„Polityka i Społeczeństwo" 3(22) / 2024
DOI: 10.15584/polispol.2024.3.2

ARTYKUŁY

Robert Białoskórski*

STRUKTURALNA (HOLISTYCZNA) KONCEPCJA DEFINIOWANIA BEZPIECZEŃSTWA INFORMACYJNEGO

Streszczenie

W artykule przedstawiono strukturalną (holistyczną) koncepcję metody definiowania bezpieczeństwa informacyjnego opartą na strukturze bazowej złożonej z relacji trzech składowych determinantów: społeczeństwa informacyjnego, przestrzeni informacyjno-komunikacyjnej (infosfery) oraz zagrożeń bezpieczeństwa informacyjnego. Te trzy składowe rozpatrywane są w relacyjnym aspekcie zasobów informacyjnych i wartości informacyjnych (ludzi, infrastruktury, technologii, wiedzy i etyki). Zaproponowana w konkluzjach definicja bezpieczeństwa informacyjnego doprowadziła do opracowania relacyjnych kategorii bezpieczeństwa informacyjnego skorelowanych w fizycznej i wirtualnej sferze przestrzeni informacyjno-komunikacyjnej (infosferze). Wyniki badań pokazały, że strukturalne (holistyczne) podejście do definiowania bezpieczeństwa informacyjnego wyróżnia się ścisłą logiczną relacją w porównaniu do innych „rozproszonych" wieloautorskich paradygmatów metodologicznych.

Słowa kluczowe: bezpieczeństwo informacyjne, cyberbezpieczeństwo, zagrożenia cyberbezpieczeństwa, społeczeństwo informacyjne, przestrzeń informacyjno-komunikacyjna

Wstęp

W literaturze przedmiotu występuje szerokie spektrum definicji pojęcia „bezpieczeństwo informacyjne". W tym zakresie dominuje wieloautorskie podejście leksykalne, charakteryzujące się różnorodnością koncepcji metodologicznych prezentowanych przez poszczególnych autorów. W efekcie uzyskujemy w tym zakresie inspirujący przegląd różnych kierunków badań oraz determinujących je składowych (czynników). Jednak brak jednolitego paradygmatu metodologicznego skutkuje brakiem możliwości ścisłego odniesienia i powiązania tego pojęcia z jego składowymi determinantami (struktura bazowa) oraz innymi *de*

* Uniwersytet w Siedlcach, e-mail: robert.bialoskorski@uws.edu.pl, ORCID: 0000-0003-3038-7560.

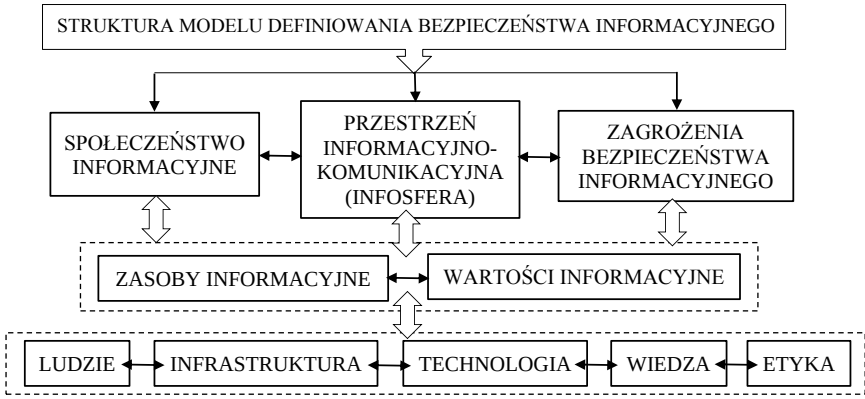
facto wynikającymi z niego kategorii bezpieczeństwa informacyjnego, do których należą: „cyberbezpieczeństwo", „bezpieczeństwo informacji", „bezpieczeństwo teleinformatyczne" oraz „bezpieczeństwo komputerowe" (struktury relacyjne). Powoduje to nie tylko nieuzasadnione oderwanie tych pojęć od struktury bazowej, jakim jest „bezpieczeństwo informacyjne", a nawet ich pojęciowe mieszanie czy wzajemne utożsamianie[1]. Wady tej nie ma proponowane w artykule strukturalne (holistyczne) podejście definicyjne wynikające z jednolitego i spójnego paradygmatu metodologicznego.

W artykule zaprezentowano wyniki badań, których **celem było** opracowanie strukturalnej (holistycznej) koncepcji definiowania pojęcia „bezpieczeństwo informacyjne" jako struktury bazowej oraz wynikających z niego i wzajemnie powiązanych kategorii bezpieczeństwa informacyjnego (struktur relacyjnych), a mianowicie: „cyberbezpieczeństwo", „bezpieczeństwo informacji", „bezpieczeństwo teleinformatyczne" oraz „bezpieczeństwo komputerowe". **Podjęty roblem badawczy** zawierał się w pytaniu: w jaki sposób można definiować pojęcie „bezpieczeństwo informacyjne" w podejściu strukturalnym i w jaki sposób fakt ten oddziałuje na sposób definiowania jego kategorii (struktur relacyjnych)? Przyjęta **hipoteza badawcza** zawierała się w przypuszczeniu, że strukturalne (holistyczne) podejście do definiowania wyróżnia się ścisłą logiczną relacją wynikową w porównaniu do innych paradygmatów metodologicznych. Prezentowana koncepcja ma charakter autorski i jest wynikiem **studiów porównawczych nad przedmiotem badań** opartych na piśmiennictwie naukowym badaczy polskich i zagranicznych.

Proponowana koncepcja definiowania ma charakter strukturalny. Z definicji „struktura" to „układ i wzajemne relacje stanowiące całość", inaczej „całość zbudowana w pewien sposób z poszczególnych elementów"[2]. Przyjmując, że istotą struktury jest układ elementów oraz ich relacje, punktem wyjścia przedmiotowych badań było określenie jego składowych determinantów oraz skorelowanych relacji. W tym zakresie za wystarczające uznano przyjęcie trzech kluczowych determinantów, a mianowicie: **(1) społeczeństwo informacyjne, (2) przestrzeń informacyjno-komunikacyjną (infosferę) oraz (3) zagrożenia bezpieczeństwa informacyjnego oraz ich wzajemne relacje.** Te trzy składowe struktury bazowej rozpatrywane były w relacyjnym aspekcie zasobów informacyjnych i wartości informacyjnych, na które składają się: ludzie, infrastruktura, technologia, wiedza i etyka (rys. 1).

[1] Zob. np.: *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023; *Vademecum bezpieczeństwa informacyjnego*, tom 1, red. O. Wasiuta, R. Klepka, Kraków 2019.

[2] *Struktura* [w:] *Słownik języka polskiego PWN*, 2024, https://sjp.pwn.pl (14.07.2024).



Rysunek 1. Determinanty strukturalnej (holistycznej) koncepcji definiowania bezpieczeństwa informacyjnego

Źródło: opracowanie własne.

Społeczeństwo informacyjne

W naukach o bezpieczeństwie społeczeństwo informacyjne[3] pełni funkcję zarówno podmiotu (kto zapewnia bezpieczeństwo informacyjne?), jak i przedmiotu referencyjnego (komu zapewnia się bezpieczeństwo informacyjne?)[4]. Człowiek, jako najmniejszy element łańcucha, jakim jest społeczeństwo informacyjne, jest najsilniejszym i zarazem najsłabszym ogniwem bezpieczeństwa informacyjnego. Albowiem to człowiek stworzył technologię informacyjno-komunikacyjną i sztuczną inteligencję, w tym systemy bezpieczeństwa informacyjnego, i jednocześnie jest najbardziej podatny na najgroźniejsze obecnie statystycznie zagrożenia w infosferze, jakim są oszustwa komputerowe, wykorzystujące socjotechniczne metody ataku komputerowego, typu *phishing and spoofing*, czy też jednostkowe, ale na masową skalę incydenty kradzieży i ujawnienia informacji niejawnych[5]. W literaturze przedmiotu istnieje wiele różnorodnych definicji społeczeństwa informacyjnego[6]. Zdaniem autora w definiowaniu społeczeństwa

[3] Innymi najczęściej używanymi w literaturze przedmiotu terminami są: „społeczeństwo wiedzy" oraz „społeczeństwo sieciowe".

[4] Zob. R. Wróblewski, *Wprowadzenie do nauk o bezpieczeństwie*, Siedlce 2017, s. 84–85.

[5] Np. *Raporty CERT Polska*, CERT, https://cert.pl (14.07.2024) oraz kazus Edwarda J. Snowdena.

[6] J.S. Nowak, *Społeczeństwo informacyjne – geneza i definicje* [w:] *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, red. P. Sienkiewicz, J.S. Nowak, Katowice 2005, s. 11–15.

informacyjnego istotne jest poszukiwanie zależności przyczynowo-skutkowych pomiędzy „informacją" i „społeczeństwem". Informacja jest nieodłącznym atrybutem towarzyszącym człowiekowi od zarania ludzkości. Jednak dopiero rewolucja cyfrowa i technologia informacyjno-komunikacyjna przyczyniły się do powstania i rozwoju pojęcia „społeczeństwo informacyjne" w różnych wymiarach jego funkcjonowania, a w szczególności w rozwojowym obszarze psycho-socjologicznym. W efekcie prowadzi to do postrzegania społeczeństwa informacyjnego jako **„społeczeństwa o głębokich zmianach w świadomości społecznej wywołanych skutkiem rewolucji cyfrowej oddziałujące wielowymiarowo (politycznie, gospodarczo, społecznie, kulturowo, etc.) na rzeczywistość za pomocą informacji"**[7]. Zbiorowa świadomość społeczna jest efektem oddziaływania jednostkowych świadomości ludzkich zarówno w sferze realnej, jak i wirtulanej i w tym sensie jest ona zdeterminowana wyłącznie do ludzkich organizmów żywych i nie zależy od przyszłych kierunków i cywilizacyjnych skutków rozwoju sztucznej inteligencji.

Przestrzeń informacyjno-komunikacyjna (infosfera)

Pojęcie przestrzeni informacyjno-komunikacyjnej, zwanej przez autora w skrócie „infosferą", odwołuje się wprost do jej zależności od „technologii informacyjno-komunikacyjnej"[8], podkreślając tym samym zarówno aspekt wytwarzania i przetwarzania informacji, jak i jej komunikacyjnej dystrybucji i implementacji. W literaturze przedmiotu pojęcie infosfery wywodzi się z teorii informacji i przyjmuje różne znaczenia. Przykładowo oznacza: „całość zasobów informacyjnych, do których ma dostęp dany podmiot"[9], „środowisko obejmujące wszelkie relacje i procesy, jakie zachodzą pomiędzy użytkownikami a zbiorami informacji"[10], „ogół informacji dostępnych człowiekowi poprzez jego świadomość, które potencjalnie może on zużytkować przy realizacji swych życiowych celów"[11]. W szerszym aspekcie

[7] Zob. R. Białoskórski, *Pojęcie społeczeństwa informacyjnego jako przyczynek do dyskusji*, „Zeszyty Naukowe WSCiL", 2010, nr 26, s. 187–95.

[8] W literaturze przedmiotu termin ten, jak przyjęto w artykule, występuje w liczbie pojedynczej, jako „technologia informacyjno-komunikacyjna" (ang. *information-communication technology*) lub też w liczbie mnogiej w rozumieniu „technologie informacyjno-komunikacyjne" (ang. *information-communication technologies*).

[9] T.R. Aleksandrowicz, *Infosfera* [w:] *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023, s. 176.

[10] H. Batorowska, *Infosfera* [w:] *Vademecum bezpieczeństwa informacyjnego*, red. O. Wasiuta, R. Klepka, Kraków 2020.

[11] J.L. Kulikowski, *Człowiek i infosfera*, „Problemy", 1978, nr 3, s. 2–6.

antroposfery bezpieczeństwa termin ten jest postrzegany jako „infosfera bezpieczeństwa", gdzie informacja jest traktowana jako środek kreowania bezpieczeństwa państwa, w tym bezpieczeństwa informacyjnego rozumianego jako „ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania"[12]. W odróżnieniu do alterantywnych podejść strukturalna (holistyczna) koncepcja definiowania infosfery zakłada dualność fizycznej i wirtualnej natury środowiska informacyjno-komunikacyjnego i jej ścisłą relatywność do społeczeństwa informacyjnego. W efekcie na potrzeby przedmiotowych rozważań przyjmuje się, iż **przestrzeń informacyjno-komunikacyjna (infosfera) to fizyczne i wirtualne środowisko informacyjno-komunikacyjne wykorzystywane przez społeczeństwo informacyjne do realizacji i osiągania jego celów, interesów i wartości.**

Zagrożenia bezpieczeństwa informacyjnego

W ogólnym sensie należy się zgodzić, iż zagrożenia bezpieczeństwa informacyjnego to mające różnorodny charakter procesy, zjawiska, zdarzenia i sytuacje, w wyniku których mamy do czynienia z uświadamianymi lub nieuświadamianymi ograniczeniami, błędami, zaniechaniami, nadużyciami lub przestępczymi (wrogimi) działaniami godzącymi w swobodny (zgodny z potrzebami i prawem) dostęp do aktualnych, rzetelnych i integralnych zasobów informacyjnych. Typologia zagrożeń jest zróżnicowana i najczęściej obejmuje różne kategorie zagrożeń o charakterze wewnętrznym i zewnętrznym[13]. W przedmiotowym aspekcie badań celowe jest wyróżnienie zagrożeń bezpieczeństwa informacyjnego w sferze realnej i w sferze wirtualnej. Sfera realna jest fizycznym (materialnym), zaś sfera wirtualna niefizycznym (niematerialnym) środowiskiem bezpieczeństwa informacyjnego. Obie sfery odnoszą się do aspektów prawnych, techniczno-technologicznych, organizacyjnych i fukcjonalnych zarządzania bezpieczeństwem informacyjnym. Przykładowo system ochrony informacji niejawnych w Polsce normatywnie oparty na ustawie o ochronie informacji niejawnych zakłada działania ochronne w sferze realnej (podsystem kancelarii tajnych) oraz wirtulanej (podsystem teleinformatyczny), a przestrzeń wspólną stanowi fizyczne bezpieczeństwo osobowe (rękojmia zachowania

[12] S. Jarmoszko, *Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa* [w:] *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, red. R. Białoskórski, M. Kubiak, Siedlce 2016, s. 34–59.

[13] W. Fehler, *Zagrożenia bezpieczeństwa informacyjnego* [w:] *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023, s. 388–389.

tajemnicy)[14]. Zatem w badanym przypadku pod pojęciem zagrożenia bezpieczeństwa informacyjnego należy rozumieć **jakiekolwiek nieuprawnione wejście lub usiłowanie wejścia do fizycznych lub wirtualnych zasobów informacyjnych podmiotów społeczeństwa informacyjnego (organizacje, jednostki) oraz naruszenie ich integralności i poufności na każdym etapie gromadzenia, przechowywania, przetwarzania i dystrybucji informacji.** Studia nad literaturą przedmiotu wskazują na cztery kategorie zagrożeń bezpieczeństwa informacyjnego: **(1) walkę informacyjną, (2) szpiegostwo, (3) przestępczość i (4) terroryzm**. Z tych czterech tylko pierwsza z konieczności ma przymiotnik „informacyjna", podczas gdy pozostałe tego nie wymagają, chociaż istotą ich zrozumienia jest również informacja. Chociaż brakuje w tym zakresie kompleksowych badań ilościowych, to mając na uwadze jedynie dynamikę rozwoju cyberprzestrzeni, można przypuszczać, iż wszystkie te kategorie obecnie dominują w sferze wirtualnej w stosunku do sfery realnej. Tak przyjętą na potrzeby badań kodyfikację zagrożeń bezpieczeństwa informacyjnego określają takie determinanty, jak: podmiot atakujący (agresor), podmiot atakowany (ofiara) oraz motywacja (cel) (tab. 1)[15].

Tabela 1. Matryca determinantów kategoryzacji zagrożeń bezpieczeństwa informacyjnego

Rodzaj zagrożenia bezpieczeństwa informacyjnego	Determinanty (wskaźniki) kodyfikacyjne		
	Podmiot atakujący (agresor)	Podmiot atakowany (ofiara)	Motywacja (cel)
Walka informacyjna	P/MOM	P/MOM/POM/ ZGP/MOT/PPG	Polityczna
Szpiegostwo	P/MOM/PPG	P/MOM/POM/PPG	Polityczna/Biznesowa
Przestępczość	ZGP/J	P/MOM/POM/ZGP/ MOT/PPG/J	Finansowa/ Materialna/ Psychologiczna
Terroryzm	MOT/J	P/MOM/POM/ZGP/ MOT/PPG	Polityczna/Ideologiczna/ Religijna

Legenda: P – państwa, MOM – międzyrządowe organizacje międzynarodowe, POM – pozarządowe organizacje międzynarodowe, ZGP – zorganizowane grupy przestępcze, MOT – międzynarodowe organizacje terrorystyczne, PPG – prywatne podmioty gospodarcze, J – jednostki.

Źródło: opracowanie własne.

[14] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228 ze zm.).

[15] Por. R. Białoskórski, *Cyberthreats in the Security Environment of the 21st Century*, „Journal of Security and Sustainability Issues", 2012, no. 4, s. 249–260.

Walka informacyjna[16] jest domeną działania państw, jako podstawowych jednostek politycznych, w tym międzyrządowych organizacji międzynarodowych. Państwa atakują informacyjnie wyłącznie podmioty zorganizowane, a nie jednostki (osoby). Przykładowo, nawet jeśli celem ataku jest personalnie prezydent czy premier danego kraju, to dotyczy to bezpośrednio urzędu, a nie prywatnej osoby. Decydują o tym politycznie motywowany cel postrzegany we wszystkich obszarach aktywności państwa – politycznej, gospodarczej, militarnej, technologicznej i kulturowej, oraz podmioty atakowane[17]. Podmiotami szczególnie zaangażowanymi w walkę informacyjną są struktury bezpieczeństwa państwa powołane do prowadzenia tajnych operacji specjalnych, a więc służby specjalne, czyli służba wywiadu (wywiad) i służba kontrwywiadu (kontrwywiad). Warto w tym miejscu zauważyć, że działalność wywiadowcza jest legalna z punktu widzenia prawa państwa powołującego służbę, natomiast nielegalna z punktu widzenia prawa obcego państwa, na którego terytorium wywiad prowadzi czynności operacyjno-rozpoznawcze. W tym drugim przypadku używa się często popularnego żargonu „szpiegostwo" i tym terminem ogólnie określono drugą kategorię zagrożeń bezpieczeństwa informacyjnego.

Szpiegostwo jest *de facto* działalnością polegającą na kradzieży informacji niejawnych i(lub) innych informacji prawnie chronionych i nie ma w tym wypadku znaczenia, czy sprawcą jest państwo („szpiegostwo" państwowe), czy prywatny podmiot gospodarczy (szpiegostwo biznesowe oraz wywiad biznesowy). W obu przypadkach z punktu widzenia prawa i interesu podmiotu atakowanego sprawca dopuszczający się szpiegostwa popełnia czyn przestępny i podlega ściganiu na mocy obowiązującego prawa krajowego i międzynarodowego. Szpiegostwo państwowe, inaczej wywiad państwowy, odróżnia od kategorii wywiadu

[16] Warto w tym miejscu odróżnić pojęcie „walka informacyjna" od zbyt powszechnie używanego terminu „wojna informacyjna". Ten pierwszy ma charakter naukowy, a ten drugi publicystyczny (medialny), aczkolwiek niestety również jest spotykany w pracach naukowych. Zdaniem autora wynika to z braku wiedzy w zakresie sztuki wojennej. Współcześnie nie prowadzi się bowiem wojen wyłącznie w jednej z 5 domen (lądowej, morskiej, powietrznej, kosmicznej, informacyjnej) i operacje wojenne mają charakter wielodomenowy (hybrydowy). Zatem tak jak nie ma wyłącznie „wojny lądowej", „wojny powietrznej", „wojny morskiej", „wojny kosmicznej", nie ma także „wojny informacyjnej". Mamy natomiast do czynienia z „walką lądową", „walką informacyjną", itd.

[17] Atak informacyjny może być elementem psychologicznych operacji informacyjnych (POI) lub cybernetycznych operacji informacyjnych (COI). Zob. R. Białoskórski, *The Theoretical Concept of Information Warfare: A General Outline*, „Humanities and Social Sciences", 2023, nr 4, s. 7–24.

prywatnego analiza matrycy sześciu wskaźników, takich jak: podmiot, obszar działania, obiekt rozpracowania, rodzaj informacji, metoda oraz cel działania (tab. 2).

Tabela 2. Matryca determinantów kategorii „szpiegostwa"

Kategoria wywiadu	Podmiot	Obszar działania	Obiekt rozpracowania	Rodzaj informacji	Metody działania	Cel działania
Wywiad państwowy (służba wywiadu)	Państwo	Środowisko międzynarodowe	Państwa Organizacje międzynarodowe (międzyrządowe i pozarządowe) Podmioty transnarodowe	Informacje jawne Informacje niejawne (operacyjne źródła osobowe i nieosobowe)	Wywiad otwarty (biały) Tajny wywiad operacyjny (praca typowniczo-werbunkowa; agenturalne źródła informacji; tajne operacje wywiadowcze)	Informacyjne wsparcie systemu władzy państwa w podejmowaniu strategicznych decyzji w zakresie bezpieczeństwa państwa
Wywiad prywatny (wywiad biznesowy/ szpiegostwo biznesowe)	Prywatny podmiot biznesowy	Środowisko biznesowe	Państwo Klient Kooperant Konkurent	Informacje jawne (wywiad biznesowy) ----- Poufne informacje stanowiące tajemnicę przedsiębiorstwa (szpiegostwo biznesowe)	Wywiad otwarty (wywiad biznesowy) ----- Przestępne czyny pozyskiwania informacji biznesowych (kradzież, korupcja, itp.) (szpiegostwo biznesowe)	Informacyjne wsparcie organów własnościowych i zarządczych organizacji w podejmowaniu decyzji menedżerskich

Źródło: opracowanie własne.

W przypadku kategorii wywiadu prywatnego mamy do czynienia z dwoma subkategoriami zagrożeń bezpieczeństwa informacyjnego, a mianowicie: wywiadem biznesowym oraz szpiegostwem biznesowym. Cel ich działania jest ten sam, a zasadnicza różnica polega na rodzaju i sposobach pozyskiwania informacji wywiadowczych. Wywiad biznesowy jest rodzajem zaawansowanej analityki biznesowej operującej wyłącznie na jawnych źródłach informacji (wywiad biały)[18]. Szpiegostwo

[18] Zob. J. Surma, *Business Intelligence. Systemy wspomagania decyzji biznesowych*, Warszawa 2009; R. Białoskórski, *Koncepcja strategii wywiadu biznesowego*, „Secretum", 2015, nr 2, s. 61–74.

biznesowe polega na pozyskiwaniu poufnych informacji stanowiących tajemnicę przedsiębiorstwa za pomocą czynów przestępnych, takich jak kradzież czy korupcja (wywiad czarny)[19].

Przestępczość, jako kategoria zagrożenia bezpieczeństwa informacyjnego, może mieć charakter jednostkowy (przestępca) lub zorganizowany (grupa przestępcza) oraz pospolity (np. kradzież lub zniszczenie dokumentów niejawnych w formie dokumentów materialnych) albo też zaawansowany (np. kradzież lub zniszczenie zbioru danych w formie elektronicznej z systemu teleinformatycznego). Obecnie dynamika zaawansowanej przestępczości w cyberprzestrzeni (cyberprzestępczości) ma trend rosnący, do czego istotnie przyczyniła się sprzyjająca temu sytuacja pandemiczna. Definiowanie cyberprzestępczości na gruncie prawnym jest niezwykle złożone. Niektóre czyny związane z cyberprzestępczością są odzwierciedleniem przestępstw i wykroczeń mających miejsce w świecie realnym, ale zostały odpowiednio zaadaptowane do warunków, jakie oferuje cyberprzestrzeń[20]. Interesującą w tym względzie analizę przedmiotowo-podmiotową zawiera dysertacja Janusza Wasilewskiego[21].

Terroryzm, jako kategoria zagrożenia bezpieczeństwa informacyjnego, jest głównie domeną organizacji terrorystycznych, aczkolwiek odnotowuje się także przypadki jednostkowych (personalnych) ataków klasyfikowanych jako terrorystyczne[22]. Współcześnie terroryzm w cyberprzestrzeni, czy też z wykorzystaniem cyberprzestrzeni (cyberterroryzm), ogranicza się do następujących działań: planowanie zamachów terrorystycznych (rozpracowywanie celów ataku), komunikacja (cyfrowa łączność szyfrowana), szerzenie propagandy ideologii terroryzmu, radykalizacja i rekrutacja nowych członków, pozyskiwanie funduszy na działalność terrorystyczną oraz instruktaż i szkolenie w zakresie metod i technik terrorystycznych[23].

---

[19] *Idem*, *Prawno-etyczny wymiar wywiadu biznesowego*, „Secretum", 2016, nr 1, s. 22–35.

[20] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law", 2019, nr 2, s. 16.

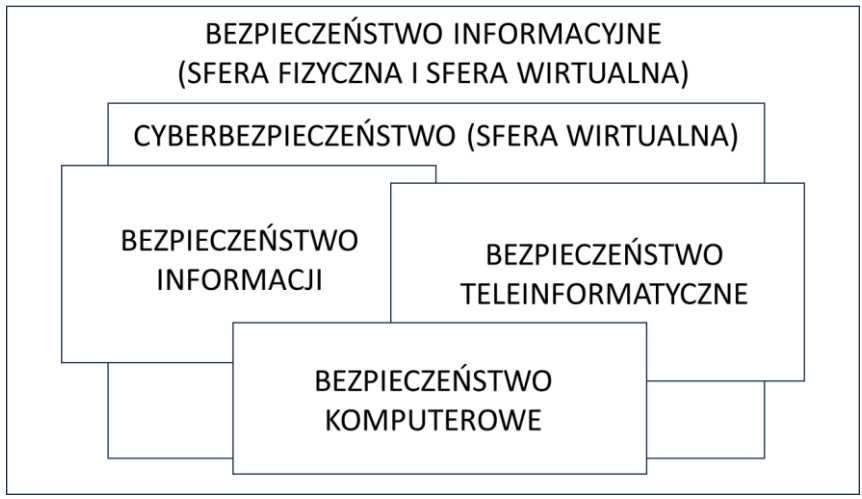
[21] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Dysertacja, Uniwersytet w Białymstoku, Białystok 2017, https://repozytorium.uwb.edu.pl (14.07.2024).

[22] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Warszawa 2011.

[23] *Cyberterrorism. Understanding, Assessment, and Response*, eds T.M. Chen, L. Jarvis, S. Macdonald, Springer 2014.

Strukturalna definicja bezpieczeństwa informacyjnego

Na podstawie przedstawionych ogólnych założeń strukturalnej (holistycznej) koncepcji definiowania bezpieczeństwa informacyjnego przyjmujemy, iż **bezpieczeństwo informacyjne to bezpieczeństwo przestrzeni informacyjno-komunikacyjnej (infosfery) polegające na wczesnym ostrzeganiu, zapobieganiu i przeciwdziałaniu wszelkim zagrożeniom bezpieczeństwa informacyjnego w sferze fizycznej i wirtualnej.** Tak zdefniowane bezpieczeństwo informacyjne implikuje definiowanie jego kategorii (pojęć relacyjnych), do których należą: cyberbezpieczeństwo, bezpieczeństwo informacji, bezpieczeństwo teleinformatyczne i bezpieczeństwo komputerowe. W prezentowanym podejściu istotna jest korelacja badanych pojęć w fizycznej i wirtualnej sferze przestrzeni informacyjno-komunikacyjnej (rys. 2).



Rysunek 2. Korelacja bezpieczeństwa informacyjego i jego kategorii

Źródło: opracowanie własne.

Bezpieczeństwo cyberprzestrzeni (cyberbezpieczeństwo) to bezpieczeństwo wirtualnej (niefizycznej) sfery przestrzeni informacyjno-komunkacyjnej (infosfery) polegające na wczesnym ostrzeganiu, zapobieganiu i przeciwdziałaniu zagrożeniom bezpieczeństwa informacyjnego podmiotów (użytkowniów), zasobów i wartości informacyjnych społeczeństwa informacyjnego.

Bezpieczeństwo informacji to bezpieczeństwo gromadzenia, składowania, przetwarzania, transmitowania i dystrybuowania zasobów

i wartości informacyjnych społeczeństwa informacyjnego w przestrzeni informacyjno-komunikacyjnej (infosferze).

Bezpieczeństwo teleinformatyczne to bezpieczeństwo systemów informacyjno-komunikacyjnych w przestrzeni informacyjno-komunikacyjnej (infosferze), w których są gromadzone, składowane, przetwarzane i transmitowane zasoby i wartości informacyjne społeczeństwa informacyjnego.

Bezpieczeństwo komputerowe to bezpieczeństwo stacjonarnych i mobilnych urządzeń komputerowych w przestrzeni informacyjno-komunikacyjnej (infosferze), w których są gromadzone, składowane, przetwarzane i transmitowane zasoby i wartości informacyjne społeczeństwa informacyjnego.

Zakończenie

Przedstawiona w artykule strukturalna (holistyczna) koncepcja definiowania bezpieczeństwa informacyjnego została oparta na strukturze bazowej złożonej z relacji trzech składowych determinantów: społeczeństwa informacyjnego, przestrzeni informacyjno-komunikacyjnej (infosfery) oraz zagrożeń bezpieczeństwa informacyjnego. Te trzy składowe były rozpatrywane w relacyjnym aspekcie zasobów informacyjnych i wartości informacyjnych (ludzi, infrastruktury, technologii, wiedzy i etyki). Uzyskana w efekcie definicja bezpieczeństwa informacyjnego pozwoliła na wypracowanie relacyjnych kategorii bezpieczeństwa informacyjnego skorelowanych w fizycznej i wirtualnej sferze przestrzeni informacyjno-komunikacyjnej (infosferze). Zaproponowane strukturalne (holistyczne) podejście do definiowania bezpieczeństwa informacyjnego wyróżnia się ścisłą logiczną relacją wynikową w porównaniu do innych „rozproszonych" wieloautorskich paradygmatów metodologicznych.

Bibliografia

Aleksandrowicz T.R., *Infosfera* [w:] *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023.

Batorowska H., *Infosfera* [w:] *Vademecum bezpieczeństwa informacyjnego*, red. O. Wasiuta, R. Klepka, Kraków 2020.

Białoskórski R., *Cyberthreats in the Security Environment of the 21st Century*, „Journal of Security and Sustainability Issues", 2012, no. 4.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku*, Warszawa 2011.

Białoskórski R., *Koncepcja strategii wywiadu biznesowego*, „Secretum", 2015, nr 2.

Białoskórski R., *Pojęcie społeczeństwa informacyjnego jako przyczynek do dyskusji*, „Zeszyty Naukowe WSCiL", 2010, nr 26.

Białoskórski R., *Prawno-etyczny wymiar wywiadu biznesowego*, „Secretum", 2016, nr 1.
Białoskórski R., *The Theoretical Concept of Information Warfare: A General Outline*, „Humanities and Social Sciences", 2023, no. 4.
Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law", 2019, nr 2.
Cyberterrorism. Understanding, Assessment, and Response, eds T.M. Chen, L. Jarvis, S. Macdonald, Springer 2014.
Fehler W., *Zagrożenia bezpieczeństwa informacyjnego* [w:] *Leksykon bezpieczeństwa informacyjnego*, red. W. Fehler, Siedlce 2023.
Jarmoszko S., *Bezpieczeństwo informacyjne a casus infosfery bezpieczeństwa* [w:] *Informacyjne uwarunkowania współczesnego bezpieczeństwa*, red. R. Białoskórski, M. Kubiak, Siedlce 2016.
Kulikowski J.L., *Człowiek i infosfera*, „Problemy", 1978, nr 3.
Nowak J.S., *Społeczeństwo informacyjne – geneza i definicje* [w:] *Społeczeństwo informacyjne. Krok naprzód, dwa kroki wstecz*, red. P. Sienkiewicz, J.S. Nowak, Katowice 2005.
Raporty CERT Polska, CERT, https://cert.pl (14.07.2024).
Struktura [w:] *Słownik języka polskiego PWN*, 2024, https://sjp.pwn.pl (14.07.2024).
Surma J., *Business Intelligence. Systemy wspomagania decyzji biznesowych*, Warszawa–Ursynów 2009.
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228 ze zm.).
Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Dysertacja, Uniwersytet w Bałymstoku, Białystok 2017, https://repozytorium.uwb.edu.pl (14.07.2024).
Vademecum bezpieczeństwa informacyjnego, t. 1, red. O. Wasiuta, R. Klepka, Kraków 2019.
Wróblewski R., *Wprowadzenie do nauk o bezpieczeństwie*, Siedlce 2017.

A structural (holistic) concept defining information security

Abstract

The article presents a structural (holistic) concept of the method of defining information security based on a main structure composed of the relationship of three component determinants: information society, information and communication space (infosphere), and information security threats. These three components are considered in the relational aspect of information resources and information values (people, infrastructure, technology, knowledge, and ethics). The definition of information security led to the development of relational categories of information security correlated in the physical and virtual spheres of the information and communication space (infosphere). The research results have pointed that the structural (holistic) approach to defining information security is distinguished by a strict logical result compared to other 'distributed' multiauthor methodological paradigms.

Keywords: information; security, cybersecurity, security threats, information society, information-communication space