Elżbieta Żywucka-Kozłowska*
Robert Dziembowski**

Wokół definicji cyberbezpieczeństwa

Streszczenie

Pojęcie „cyberbezpieczeństw" wpisało się w rzeczywistość końca XX i pierwszej połowy XXI wieku. Termin ten jest rozumiany jako system blokujący zagrożenia polegające na niszczeniu, zmienianiu oraz nieuprawnionym przejęciu danych. Wagę problemu cyberbezpieczeństwa podkreślono, dokonując regulacji prawnej w ustawodawstwach wielu krajów świata, w tym w Polsce, Stanach Zjednoczonych Ameryki, Federacji Rosyjskiej czy w Chinach oraz na gruncie przepisów związków państw czy organizacji międzynarodowych, czego przekładem są stosowne regulacje Unii Europejskiej. Cyberbezpieczeństwo jest pojęciem wielopłaszczyznowym, stało się przedmiotem zainteresowania nie tylko krajów czy organizacji, lecz także poszczególnych jednostek żyjących w danych społecznościach. Postępująca cyfryzacja wielu dziedzin życia powoduje, niezależnie od położenia geograficznego kraju, że konieczność zapewnienia właściwego i bezpiecznego funkcjonowania tej sfery rzeczywistości przesądza o uniwersalności cyberbezpieczeństwa.

Słowa kluczowe: cyberprzestrzeń, bezpieczeństwo, prawo, cyfryzacja, dyrektywa, Unia Europejska

* Dr hab. Elżbieta Żywucka-Kozłowska, Katedra Postępowania Karnego i Prawa Karnego Wykonawczego, Wydział Prawa i Administracji, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail: malerude@poczta.onet.pl, ORCID:0000-0002-6039-5580.
** Dr Robert Dziembowski, Katedra Postępowania Karnego i Prawa Karnego Wykonawczego, Wydział Prawa i Administracji, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail: r.dziembowski@gmail.com, ORCID: 0000-0002-1697-637X.

Wstęp

Termin „cyberbezpieczeństwo" na stałe wpisał się w rzeczywistość końca XX wieku i XXI wiek. Stał się tak samo powszechny jak cyberprzestrzeń i wszystko, co wiąże się z istnieniem tej wyjątkowej struktury. W literaturze przedmiotu nie brakuje definicji zarówno cyberprzestrzeni, jak i bezpieczeństwa. Każde z tych pojęć zawiera zasadnicze elementy opisujące choćby zakres charakterystyczny dla nieograniczonej cyberprzestrzeni czy brak zagrożenia dla bezpieczeństwa. Pod koniec XX wieku zwrócono szczególną uwagę na cyberbezpieczeństwo rozumiane jako system blokujący zagrożenia, w tym niszczący, zmieniający czy przejmujący dane w nieuprawniony sposób. Nie są to, rzecz jasna, wszystkie zagrożenia tej przestrzeni. Nie sposób nie podkreślić, że sama w sobie (jeżeli tak można to nazwać) stanowi zagrożenie, chociażby jako transmiter różnych informacji. Celem niniejszego opracowania jest próba analizy definicji „cyberbezpieczeństwo" z różnego punktu widzenia, uwzględniającej różne elementy stanowiące o przypisaniu tego pojęcia do różnych dziedzin współczesnej egzystencji. Przedmiotowe pojęcie ma uniwersalny charakter, co poniekąd wynika z istoty cyberprzestrzeni, która nie ma granic, jest wszechobecna, powszechnie dostępna. Wobec tego, czy ta uniwersalność jako cecha cyberbezpieczeństwa jawi się w istniejących w literaturze naukowej definicjach, a jeżeli tak, to w jaki sposób? Tak formułowany problem badawczy wymaga sformułowania hipotezy. Warto w tym miejscu zastanowić się nad konstrukcją zdania, które ma być hipotezą, powinno ono bowiem zawierać dwa elementy – uniwersalność rozumianą szeroko oraz sposób definiowania pojęcia. Z tego też względu za hipotezę przyjęto zdanie w brzemieniu: Cyberbezpieczeństwo ma charakter uniwersalny i jest opisywane z różnych punktów widzenia. Poszukiwanie odpowiedzi w tym względzie wymaga pewnej metody badawczej, pewnych technik i narzędzi badawczych. Nie ma w tym niczego odkrywczego w procesie badawczym o naukowym charakterze. Wydaje się, że metodą w tym przypadku najbardziej odpowiednią jest analiza źródeł, w których znajdują się przedmiotowe definicje. Zapewne uda się sformułować odpowiedź na podstawowe pytanie stanowiące problem analizy, lecz czy sformułowana hipoteza się potwierdzi, trudno ocenić prawdopodobieństwo prawdziwości bądź fałszu (pomijając proste rozwiązanie – tak bądź nie).

W gąszczu definicji

Cyberbezpieczeństwo na stałe wpisało się do literatury przedmiotu powszechnie rozumianego bezpieczeństwa. Trudno się dziwić, bo jest jego odmianą, rodzajem, sektorem czy obszarem. Nieodłącznie jest związane z cyberprzestrzenią rozumianą jako „[...] globalna domena środowiska informacyjnego składająca się ze współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesy oraz kontrolery”[1]. W literaturze przedmiotu nietrudno dostrzec składowych cyberprzestrzeni objętych szczególną ochroną, w tym w szczególności infrastruktury krytycznej. Krystian Radziejewski zwraca uwagę na cyberbezpieczeństwo w administracji rządowej Rzeczypospolitej Polskiej[2]. Prezentowane przez autora elementy składające się na infrastrukturę krytyczną oraz ich zabezpieczenia dowodzą uniwersalności terminu choćby z jednego prostego powodu – każde państwo, niezależnie od ustroju politycznego, kondycji gospodarczej, pozycji na arenie międzynarodowej, strzeże w możliwie jak najbardziej skuteczny sposób dane (w powszechnym ujęciu) dotyczące tego segmentu bezpieczeństwa. Równie interesujące są prace innych autorów z tej tematyki[3]. Władysław Hydzik, analizując problem prawnej regulacji cyberbezpieczeństwa i ochrony danych osobowych w świetle regulacji europejskich i krajowych, przywołuje definicję przedmiotowego terminu z wniosku Komisji Europejskiej z 7 lutego 2013 roku, w którym cyberbezpieczeństwo zostało zdefiniowane jako „[...] odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług

1 K. Chałubińska-Jentkiewicz, *Cyberbepieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law 2019, nr 2, s. 9.

2 R. Radziejewski, *Cyberbezpieczeństwo w administracji rządowej w Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2017, nr 16, s. 308–330.

3 Zob. m.in.: J. Worona, *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, „Białostockie Studia Prawnicze” 2016, z. 20/B, s. 465–474; S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2022, nr 27, s. 198–217; D. Lisiak-Felicka, M. Pytko, *Cyberbezpieczeństwo urzędów gmin w województwie łódzkim*, „Przedsiębiorczość i Zarządzanie” 2017, t. 18, nr 4, cz. 1, s. 439–451.

oferowanych lub dostępnych poprzez te sieci i systemy”[4]. Trudno nie zgodzić się z przytoczoną definicją, zważywszy nie tylko na zakres, lecz przede wszystkim na uniwersalność cyberbezpieczeństwa w ujęciu zarówno międzynarodowym (Unii Europejskiej), jak i krajowym.

Na gruncie prawa polskiego ustawodawca zdefiniował cyberbezpieczeństwo jako „[...] odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[5]. Ustawa ta w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE 2016, L 194/1). Leksykalnie treść definicji odpowiada treści wskazywanej wyżej przez Władysława Hydzika, autor bowiem powołał się na wniosek KE w przedmiotowym zakresie. Jak już wcześniej wskazano, każde państwo w XXI wieku podejmuje wysiłki w celu zwiększenia cyberbepieczeństwa, zwłaszcza sektorów mających szczególne znaczenie dla zarządzania państwem. Dominika Janus analizuje zarządzanie internetem w Chinach, podkreśla znaczenie zarówno informacji, jak i samego pojmowania cyberbezpieczeństwa w tym państwie. Autorka wskazuje, że jest ono sektorem bezpieczeństwa narodowego Chin, ale definicja tego terminu nie odbiega od tych, które funkcjonują w innych regionach świata[6].

Nie sposób nie odnieść się do cyberbezpieczeństwa w Federacji Rosyjskiej (FR), zwłaszcza w czasie wywołanej przez to państwo wojny w Ukrainie. Helena Giebień pisze: „[...] w celu zabezpieczenia jednostek, organizacji oraz państwa przed zagrożeniami płynącymi z cyberprzestrzeni zarówno wewnątrz kraju, jak i zewnątrz władze FR opracowały doktrynę cyberbezpieczeństwa państwa”[7]. Głównym założeniem strategii w tym obszarze stały się umowy międzynarodowe z innymi państwami. Z dostępnych danych wynika, że taką Federacja Rosyjska podpisała z Chinami w 2015 roku[8]. Doktryna bezpieczeństwa

4 Cyt. za: W. Hydzik, *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego” 2019, nr 3, s. 85.

5 Ustawa z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2022, poz. 1863.

6 D. Janus, *Między siłą a informacją. Zarządzanie Internetem, cyberbezpieczeństwo i nowe technologie w Chinach po XIX Zjeździe KPCh*, „Azja–Pacyfik” 2020, nr 23, s. 230–241.

7 H. Giebień, *Cyberbezpieczeństwo w Federacji Rosyjskiej. Zarys problemu*, „Wschodnioznawstwo” 2018, nr 12, s. 195.

8 Ibidem, s. 195.

w cyberprzestrzeni, o której pisze Giebień, przede wszystkim opiera się na koncepcji umów bilateralnych z innymi państwami. Można ostrożnie przyjąć, że takie porozumienia zapewne podpisano z krajami podobnymi politycznie (reżim). Cyberprzestrzeń w FR stała się nie tylko polem propagandy rządowej, lecz także polem walki z innymi państwami. W tej sytuacji trudno w jakikolwiek racjonalny sposób odnieść się do bezpieczeństwa cyberprzestrzeni. Można jedynie (na swój sposób) przyjąć (choć ograniczenie), że cyberprzestrzeń jest postrzegana uniwersalnie, m.in. z punktu widzenia obszaru i znacznej liczby użytkowników sieci.

W Stanach Zjednoczonych Ameryki cyberbezpieczeństwo zajmuje szczególne miejsce w doktrynie obronnej państwa[9]. Po ataku terrorystycznym z 11 września 2001 roku uznano za zagrożenia niekonwencjonalne m.in. cyberataki[10]. Działania takie zaliczono do zagrożeń asymetrycznych[11]. Słusznie zauważa Tomasz Hoffman, że cyberbezpieczeństwo stało się polem eksploracji przedstawicieli wielu dziedzin nauki, w tym prawników, informatyków, politologów czy ekonomistów, głównie z racji zagrożeń w cyberprzestrzeni[12]. Definicje cyberbezpieczeństwa przede wszystkim podkreślają element zagrożenia cyberprzestrzeni i brak granic tego środowiska (uniwersalność informatyczna).

9 Zob. m.in.: D. Dziwisz, *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych?*, „Sprawy Międzynarodowe" 2011, nr 3, s. 103–122; M. Madej, *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego – próba teoretycznej konceptualizacji* [w:] *Porządek międzynarodowy u progu XXI wieku*, red. R. Kuźniar, Warszawa 2005, s. 486–518.

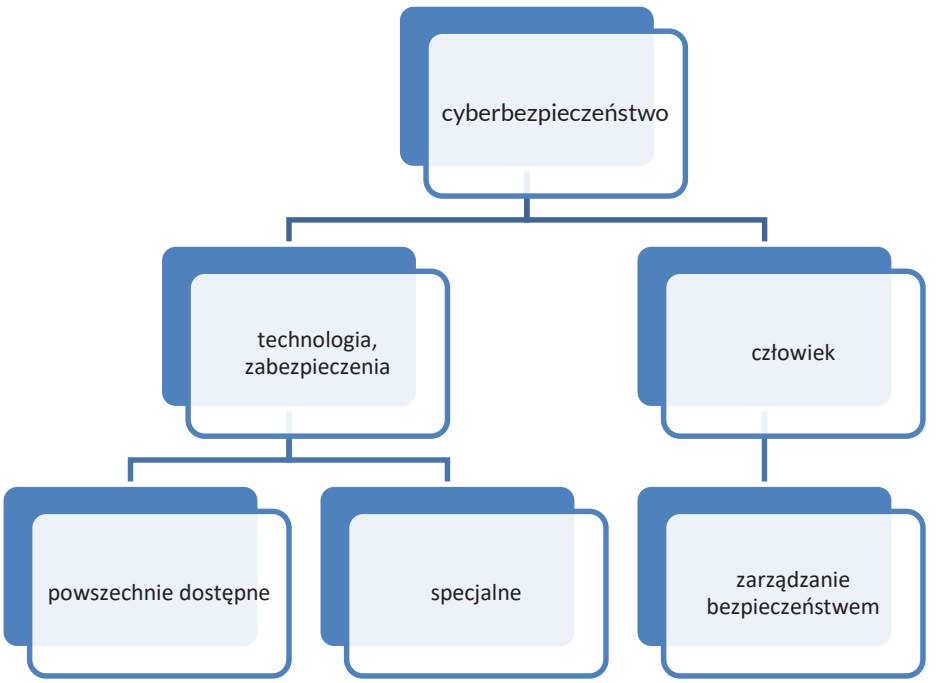
10 Zob. ibidem; A. Urbanek, *Zagrożenia asymetryczne czy asymetryczność zagrożeń* [w:] *Wyzwania i zagrożenia w XXI wieku. Aspekty militarne i niemilitarne*, red. M. Borkowski, M. Stańczyk-Minkiewicz, I. Ziemkiewicz-Gawlik, Słupsk 2013; A. Urbanek, *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa*, „Studia nad Bezpieczeństwem" 2016, nr 1, s. 5–32.

11 Edyta Sadowska (*Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11, nr 2, s. 24) pisze: „W ujęciu politologicznym natomiast badacze wychodzą poza schemat działania wojsk regularnych i tradycyjnie rozumianych konfliktów zbrojnych i przenoszą ciężar definicji na działania podmiotów niepaństwowych, wymieniając między innymi: terroryzm, przestępczość zorganizowaną, handel bronią, handel narkotykami, stosowanie technologii teleinformatycznych".

12 T. Hoffman, *Główni aktorzy cyberprzestrzeni i ich działalność* [w:] *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T. Dębowski, Łódź 2018, s. 11–30.

Kategorie cyberbezpieczeństwa

Oczywiste jest, że w XXI wieku z jednej strony cyberbepzieczeństwo jest terminem powszechnie znanym nie tylko wśród przedstawicieli nauki, lecz także społeczeństwa, które dzięki osiągnięciom techniki informatycznej stało się globalne. Z drugiej strony, jest czymś na kształt skonsolidowanego sposobu działania pozostającego w kontrze do pojawiających się zagrożeń. Trzecim wymiarem czy trzecią kategorią jest środowisko, w którym funkcjonuje.



Źródło: Opracowanie własne.

Schemat cyberbezpieczeństwa w układzie dychotomicznym

Cyberprzestrzeń ma uniwersalny charakter, podobnie jak cyberbepzieczeństwo, trzeba jednak zaznaczyć, że mimo tej niezwykłej cechy zaznaczają się tu pewne kategorie. Nie jest niczym odkrywczym ani niczym nowym bezpieczeństwo w poszczególnych sektorach ludzkiej aktywności (np. finansowe, polityczne, militarne). Systemy zabezpieczeń poszczególnych sektorów stale

się zmienia, wzmacnia[13]. Trudno sobie dziś wyobrazić codzienność bez dostępu do internetu, bez narzędzi czy urządzeń informatycznych. Wszystko jest na swój sposób powiązane, choć, co wyraźnie należy wyróżnić – dostęp do określonych danych jest możliwy tylko dla podmiotów uprawnionych. Oczywiste jest, że strategia ochrony cyberprzestrzeni stanowi jedno z najważniejszych zadań każdego państwa. Praktyka dowodzi, że właśnie ta przestrzeń jest celem ataku nie tylko pospolitych przestępców, lecz także obcych służb wywiadowczych oraz innych podmiotów mających za zadanie przejęcie informacji, zniszczenie danych, co może prowadzić do destabilizacji gospodarczej, politycznej czy społecznej. Niezmiernie ważne jest to, że właśnie uniwersalność stanowi podstawową cechę tej przestrzeni. W każdym państwie istnieje sektor publiczny i prywatny, i oba obejmuje cyberprzestrzeń. W niej usytuowane są wszystkie strefy – od komunikatorów, poprzez platformy social mediów, po sektor bankowy i militarny. Kategorie cyberbezpieczeństwa odnoszą się praktycznie do każdej sfery, a klasyfikację wyznacza przyjęte kryterium podziału.

Uniwersalność cyberbezpieczeństwa

Termin „uniwersalność" oznacza „[...] obejmujący całość, dotyczący wszystkiego lub wszystkich"[14]. Pod koniec 2020 roku „Komisja Europejska przedstawiła nowy pakiet cyberbezpieczeństwa. W jego skład, poza nową Strategią Cyberbezpieczeństwa, weszły propozycje dwóch aktów: Dyrektywa w sprawie odporności podmiotów krytycznych (Directive on the resilience of critical entities) – Dyrektywa RCE oraz Dyrektywa w sprawie działań na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (Directive on measures for high common level of cybersecurity across the Union) – Dyrektywa NIS 2"[15]. Proponowana strategia niezależnie od oferowanych rozwiązań cechuje się przede wszystkim uniwersalizmem ze względu na jednolite rozwiązania oraz odniesienie do wszystkich państw członkowskich. Podstawowe

13 Marek Górka (*Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa* [w:] ibidem, s. 31) pisze: „[...] w epoce informacji, wszystkie kluczowe sektory ludzkiej działalności jak: polityka, gospodarka, biznes, finanse, transport, infrastruktura, poczta, telekomunikacja, medycyna oraz nauka są ściśle zależne od technologii informacyjnych".

14 *Uniwersalność*, https://sjp.pwn.pl/slowniki/uniwersalność.html [dostęp: 28.06.2023].

15 M. Wrzosek, *Dyrektywa w sprawie odporności podmiotów krytycznych i Dyrektywa NIS 2 – nowe wyzwania dla operatorów w zakresie cyberbezpieczeństwa*, „Nowa Energia" 2021, nr 5–6, s. 65.

są: ocena ryzyka i polityki bezpieczeństwa, zapewnienie ciągłości działania i zarządzania kryzysowego, obsługa incydentów, kryptografia i szyfrowanie[16]. Współczesny świat zatrzymuje się, jeżeli niemożliwy staje się dostęp do sieci, kiedy nie ma prądu. Cyfryzacja stała się faktem we wszystkich dziedzinach ludzkiej aktywności. Właśnie te sektory, niezależnie od geograficznego położenia, są chronione, co czyni cyberbezpieczeństwo zagadnieniem uniwersalnym. Cyberprzestrzeń jest wszechobecna, każdy ma do niej dostęp, jest zatem uniwersalna. W literaturze przedmiotu wskazuje się, że cyberbezpieczeństwo jest problemem zarówno globalnym[17], regionalnym[18], jak i każdej organizacji, w tym państw. Takie podejści sprawia, że stało się terminem o bardzo szerokim spektrum, a zatem uniwersalnym, bo znanym każdemu. Prawdą jest, że poziom przedmiotowych zabezpieczeń jest zróżnicowany, co nie waży na uniwersalności tego pojęcia.

Zakończenie

Problem bezpieczeństwa w cyberprzestrzeni stale przybiera na znaczeniu, podobnie jak stale aktualny jest problem bezpieczeństwa rozumianego w jak najszerszym zakresie. Z jednej strony wydaje się, że wszyscy rozumiemy, czym jest bezpieczeństwo i jak bardzo jest ono ważne dla każdego podmiotu, z drugiej, rzadko zdajemy sobie sprawę z rangi zagrożeń w różnych sektorach aktywności współczesnego człowieka, w szczególności tych, które są w cyberprzestrzeni. Autorzy niniejszego opracowania podjęli próbę odpowiedzi na pytanie: Czy uniwersalność jako cecha cyberbezpieczeństwa jest przedstawiana w istniejących w literaturze naukowej definicjach, a jeżeli tak, to w jaki sposób? Analizując literaturę przedmiotu (z racji rodzaju opracowania wąski jej wycinek), można przyjąć, że cyberbezpieczeństwo ma uniwersalny charakter przejawiający się w rozwiązaniach prawnych różnych państw. Istotne są tutaj przyjęte strategie bezpieczeństwa w państwach Unii Europejskiej, a także i te obowiązujące w Stanach Zjednoczonych. Uniwersalność oznacza niezmiennie to samo – „obejmujące całość", a cyberprzestrzeń tym właśnie się wyróżnia.

16 Ibidem, s. 67.
17 Zob. m.in. A. Zieliński, *Cyberbezpieczeństwo – problem globalny*, „Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne" 2018, nr 10, s. 864–869.
18 M. Kudzin-Borkowska, *Cyberbezpieczeństwo w Grupie Wyszehradzkiej – koncepcje i strategie*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 24, s. 46–62.

Jak każda przestrzeń, wymaga ochrony, co w XXI wieku jest naturalne. Współczesny świat na swój sposób przeniósł aktywność do wirtualnej rzeczywistości, w tym finansową, medyczną, farmaceutyczną, gospodarczą, komunikacyjną, edukacyjną, ale i zarządzanie jako formę sprawowania władztwa. To przeniesienie było możliwe wyłącznie w połączeniu z zabezpieczeniem baz danych wszelkiego rodzaju, w tym także tych o wysokim stopniu wrażliwości. Skomplikowane systemy ochrony cyberprzestrzeni są stale modyfikowane, ulepszane, ponieważ, jak dowodzi praktyka, co jakiś czas dochodzi do złamania zabezpieczeń, co łączy się z poważnymi zagrożeniami w tej przestrzeni. Uniwersalność to powszechny dostęp (niekiedy z pewnymi problemami), możliwość komunikowania się z innymi ludźmi na całym świecie, korzystania z zasobów nauki, kultury w najodleglejszych zakątkach, to możliwość monitorowania miejsc o szczególnym znaczeniu dla bezpieczeństwa ludzi. Można mnożyć przykłady w tym względzie, lecz nie wydaje się to konieczne.

Jednakże najważniejsze jest jedno – umiejętność bezpiecznego korzystania z cyberprzestrzeni.

Bibliografia

Chałubińska-Jentkiewicz K., *Cyberbepieczeństwo – zagadnienia definicyjne* „Cybersecurity and Law" 2019, nr 2.

Dziwisz D., *Cyberbezpieczeństwo – nowy priorytet strategii obrony Stanów Zjednoczonych?*, „Sprawy Międzynarodowe" 2011, nr 3.

Giebień H., *Cyberbezpieczeństwo w Federacji Rosyjskiej. Zarys problemu*, „Wschodnioznawstwo" 2018, nr 12.

Górka M., *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa* [w:] *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T. Dębowski, Łódź 2018.

Hoffman T., *Główni aktorzy cyberprzestrzeni i ich działalność* [w:] *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T. Dębowski, Łódź 2018.

Hydzik W., *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 3.

Janus D., *Między siłą a informacją. Zarządzanie Internetem, cyberbezpieczeństwo i nowe technologie w Chinach po XIX Zjeździe KPCh*, „Azja–Pacyfik" 2020, nr 23.

Kudzin-Borkowska M., *Cyberbezpieczeństwo w Grupie Wyszehradzkiej – koncepcje i strategie*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 24.

Lisiak-Felicka D., Pytko M., *Cyberbezpieczeństwo urzędów gmin w województwie łódzkim*, „Przedsiębiorczość i Zarządzanie" 2017, t. 18, nr 4, cz. 1.

Madej M., *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego – próba teoretycznej konceptualizacji* [w:] *Porządek międzynarodowy u progu XXI wieku*, red. R. Kuźniar, Warszawa 2005.

Radziejewski R., *Cyberbezpieczeństwo w administracji rządowej w Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16.

Sadowska E., *Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, t. 11, nr 2.

Urbanek A., *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa*, „Studia nad Bezpieczeństwem" 2016, nr 1.

Urbanek A., *Zagrożenia asymetryczne czy asymetryczność zagrożeń* [w:] *Wyzwania i zagrożenia w XXI wieku. Aspekty militarne i niemilitarne*, red. M. Borkowski, M. Stańczyk-Minkiewicz, I. Ziemkiewicz-Gawlik, Słupsk 2013.
Worona J., *Prace naczelnych organów administracji państwowej a cyberbezpieczeństwo Polski*, „Białostockie Studia Prawnicze" 2016, z. 20/B.
Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 27.
Wrzosek M., *Dyrektywa w sprawie odporności podmiotów krytycznych i Dyrektywa NIS 2 – nowe wyzwania dla operatorów w zakresie cyberbezpieczeństwa*, „Nowa Energia" 2021, nr 5–6.
Zieliński A., *Cyberbezpieczeństwo – problem globalny*, „Przegląd Telekomunikacyjny – Wiadomości Telekomunikacyjne" 2018, nr 10.

Around the definition of cybersecurity

Abstract

The concept of cyber security has become part of the reality of the late 20th and 21st centuries. This term is understood as a system that blocks threats consisting in destroying, changing and unauthorized interception of data. The importance of the cybersecurity problem was emphasized by making legal regulations in the legislation of many countries around the world, including Poland, the United States, Russia and China, and on the basis of the provisions of state associations or international organizations, which is reflected in the relevant regulations of the European Union. The concept of cyber security is multi-faceted, becoming an object of interest not only to countries or organizations, but also to individual individuals living in given communities. The progressive digitization of many areas of life, regardless of the geographical location of the country, means that the need to ensure the proper and safe functioning of this sphere of reality determines the universality of cyber security.

Key words: cyberspace, security, law, digitization, directive, European Union