyka, jest uwarunkowane posiadaniem przynajmniej dwóch atrybutów – wiedzy i świadomości zagrożeń. Zbyt wolno w porównaniu z rzeczywistą sytuacją zagrożenia militarne rośnie powszechna świadomość i zapotrzebowanie na analityków bezpieczeństwa militarne terytorium kraju i kontynentu. Ponadto zbyt mało powszechna jest świadomość potrzeby tego, aby obok bezpieczeństwa sfery materialnej zająć się także bezpieczeństwem sfery informacyjnej.

W niniejszym artykule autorki skupiają się na absolutnych fundamentach bezpieczeństwa sfery informacyjnej. Kluczowym przesłaniem opracowania jest przypomnienie faktu, iż bezpieczeństwo nie jest obszarem zarezerwowanym dla specjalistów z poszczególnych sektorów, tj. wojska, straży pożarnej, policji itp., ale ma charakter interdyscyplinarny i dotyczy wszystkich, a przede wszystkim jest bezpośrednio związane z technologiami ICT (ang. *Information and Communication Technologies*).

2. Bezpieczeństwo informacyjne i jego skala

Przywołanie słowa „bezpieczeństwo” powoduje różne skojarzenia, którym towarzyszą różne teorie. Dla przykładu, w psychologii i zarządzaniu najczęściej jest stosowany model piramidy potrzeb A. Maslowa (w którym podstawę hierarchii tworzą potrzeby fizjologiczne i bezpieczeństwa). W socjologii i ekonomii liczy się naukowa teoria kultury B. Malinowskiego. Teoria polskiego antropologa społecznego i ekonomicznego jest ceniona w szczególności w Wielkiej Brytanii. Zidentyfikował on m.in. siedem potrzeb¹ oraz siedem odpowiadających im imperatywów kulturowych, wśród których bezpieczeństwo ma swoje antropologiczne ujęcie².

Niewątpliwie bezpieczeństwo jest bardzo ważnym stanem i jedną z podstawowych potrzeb człowieka. Jest ono istotne nie tylko dla człowieka, ale także dla grup społecznych, państw i systemów międzynarodowych. Daje ono poczucie pewności istnienia oraz gwarancji jego zachowania, a również stanowi szansę na doskonalenie. Zaspokojenie potrzeby bezpieczeństwa wymaga inteligentnego oddziaływania na otoczenie, będące współczesną cywilizacją, składającą się ze skomplikowanych systemów politycznych, gospodarczych, technicznych i społecznych. Inteligentne oddziaływania można rozumieć bardzo różnie.

Ostatnio przedstawiciele życia społeczno-gospodarczego skupiają się nad przekonującą propozycją serii norm ISO/IEC 27000 związanych z bezpieczeństwem oraz podobnych inicjatyw dotyczących dobrych praktyk dopasowanych do specyfiki podmiotu i przedmiotu. Normy te w sposób wyrazisty eksponują znaczenie bezpieczeństwa informacji³ wraz z bezpieczeństwem materialnym. Model bezpieczeństwa informacji w organizacji obejmuje ludzi, procesy i technologie.

¹ Encyklopedyczna synteza teorii kultury B. Malinowskiego podaje siedem potrzeb (metabolizm, reprodukcja, odpowiednie warunki fizyczne, bezpieczeństwo, ruchliwość, rozwój, zdrowie) oraz siedem odpowiadających im imperatywów kulturowych (zaopatrzenie, małżeństwo i rodzina, mieszkanie i ubranie, ochrona i obrona, aktywność i komunikacja, przyuczanie i szkolenie, higiena).

² J. Szacki, *Historia myśli socjologicznej*, Wydawnictwo Naukowe PWN, Warszawa 2015, s. 660–663.

³ Zgodnie z normą ISO 27002 0.1 informacje to aktywa, które – podobnie jak inne ważne aktywa biznesowe – są niezbędne do działalności biznesowej organizacji, i z tego powodu zaleca się ich odpowiednią ochronę. W konsekwencji za bezpieczeństwo informacji w normie tej uznaje się zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność, niezawodność.

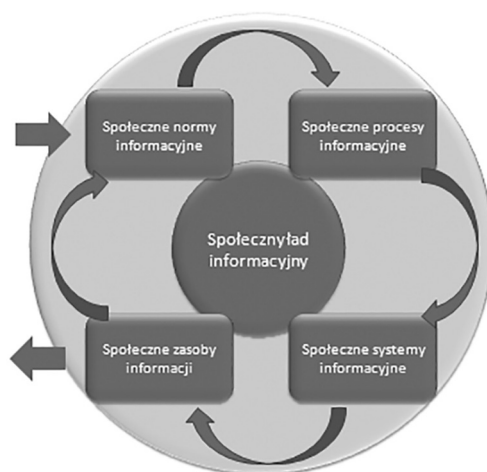
Należy podkreślić fakt, że wysiłki wdrożeniowe dotyczące owych norm są rozproszone w poszczególnych podmiotach życia społeczno-gospodarczego. Oczywiście podobnie rozproszone są zabiegi poszczególnych obywateli dbających o bezpieczeństwo swoich rodzin zgodnie z dostępnymi wzorcami. Można powiedzieć, że są to zabezpieczenia małej skali na miarę relatywnie małych możliwości. Natomiast bezpieczeństwo państw i systemów międzynarodowych jest szczególnie złożonym zagadnieniem dużej skali wobec globalizacji oraz rozwoju społeczeństwa informacyjnego i technologii ICT. Obecnie tradycyjne aspekty zachowania bezpieczeństwa państwa są rozszerzane o bezpieczeństwo informacyjne, bezpośrednio związane z walką informacyjną⁴.

Normy i wzorce spełniające uniwersalne potrzeby bezpieczeństwa człowieka i organizacji nie uwzględniają specyficznych uwarunkowań miejsca i związanej z nim kultury, która jest kluczem do zaspokojenia potrzeb i zespołem reakcji na te potrzeby. Zgodnie z teorią B. Malinowskiego umiejętność opisanie kultury jest tożsama z opisaniem warunków, jakie muszą być spełnione, aby zbiorowość była w stanie przetrwać. Podążając w tym kierunku, warto więc wyodrębnić bezpieczeństwo zarówno małej, jak i dużej skali, zachowując podstawowy aksjomat teorii systemów, że suma bezpiecznych elementów systemu nie jest tożsama z bezpieczeństwem tego systemu. W konsekwencji należy odnotować, że wdrażanie norm i dobrych praktyk przeznaczonych dla organizacji jest namiastką bezpieczeństwa w skali państwa.

Ponadto warto zauważyć, iż istniejące wzorce dotyczą ochrony posiadanych informacji, a nie uwzględniają zagrożeń wynikających z nieposiadania informacji lub posiadania informacji, które nie odwzorowują rzeczywistości. W sposób istotny wzmacnia to konieczność kompleksowego ujęcia systemowego. Warunki te spełnia koncepcja J. Oleńskiego, który zidentyfikował i zdefiniował „społeczny ład informacyjny” w państwie i gospodarce⁵. Rysunek 1 obrazuje składowe kompleksowego i spójnego systemu, jakim jest społeczny ład informacyjny w państwie, społeczeństwie, gospodarce narodowej oraz w skali międzynarodowej, ponieważ zaspokajają potrzeby informacyjne ludzi, podmiotów gospodarki narodowej i instytucji sfery publicznej.

⁴ D.E. Denning, *Walka informacyjna i bezpieczeństwo informacyjne*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002; A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki” Kolegium Analiz Ekonomicznych, nr 29, Oficyna Wydawnicza SGH, Warszawa 2013, s. 448–463.

⁵ J. Oleński, *Elementy ekonomiki informacji. Podstawy ekonomiczne informatyki gospodarczej*, Katedra Informatyki Gospodarczej i Analiz Ekonomicznych, Wydział Nauk Ekonomicznych, Uniwersytet Warszawski, Warszawa 2000.



Rysunek 1. Składowe społecznego ładu informacyjnego

Źródło: opracowanie na podstawie: J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Nowy Dziennik sp. z o.o., Uniwersytet Warszawski, Warszawa 2006, s. 20.

Według koncepcji J. Oleńskiego składowe społecznego ładu informacyjnego stanowią społeczne normy, procesy i systemy informacyjne oraz zasoby informacji. Na najwyższym poziomie abstrakcji jest zgodność pomiędzy zobowiązaniem bezpieczeństwa informacji w organizacji oraz społecznym bezpieczeństwem informacyjnym dla społecznego ładu informacyjnego.

3. Zatrucie informacyjne – zatruta infosfera

W latach 50. XXw. twórca cybernetyki, N. Wiener, wyraził przekonanie, że „społeczeństwo można zrozumieć jedynie poprzez studiowanie informacji oraz związanych z nimi sposobów porozumiewania się”⁶. Pojęcie infosfery upowszechnił w świecie A. Tofler na progu intensywnego rozwoju technologii ICT w latach 80. XXw. Na zatrutą infosferę wskazywał A. Lepa w latach 90. XXw. w kontekście przemian społeczno-gospodarczych w Polsce⁷. Z perspektywy połowy drugiej dekady XXI w. są to trzy symboliczne momenty, które ujawniają dystans czasowy skutków zatrucia infosfery w postaci „mentalności propagandowej” w naszym kraju. Niewątpliwie jedną z istotnych przyczyn trudności

⁶ N. Wiener, *Cybernetyka a społeczeństwo*, Książka i Wiedza, Warszawa 1961, s. 16.

⁷ A. Lepa, *Mass media i zatruta infosfera*, „Ład” 1993, nr 40.

dotyczących przemian społeczno-gospodarczych w Polsce jest zidentyfikowanie faktu, iż społeczeństwo postkomunistyczne „nadal zdradza postawę daleko posuniętej uległości wobec działań propagandowych”⁸.

J. Kossecki twierdzi, że propaganda ma zasadnicze znaczenie „zarówno dla walki informacyjnej, jak i dla wszelkich procesów sterowniczych w społeczeństwie”, i definiuje ją jako „planowe oddziaływanie na psychikę ludzi za pomocą odpowiednich bodźców o charakterze informacyjnym, zmierzające do wywołania u nich odpowiednich działań lub ukształtowania odpowiednich norm”⁹. Natomiast A. Lepa woli definiować propagandę jako „zaplanowane oddziaływanie na daną społeczność odpowiednich treści perswazyjnych, prowadzące poprzez urabianie postaw i opinii do wywołania oczekiwanych decyzji i zachowań”, dodając, iż „postawy i opinie stanowią liczącą się warstwę osobowości człowieka”¹⁰. Kolejne doświadczenia związane z globalnym rozwojem technologii ICT skutkowały badaniami światowej sławy socjologa i ekonomisty M. Castellsa, który przestrzega przed zapomnieniem „o najstarszej i najbardziej bezpośredniej formie polityki medialnej: propagandzie i kontroli”. Propagandę definiuje on jako „fabrykowanie i rozpowszechnianie komunikatów, które zniekształcają fakty i prowadzą do dezinformacji służącej interesom rządów”, natomiast kontrolowanie jako „cenzurowanie wszelkich komunikatów, które uważa się za zagrożenie dla tych interesów – jeśli to konieczne, poprzez kryminalizację swobodnej komunikacji i ściganie nadawców”¹¹.

Wydaje się, iż wspólnym mianownikiem owej różnorodności stanowisk jest hierarchia funkcji informacji, zobrazowana na rysunku 2. Społeczny ład informacyjny jest uwarunkowany zachowaniem tej hierarchii. Jeżeli odwzorowanie rzeczywistości (funkcja 1) jest zniekształcone (zmanipulowane) działaniami „aparatu propagandy”, to zakłócony jest cały społeczny ład informacyjny poprzez błędy funkcjonalne (funkcje 2–5). Zatruty jest cały system społecznej informacji, który jest dla życia społeczno-gospodarczego tym, czym układ nerwowy dla człowieka (metaforą „układ nerwowy społeczeństwa” posłużył się m.in. J. Dijk¹²).

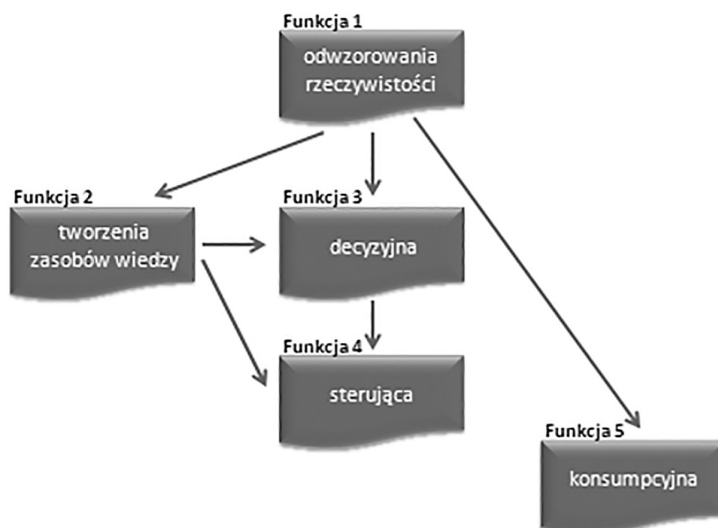
⁸ A. Lepa, *Świat propagandy*, KM, Częstochowa 2008, s. 35.

⁹ J. Kossecki, *Cybernetyka społeczna*, PWN, Warszawa 1975, s. 419.

¹⁰ A. Lepa, *Świat...*, op.cit., s. 16.

¹¹ M. Castells, *Władza komunikacji*, Wydawnictwo Naukowe PWN, Warszawa 2013, s. 266.

¹² J. Dijk, *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci*, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 35.



Rysunek 2. Hierarchia funkcji informacji warunkująca ład informacyjny

Źródło: opracowanie na podstawie: J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Nowy Dziennik sp. z o.o., Uniwersytet Warszawski, Warszawa 2006, s. 68.

Dzięki diagramowi hierarchii funkcji informacji J. Oleńskiego łatwiej wyobrazić sobie zjawisko zatrutej infosfery, zwane inaczej zatruciem informacyjnym, które A. Lepa identyfikuje w dwóch perspektywach, jako:

- skutek działań propagandy;
- technika działań propagandy¹³.

Główny mechanizm zjawiska zatrucia informacyjnego polega na tym, że sprawy ważne i bardzo ważne ukazuje się celowo jako mało istotne, a nawet bez żadnej wartości. I odwrotnie: sprawy niewiele liczące się w życiu człowieka i społeczeństwa przedstawia się jako problemy najwyższej wagi. Zatrucie informacyjne stanowi tylko jedno oblicze propagandy, ale jest ono bardzo groźne dla rozwoju osobowego człowieka, gdyż może spowodować zniekształcenia w hierarchii jego wartości i w obrębie postaw, tj. może m.in. zagrozić krytycyzmowi, niezależności myślenia, zdolności dokonywania selekcji informacji.

Warto podkreślić fakt, że perswazja propagandowa wykazuje bardzo „różnicowane formy oddziaływania: od finezyjnej treści komunikatu agencyjnego przez powszechnie stosowane manipulacje aż po brutalne »pranie mózgu«” oraz duży stopień powszechności i skuteczności¹⁴. Ponadto istotne jest to, iż te formy

¹³ A. Lepa, *Świat...*, op.cit., s. 122.

¹⁴ Ibidem, s. 18.

oddziaływania powstają w wyniku wykorzystania nie jednej lub kilku technik propagandy, lecz całego instrumentarium. Według A. Lepy na podstawowe mechanizmy składają się trzy grupy instrumentów, tj. środki (4), zasady (12) i techniki (21), które są stosowane w różnych kombinacjach i stanowią bazę do generowania nowych mechanizmów¹⁵.

Niestety to zasygnalizowane instrumentarium propagandy ma codzienny i bezpośredni wpływ na społeczny ład informacyjny. W różnych krajach wykorzystuje się je w różnych momentach z różnym natężeniem. M. Castells wybrał trzy zróżnicowane konteksty i przeprowadził analizę funkcjonowania propagandy w USA, Rosji i Chinach¹⁶. Państwa demokratyczne, z pluralistycznym zasobem multimediów lub – jak woli J. Oleński – z informacyjną infrastrukturą dostosowaną do potrzeb, gwarantują swojemu społeczeństwu i gospodarce mniejszy stopień zagrożenia oraz większy poziom bezpieczeństwa informacyjnego wobec wewnętrznych i zewnętrznych globalnych oddziaływań propagandowych powodujących zatrucie informacyjne.

W Polsce zatrucie informacyjne jest znacznie groźniejsze niż w wysoko rozwiniętych państwach demokratycznych. Ciekawy wymiar bezpieczeństwa w Polsce stanowi interpretacja badań dotyczących społeczeństwa informacyjnego opracowana przez Ministerstwo Administracji i Cyfryzacji (MAC) w podziale na trzy cele strategiczne z obszarów „człowiek–gospodarka–państwo”¹⁷. Jednym z sześciu celów działania z obszaru „człowiek”, za które odpowiada MAC, jest „podniesienie poczucia bezpieczeństwa w społeczeństwie poprzez wykorzystanie technologii informacyjnych i komunikacyjnych”. Wyniki badań i wnioski z nich płynące świadczą o istnieniu stanu bliskiego ideałowi¹⁸. W opracowaniu tym przedstawiono m.in. badania CBOS (z okresu 2007–2014) dotyczące poczucia bezpieczeństwa wśród Polaków, którzy w 2014 r. na pytanie „Czy Pana(i) zdaniem Polska jest krajem, w którym żyje się bezpiecznie?” odpowiedzieli „tak” w 70%, „nie” w 24%, a reszta miała trudności z odpowiedzią. Podobnie bardzo wysokie poczucie bezpieczeństwa potwierdzają odpowiedzi udzielone CBOS na pytanie o charakterze lokalnym: „Czy miejsce, w którym Pan(i) mieszka, można nazwać bezpiecznym i spokojnym?”, ponieważ 90% pytanych odpowiedziało twierdząco, 9% – zaprzeczyło, a tylko 1% osób miało trudności z odpowiedzią. Badania te są prowadzone od 1987 r. i ich wyniki potwierdzają to, że jest coraz

¹⁵ Ibidem, s. 68–101.

¹⁶ M. Castells, op.cit., s. 266–286.

¹⁷ *Społeczność informacyjne w liczbach 2014*, red. V. Szymanek, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014.

¹⁸ Ibidem, s. 71–75.

bezpieczniej i spokojniej. Ponadto w większości Polacy nie obawiają się (61% w 2014 r.) tego, że mogą stać się ofiarą przestępstwa (te badania przeprowadza się od 1996 r. i one także wskazują na to, że sytuacja do 2014 r. stopniowo poprawiała się). MAC posłużyło się także wynikami badań OBOP, które są prowadzone od 2002 r. Monitorowane są opinie dotyczące tego, „czy dzięki nowym technologiom, takim jak Internet i telefonia komórkowa, świat staje się lepszy czy też gorszy”. Na 4-stopniowej skali (lepszy; gorszy; ani lepszy, ani gorszy; trudno powiedzieć) w 2014 r. kolejno wskazano: 41%, 17%, 38% i 4%. W przypadku tych badań wyniki nieco pogorszyły się (np. w 2012 r. było to: 53%, 13%, 29%, 5%). W opracowaniu powołano się jeszcze na badania własne MAC w zakresie bezpieczeństwa korzystania z usług w Internecie (sięgnięto po skalę od 1 do 10). Wybrano następujące obszary: bankowość, zakupy, sprawy urzędowe i ochrona zdrowia. Średnie oceny były następujące: 7,4; 7,3; 6,1; 6. Natomiast na najwyższe oceny w skali od 1 do 5 wskazało kolejno 82%, 83%, 60% i 57% osób. Podano jeszcze dwie interpretacje w zbliżonym kontekście oraz z doskonałym zobrazowaniem graficznym badań.

Powyższe wyniki i ich interpretacje posłużyły MAC do podsumowania działań mających służyć podniesieniu poczucia bezpieczeństwa w polskim społeczeństwie poprzez wykorzystanie technologii informacyjnych i komunikacyjnych. Podano wartość wskaźnika w 2014 r. na poziomie 70% oraz jego poziom docelowy 78% (w strategii do 2013 r.) oraz uznano, iż zabrakło „8 punktów procentowych, aby uznać, że cel 4 został zrealizowany”¹⁹. Bez wątpienia opracowanie jest doskonałym przykładem wykorzystania instrumentarium propagandy przyczyniającego się do zatrucia informacyjnego. Powyższe interpretacje dziwią m.in. z powodu rozbieżności pomiędzy opiniami nieoficjalnymi i oficjalnymi. Przyczyn tych rozbieżności jest kilka. Pierwszym powodem znacznego zagrożenia życia społeczno-gospodarczego zatrutą infosferą jest bardzo niedoskonała informacyjna infrastruktura państwa, a drugim – niska odporność społeczna na oddziaływanie propagandy, jako pozostałość historyczna odznaczająca się zakłóconym poziomem zaufania²⁰.

¹⁹ Ibidem, s. 79.

²⁰ Autorki szczegółowo podejmowały te zagadnienia m.in. w następujących publikacjach: J. Sala, H. Tańska, *Pomiędzy utopią a rzeczywistością rozwoju społeczeństwa informacyjnego*, w: *Drogi do dochodzenia do społeczeństwa informacyjnego. Stan obecny, perspektywy rozwoju i ograniczenia*, red. H. Babis, R. Czaplowski, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, nr 650, „Ekonomiczne Problemy Usług”, nr 67, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2011, s. 195–202; J. Sala, H. Tańska, *Syndrom „kota w worku” w społeczeństwie informacyjnym*, w: *Społeczeństwo informacyjne w świecie rzeczywistym i wirtualnym*, red. A. Szewczyk, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, nr 656, „Studia

4. Podsumowanie i kierunki dalszych badań

Kontekst zatrucia informacyjnego w Polsce wielokrotnie stanowił dla autorek niniejszego artykułu barierę w badaniach naukowych, edukacji i eksperymentach w praktyce społeczno-gospodarczej. Niemniej w XXI w. wraz z gwałtownym rozwojem technologii ICT coraz groźniejsze stają skutki tego zatrucia (autorki badały niektóre z nich²¹). Niemniej obecnie ma miejsce kumulacja tak wielu negatywnych skutków, iż wymaga ona holistycznego ujęcia. Stanowi poważne zagrożenie społeczno-gospodarczego bezpieczeństwa informacyjnego w Polsce.

Konieczna jest naprawa stanu społecznego ładu informacyjnego przy zachowaniu uwarunkowań hierarchii funkcji informacji ze wskazaniem bezwzględniego priorytetu w postaci rzetelnego odwzorowania rzeczywistości (funkcja 1, rysunek 2). Konieczność ta dotyczy zarówno poszczególnych podmiotów społeczno-gospodarczych, jak i całego państwa. Autorki planują kontynuację badań w tym zakresie, w szczególności w kontekście luki informacyjnej i minimum informacyjnego.

Bibliografia

- Castells M., *Władza komunikacji*, Wydawnictwo Naukowe PWN, Warszawa 2013.
- Denning D.E., *Walka informacyjna i bezpieczeństwo informacyjne*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
- Dijk J., *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci*, Wydawnictwo Naukowe PWN, Warszawa 2010.
- Kossecki J., *Cybernetyka społeczna*, PWN, Warszawa 1975.
- Lepa A., *Mass media i zatruta infosfera*, „Ład” 1993, nr 40.
- Lepa A., *Świat propagandy*, KM, Częstochowa 2008.
- Oleński J., *Elementy ekonomiki informacji. Podstawy ekonomiczne informatyki gospodarczej*, Katedra Informatyki Gospodarczej i Analiz Ekonomicznych, Wydział Nauk Ekonomicznych, Uniwersytet Warszawski, Warszawa 2000.

Informatica”, nr 28, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2011, s. 455–465.

²¹ Zob. wyniki tych badań m.in. w: J. Sala, H. Tańska, *Procesy integracji w gospodarce sieciowej*, w: *E-gospodarka w Polsce. Stan obecny i perspektywy*, red. H. Babis, J. Buko, R. Czaplewski, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, nr 597, cz. 1, „Ekonomiczne Problemy Usług”, nr 57, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2010, s. 689–698.

- Oleński J., *Infrastruktura informacyjna państwa w globalnej gospodarce*, Nowy Dziennik sp. z o.o., Uniwersytet Warszawski, Warszawa 2006.
- Sala J., Tańska H., *Pomiędzy utopią a rzeczywistością rozwoju społeczeństwa informacyjnego*, w: *Drogi do dochodzenia do społeczeństwa informacyjnego. Stan obecny, perspektywy rozwoju i ograniczenia*, red. H. Babis, R. Czaplewski, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, nr 650, „Ekonomiczne Problemy Usług”, nr 67, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2011, s. 195–202.
- Sala J., Tańska H., *Procesy integracji w gospodarce sieciowej*, w: *E-gospodarka w Polsce. Stan obecny i perspektywy*, red. H. Babis, J. Buko, R. Czaplewski, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, nr 597, cz. 1, „Ekonomiczne Problemy Usług”, nr 57, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2010, s. 689–698.
- Sala J., Tańska H., *Syndrom „kota w worku” w społeczeństwie informacyjnym*, w: *Społeczeństwo informacyjne w świecie rzeczywistym i wirtualnym*, red. A. Szewczyk, „Zeszyty Naukowe” Uniwersytetu Szczecińskiego, nr 656, „Studia Informatica”, nr 28, Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 2011, s. 455–465.
- Społeczeństwo informacyjne w liczbach 2014*, red. V. Szymanek, Ministerstwo Administracji i Cyfryzacji, Warszawa 2014.
- Szacki J., *Historia myśli socjologicznej*, Wydawnictwo Naukowe PWN, Warszawa 2015.
- Wiener N., *Cybernetyka a społeczeństwo*, Książka i Wiedza, Warszawa 1961.
- Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Roczniki” Kolegium Analiz Ekonomicznych, nr 29, Oficyna Wydawnicza SGH, Warszawa 2013, s. 448–463.

* * *

Socio-economic information security in the context of information poisoning

Summary

The article attempts to identify the foundations of contemporary information security at the level of economic and social players and of the entire state. The axiom of that identification is the anthropological and cultural approach to security developed by B. Malinowski. The basis is the concept of social information governance developed by J. Oleński and his hierarchy of information functions model. The main context of information security identification is information poisoning equated with propaganda. This context is in the global dimension supported by the analytical research results of M. Castells and the national specifics stemming from own research.

Keywords: information security, information governance, hierarchy of functions of information, information poisoning, propaganda