CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski
Władysław Hydzik, Dariusz Jagiełło, Filip Krzyżankiewicz
Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak
Adam Szafrański, Ryszard Szpyra, Kazimierz Waćkowski
Paweł Widawski, Joanna Worona, Zofia Zawadzka

SERIA AKADEMICKA

Wolters Kluwer

CYBERBEZPIECZEŃSTWO

Zarys wykładu

redakcja naukowa Cezary Banasiński

Cezary Banasiński, Cezary Błaszczyk, Jacek M. Chmielewski
Władysław Hydzik, Dariusz Jagiełło, Filip Krzyżankiewicz
Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak
Adam Szafrański, Ryszard Szpyra, Kazimierz Waćkowski
Paweł Widawski, Joanna Worona, Zofia Zawadzka

SERIA AKADEMICKA

Wolters Kluwer

WARSZAWA 2018

Stan prawny na 15 października 2018 r.

Recenzent
Prof. dr hab. Hanna Gronkiewicz-Waltz

Wydawca
Agata Jędrasik

Redaktor prowadzący
Joanna Ołówek

Opracowanie redakcyjne i łamanie
Violet Design Wioletta Kowalska

Poszczególne rozdziały napisali:

Cezary Banasiński – rozdz. I
Cezary Banasiński, Włodzimierz Nowak – rozdz. III
Cezary Błaszczyk – rozdz. VII
Jacek M. Chmielewski, Kazimierz Waćkowski – rozdz. II
Władysław Hydzik – rozdz. IX
Dariusz Jagiełło – rozdz. XIV, XV
Filip Krzyżankiewicz, Arwid Mednis – rozdz. XII
Włodzimierz Nowak – rozdz. IV
Marcin Rojszczak – rozdz. V, VIII
Adam Szafrański – rozdz. XIII
Ryszard Szpyra – rozdz. VI
Paweł Widawski – rozdz. X
Joanna Worona, Zofia Zawadzka – rozdz. XI

ISBN 978-83-8160-139-9

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa NIS	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)
dyrektywa o e-prywatności	–	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.Urz. UE L 201, s. 37)
dyrektywa PSD2	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L 337, s. 35)
dyrektywa ramowa	–	dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.Urz. UE L 108, s. 33)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2018 r. poz. 1025 ze zm.)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2017 r. poz. 2204 ze zm.)
Konstytucja RP	–	Konstytucja Rzeczpospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze zm.)
k.p.c.	–	ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2018 r. poz. 1360)
k.p.k.	–	ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2017 r. poz. 1907 ze zm.)
KPP	–	Karta Praw Podstawowych Unii Europejskiej z 30.03.2010 r. (Dz.Urz. UE C 83, s. 389)
k.s.h.	–	ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2017 r. poz. 1577 ze zm.)
k.w.	–	ustawa z 20.05.1971 r. – Kodeks wykroczeń (Dz.U. z 2018 r. poz. 618 ze zm.)
pr. aut.	–	ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2018 r. poz. 1191 ze zm.)
pr. kon.	–	ustawa z 30.05.2014 r. o prawach konsumenta (Dz.U. z 2017 r. poz. 683 ze zm.)

pr. tel. – ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017 r. poz. 1907 ze zm.)

p.w.p. – ustawa z 30.06.2000 r. – Prawo własności przemysłowej (Dz.U. z 2017 r. poz. 776 ze zm.)

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)

rozporządzenie eIDAS – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73)

TUE – Traktat o Unii Europejskiej z 7.06.2016 r. (wersja skonsolidowana: Dz.Urz. UE C 202 z 2016 r., s. 13)

u.o.b.d. – ustawa z 27.07.2001 o ochronie baz danych (Dz.U. poz. 1402 ze zm.)

u.o.d.o. – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000)

u.ś.u.d.e. – ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2017 r. poz. 1219 ze zm.)

u.u.p. – ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2017 r. poz. 2003 ze zm.)

u.u.z.i.e. – ustawa z 5.09.2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r. poz. 1579 ze zm.)

u.z.n.k. – ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2018 r. poz. 419)

Czasopisma

OSNC – Orzecznictwo Sądu Najwyższego. Izba Cywilna

OSNKW – Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa

OSNP – Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych

OSNwSK – Orzecznictwo Sądu Najwyższego w Sprawach Karnych

OTK-A – Orzecznictwo Trybunału Konstytucyjnego. Seria A

ZNUJ PPWI – Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej

ZNUJ PWiOWI – Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej

Inne

ABW – Agencja Bezpieczeństwa Wewnętrznego

APT – złożony permanentny atak (ang. *advanced persistent threat*)

DNS – system nazw domenowych (ang. *domain name system*)

ENISA – Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ang. *European Network and Information Security Agency*)

EBC – Europejski Bank Centralny
EUNB – Europejski Urząd Nadzoru Bankowego
GIODO – Generalny Inspektor Ochrony Danych Osobowych
ICT – technologie informacyjne i komunikacyjne (ang. *information and communication technologies*)
IGF – Forum Zarządzania Internetem (ang. *Internet Governance Forum*)
IT – technologia informacyjna (ang. *information technology*)
KNF – Komisja Nadzoru Finansowego
NASK – Naukowa i Akademicka Sieć Komputerowa
NATO – Organizacja Traktatu Północnoatlantyckiego (ang. *North Atlantic Treaty Organization*)
ONZ – Organizacja Narodów Zjednoczonych
resp. – odnośnie, względnie (ang. *respective*)
SA – sąd apelacyjny
SCA – silne uwierzytelnianie klienta (ang. *strong customer authentication*)
SN – Sąd Najwyższy
SR – sąd rejonowy
SZBI – system zarządzania bezpieczeństwem informacji
TSUE – Trybunał Sprawiedliwości Unii Europejskiej
UE – Unia Europejska
UKE – Urząd Komunikacji Elektronicznej
UODO – Urząd Ochrony Danych Osobowych
UOKIK – Urząd Ochrony Konkurencji i Konsumentów
WSA – wojewódzki sąd administracyjny

WSTĘP

Postępująca cyfryzacja niemal wszystkich dziedzin współczesnego życia niesie za sobą nie tylko korzyści, lecz także zagrożenia, wzmacniane przy tym przez niezwykłą wręcz dynamikę i nieprzewidywalność rozwoju technologicznego ostatnich lat. Stąd też zainteresowanie tematyką zagrożeń w cyberprzestrzeni i ochrony przed nimi przestało być domeną wąskiej grupy specjalistów, stając się niebudzącym wątpliwości istotnym problemem współczesnego świata. Pytanie, na ile możliwość ziszczenia się ponurych wizji „cybernetycznego Pearl Harbor" jest realna, pozostaje w sposób oczywisty bez odpowiedzi. Niemniej zagwarantowanie bezpieczeństwa w cyberprzestrzeni jest wyjątkowo aktualnym wyzwaniem praktycznie dla każdego użytkownika systemów teleinformatycznych.

Podręcznik skierowany jest do osób, których przedmiotem zainteresowania jest problematyka cyberbezpieczeństwa, i to zarówno z zakresu nauk ścisłych, jak i nauk humanistycznych. Zagadnienie cyberbezpieczeństa ma bowiem charakter interdyscyplinarny, podobnie jak nauki o bezpieczeństwie, których integralnym i niezwykle istotnym współcześnie fragmentem jest właśnie bezpieczeństwo w cyberprzestrzeni. Problem cyberbezpieczeństwa dotyczy przy tym różnych dziedzin aktywności ludzkiej. Podmiotami cyberbezpieczeństwa są przedsiębiorcy, państwa, organizacje międzynarodowe, wirtualne społeczności internetowe czy wreszcie poszczególni użytkownicy sieci. Dlatego każdy zainteresowany obszarem bezpieczeństwa sieci oraz systemów informatycznych Czytelnik tej książki – pomimo że formalnie jest ona podręcznikiem akademickim – znajdzie w niej zapewne coś interesującego dla siebie. Publikacja zawiera bowiem niezbędne informacje techniczne, prawne, organizacyjne dotyczące bezpieczeństwa systemów operacyjnych, sieci komputerowych oraz telekomunikacyjnych i zarazem bezpieczeństwa gromadzonych, przetwarzanych i wysyłanych danych. Zakres treściowy opracowania wychodzi naprzeciw także potrzebom praktyków uczestniczących w procesach zachowania bezpieczeństwa informatycznego, których zadaniem jest monitorowanie, detekcja oraz analiza ryzyk i zagrożeń dla sprawnego funkcjonowania systemów informatycznych.

W książce – będącej jak każdy podręcznik kompromisem między wymogiem zwięzłości wykładu a potrzebą jego wszechstronności – skupiono się na najważniejszych kwestiach z zakresu bezpieczeństwa w cyberprzestrzeni.

Część pierwsza jest wprowadzeniem do problematyki cyberbezpieczeństwa. Omówione zostały podstawy prawne bezpieczeństwa w cyberprzestrzeni. Przedstawiono również zasadnicze dylematy terminologiczne związane z prezentowaną w książce tematyką. Przybliżono kwestie technologii teleinformatycznych, ich rozwoju oraz bezpieczeństwa, zwłaszcza w kontekście zarządzania usługami IT, przeanalizowano rodzaje ataków sieciowych, w tym ataków ukierunkowanych, a także odniesiono się do problemu zapór sieciowych czy czynników wpływających na podatność infrastruktury na cyberataki.

Część druga odnosi się do cyberbezpieczeństwa z perspektywy państwa. Omówione zostały ustrojowe (organizacyjne) podstawy europejskiego i krajowego systemu cyberbezpieczeństwa. Przedstawiono także zasadnicze zasady ochrony infrastruktury krytycznej służące zapewnieniu sprawnego funkcjonowania administracji publicznej, instytucji i przedsiębiorców z punktu widzenia zagrożeń i ryzyk wykorzystywania tej infrastruktury; z uwagi na złożoność problemu kwestię tę ujęto z punktu widzenia norm technicznych oraz od strony nauk o zarządzaniu. Odniesiono się również do sektora łączności elektronicznej, którego znaczenie jest bezprecedensowe z perspektywy omawianej w podręczniku tematyki. Dopełnieniem tej części opracowania jest ukazanie problemu w płaszczyźnie militarnej, gdzie analiza podstawowych elementów cyberbezpieczeństwa skorelowana została ze współczesnymi militarnymi koncepcjami prowadzenia operacji wojskowych w cyberprzestrzeni.

Część trzecia jest analizą cyberbezpieczeństwa z punktu widzenia przedsiębiorcy. Przybliżone zostały zagadnienia cywilnoprawnego obrotu gospodarczego w cyberprzestrzeni. Odniesiono się także do modeli wdrażania cyberbezpieczeństwa przez przedsiębiorców, jak np. warstwowego modelu bezpieczeństwa informacyjnego, modeli zarządzania bezpieczeństwem IT według norm ISO/IEC oraz innych koncepcji, w tym m.in. opartych na zaleceniach i wytycznych Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji. Kwestie te istotnie uzupełnia problematyka zarządzania ryzykiem przez przedsiębiorcę. Omówiono również zagadnienia cyberbezpieczeństwa w najbardziej wrażliwym z punktu widzenia przedmiotu opracowania sektorze gospodarki, a mianowicie sektorze bankowym. Tę część zamyka analiza cyberbezpieczeństwa od strony prawa własności intelektualnej.

Część czwarta dotyczy bezpieczeństwa obywateli w cyberprzestrzeni. Zwrócono tu uwagę, z jednej strony, na fundamentalną dla każdego obywatela ochronę prywatności i danych osobowych, z drugiej zaś – na wyjątkowo newralgiczną społecznie ochronę dzieci i młodzieży w cyberprzestrzeni przed szkodliwymi dla ich rozwoju treściami.

W części ostatniej, poświęconej cyberprzestępczości, przybliżono karnoprawne ramy odpowiedzialności za przestępstwa popełniane w cyberprzestrzeni, uzupełniając regulacje materialnoprawne także problematyką karnoprocesową i śledczą.

Idea podręcznika do cyberbezpieczeństwa powstała w ramach Pracowni Nowych Technologii Zakładu Prawa Administracyjnego Gospodarczego i Bankowego Wydziału Prawa i Administracji Uniwersytetu Warszawskiego na potrzeby wykładu specjalizacyjnego. Stąd też książka została podzielona na pięć bloków tematycznych podporządkowanych 30-godzinnemu semestralnemu wykładowi akademickiemu, a zatem 15 półtoragodzinnym standardowym wykładom. Zagadnienia prezentowane w podręczniku uzupełnia obszerna bibliografia oraz liczne odniesienia do materiałów źródłowych dające Czytelnikowi szansę pogłębienia zagadnień zawartych w publikacji.

Przygotowując podręcznik, autorzy dążyli nie tylko do przekazania niezbędnej wiedzy teoretycznej, lecz także koniecznych informacji praktycznych, co przy wykładaniu problematyki cyberbezpieczeństwa jest warunkiem jej efektywnego nauczania. Proporcje w tym zakresie zostały podporządkowane treści poszczególnych obszarów tematycznych. Mając świadomość, że opracowanie siłą rzeczy nie obejmuje wszystkich zagadnień tej niezwykle szerokiej tematyki, jaką jest cyberbezpieczeństwo, autorzy będą wdzięczni za wszelkie uwagi dotyczące zawartości oddawanej do rąk Czytelników książki.

Autorzy

Część I

WPROWADZENIE DO PROBLEMATYKI CYBERBEZPIECZEŃSTWA

Rozdział I

PODSTAWOWE POJĘCIA I PODSTAWY PRAWNE BEZPIECZEŃSTWA W CYBERPRZESTRZENI

1. Pojęcia cyberbezpieczeństwa i cyberprzestrzeni

1.1. Wprowadzenie

Pojęcia cyberbezpieczeństwa i cyberprzestrzeni nieodłącznie wiążą się z rewolucją dostępu do informacji wskutek rewolucji informatycznej ostatnich lat; oba zjawiska są ze sobą ściśle związane.

W literaturze brak jest powszechnie akceptowanego pojęcia informacji; w pewnym sensie jest to termin złożony, interdyscyplinarny, definiowany odmiennie w różnych naukach, niemający jednoznacznej, powszechnej definicji. Często nie definiuje się w rozważaniach dotyczących informacji samego pojęcia informacji, „zadowalając się jego znaczeniem potocznym jako komunikatu – wiadomości, wyrażonych w dowolny sposób”[1].

Z punktu widzenia cybernetyki oraz teorii informacji[2] termin ten definiowany jest jako „zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne”[3]. W ujęciu tym informacja jest pojęciem

[1] T. Szewc, *Publicznoprawna ochrona informacji*, Warszawa 2007, s. 4.

[2] Szerzej o informacji J. Petzel, *Informatyka prawnicza, Zagadnienia teorii i praktyki*, Warszawa 1999, s. 35 i n.

[3] P. Sienkiewicz, *10 wykładów*, Warszawa 2005, s. 62, cyt. za M. Kłodawski, *Pojęcie informacji w naukach teoretycznoprawnych*, s. 5; https://depot.ceon.pl/bitstream/handle/123456789/316/Maciej_Klodawski_-_Pojecie_informacji_w_naukach_teoretycznoprawnych.pdf (dostęp: 20.08.2018 r.).

ściśle związanym z człowiekiem i zdolnością jego celowego działania[4]. Ale już w ujęciu szerszym, pozwalającym połączyć podejście jakościowe do informacji z ilościowym ujęciem matematycznym (ITI), informacja to każdy czynnik, który ludzie, inne organizmy żywe, ale również i urządzenia automatyczne mogą spożytkować do celowego działania. Tak też traktuje informację – na potrzeby jej przetwarzania – Polska Norma PN-ISO/IEC 2382-1:1996-01.01.02, która utożsamia informację z wiedzą dotyczącą obiektów, takich jak: fakty, zdarzenia, przedmioty, procesy lub idee, zawierającą koncepcję, która w określonym kontekście ma określone znaczenie; pozwala to odróżnić informację od terminu „dane", który w tej samej normie traktowany jest jako „reprezentacja informacji mająca interpretację, właściwą do komunikowania się, interpretacji lub przetwarzania"[5].

Niezależnie jednak od różnych prób definiowania pojęcia informacji można przyjąć generalnie, że informacja jest przenaszalnym dobrem niematerialnym zmniejszającym niepewność[6]. Informacja zawarta w komunikacie umożliwia przy tym podjęcie określonej reakcji na treści w niej zawarte.

Istotny jest jednak nie tyle spór definicyjny o istotę tego pojęcia[7], ile fakt, że rozwój technologii informacyjnych i komunikacyjnych (ICT, ang. *information and communication technologies*[8]) i ich współczesna powszechność[9] spowodował natomiast wyjątkową łatwość (swobodę) dystrybucji, dostępu i wymiany informacji. Ta będąca wynikiem rewolucji informatycznej dostępność informacji stworzyła podstawę dla integracji wiedzy, technologii, gospodarki i kultury[10], ewoluując w efekcie w kierunku społeczeństwa informacyjnego z jego informacyjną, nierzadko globalną, gospodarką, pozbawionego organizacyjnych czy administracyjnych granic terytorialnych[11]. Informacja stała się zasadniczym dobrem ekonomicznym, warunkując rozwój społeczny, ale także niosąc dla tego rozwoju istotne zagrożenia społeczne, gospodarcze czy kul-

[4] L. Ciborowski cyt. za R. Kwećka, *Informacja w walce zbrojnej*, Warszawa 2001, s. 17.

[5] Szeroko D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 25 i n.

[6] G. Szpor, *Bezpieczeństwo danych osobowych a ochrona informacji niejawnych i biznesowych* [w:] *Ochrona informacji niejawnych i biznesowych*, red. M. Gajos, S. Zalewski, Katowice 2005, s. 34.

[7] Szeroko M.J. Schroeder, *Spór o pojęcie informacji*, „Studia Metodologiczne" 2015/34, s. 11.

[8] Pod pojęciem tym należy rozumieć grupę technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej. Węższym pojęciem są technologie informatyczne (IT), które odnoszą się do technologii związanych z komputerami i oprogramowaniem, niezwiązanych jednak z technologiami komunikacyjnymi i dotyczącymi sieci. Rozwój tych technologii sprawia, że oba pojęcia stają się coraz bardziej zbliżone treściowo.

[9] M. Leszczyńska, *Współczesny model rozwoju społecznego z perspektywy rewolucji informacyjnej* [w:] *Nierówności społeczne a wzrost gospodarczy. Społeczeństwo informacyjne – regionalne aspekty rozwoju*, red. M. Woźniak, Rzeszów 2011, s. 129.

[10] M. Niezgoda, *Społeczeństwo informacyjne w perspektywie socjologicznej: idea czy rzeczywistość?* [w:] *Społaczeństwo informacyjne – wizja czy rzeczywistość*, red. L. Haber, Kraków 2003, s. 122 i n.

[11] Szeroko T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania*, Kraków 1999, s. 78.

turowe. Najczęściej wyróżnianymi formami zagrożeń teleinformatycznych są: haking, haktywizm, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, wykorzystanie cyberprzestrzeni jako piątego teatru działań zbrojnych[12] czy wreszcie skutki niekontrolowanego użycia internetu w sferze społecznej i psychicznej[13].

1.2. Pojęcie cyberprzestrzeni

Pojęcie cyberprzestrzeni należy do kategorii pojęć niedookreślonych. Od strony semantycznej cyberprzestrzeń jest hybrydą pojęciową będącą skrótem od sformułowania ang. *cybernetics space*, czyli przestrzeni cybernetycznej.

Termin „cyberprzestrzeń" został wykreowany na potrzeby literatury science fiction i spopularyzowany przez Williama Gibsona, który określił cyberprzestrzeń jako niewyobrażalną złożoność będącą niczym „konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach (…)"[14]. To literackie określenie cyberprzestrzeni z trudnością poddaje się naukowemu zdefiniowaniu, które odpowiadałoby wymogom teorii zastosowania reguł semiotycznych i praw logiki formalnej do działalności naukowej, czyli ogólnej metodologii nauk. Stąd też pojęcie cyberprzestrzeni traktowane jest czasami jako nic nie znaczące hasło, całkowicie nieprzydatne w badaniach naukowych, co dotyczy zwłaszcza nauk technicznych, czasem jako dość ogólne sformułowanie odnoszące się do środowiska społecznego komunikującego się przy pomocy technik stosowanych z użyciem komputera (cybertechnologie), czy też jako zjawisko, którego skutki występowania są analizowane w ramach stosowania cybernetyki społecznej do komunikacji komputerowej (cyberkomunikacji)[15]. Nie jest nawet jasny źródłosłów pojęcia cyberprzestrzeni; jedynie ogólnie można stwierdzić, że jest to zbitka słowna (hybryda) dwóch słów – *kybernets,* co w języku greckim oznacza sternik, zarządca, kontrolować, oraz *space*, czyli – w dosłownym tłumaczeniu z języka angielskiego – przestrzeń. Niejednoznaczne są zwłaszcza związki pojęcia cyberprzestrzeni z cybernetyką, z której bez wątpienia zapożyczono pojęcie cyberprzestrzeni w literaturze science fiction. Związki te są krytykowane w literaturze[16], aczkolwiek z drugiej strony zwraca się również uwagę, że z punktu widzenia etymologicznego pojęcie cyberprzestrzeni wywodzi się z cybernetyki[17], ukształtowanej przez Norberta Wienera, jako nauki o sterowaniu i komu-

[12] Szeroko *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.

[13] Szeroko *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, red. D. Morańska, Dąbrowa Górnicza 2015.

[14] Za J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013/9, s. 226.

[15] Zob. m.in. J. Janowski, *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*, Warszawa 2012; J. Janowski, *Globalna cyberkultura polityki i prawa*, http://www.bibliotekacyfrowa.pl/Content/46512/23_Jacek_Janowski.pdf, s. 311 i n. (dostęp: 20.08.2018 r.).

[16] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 60 i n.

[17] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, s. 74.

Cyberbezpieczeństwo jest przedmiotem analiz zarówno w naukach prawnych, technicznych, jak i stosunkach międzynarodowych czy wojskowości. Praca została zaplanowana jako interdyscyplinarny podręcznik akademicki, zawierający omówienie najważniejszych obszarów cyberbezpieczeństwa, m.in.:
– bezpieczeństwa państwa,
– bezpieczeństwa cyfrowego obrotu gospodarczego,
– cyberbezpieczeństwa przedsiębiorcy oraz obywatela.

W publikacji odniesiono się do aktualnych regulacji prawnych – takich jak rozporządzenie 2016/679 (RODO) oraz ustawa o krajowym systemie cyberbezpieczeństwa. Przedstawiono także omówienie uznawanych międzynarodowo standardów z rodziny ISO/IEC 27000 w obszarze zarządzania ryzykiem oraz budowy systemów zarządzania bezpieczeństwem informacji. Dokonano także analizy aktualnych przepisów prawnokarnych związanych z obszarem przestępstw komputerowych oraz zaleceń związanych z procesem zabezpieczania dowodów elektronicznych.

Autorami są zarówno pracownicy naukowi reprezentujący różne środowiska naukowe, m.in.: Uniwersytet Warszawski, Uniwersytet SWPS, Politechnika Warszawska czy Akademia Obrony Narodowej, jak i praktycy zajmujący się problematyką cyberbezpieczeństwa w pracy zawodowej.

Publikacja jest przeznaczona dla studentów prawa oraz informatyki, a także słuchaczy studiów podyplomowych z zakresu cyberbezpieczeństwa. Będzie także cennym źródłem wiedzy dla szerokiego grona praktyków, specjalistów zajmujących się na co dzień zagadnieniami z obszaru bezpieczeństwa IT.

9788381601399 W01P01

ZAMÓWIENIA:
INFOLINIA 801 04 45 45, FAX 22 535 80 01
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL

ISBN 978-83-8160-139-9
9 788381 601399

CENA 59 ZŁ (W TYM 5% VAT)