Kultura Bezpieczeństwa
Nr 10/2018

Weronika Siłuszyk
Uniwersytet Przyrodniczo-Humanistyczny
w Siedlcach

Bezpieczeństwo informacyjne w XXI wieku, redakcja naukowa Mariusz Kubiak i Stanisław Topolewski, Siedlce-Warszawa 2016, ss. 187.

Information security in the 21st century, scientific editors: Mariusz Kubiak and Stanisław Topolewski, Siedlce-Warsaw 2016, pp. 187.

XXI wiek to czas gwałtownych przemian dokonujących się w obszarze technologicznym i informatycznym. Urządzenia mobilne, takie jak telefony komórkowe, tablety, laptopy nieodłącznie towarzyszą życiu człowieka. Można by rzec, że opanowały one całą sferę życiową człowieka. Podobnie jak media społecznościowe i komunikacyjne, które przyczyniły się do tego, że z każdej strony zalewa nas fala informacji, nie do końca prawdziwych i rzetelnych. Dla zwykłego obywatela, odbiorcy są one niespójnym, chaotycznym przekazem, przez który może zostać zakłócone jego prawidłowe funkcjonowanie. Obecnie informacja stanowi także ważny element strategiczny państwa. Wyciek ważnych, ściśle tajnych danych poza terytorium państwa bądź strukturę organizacyjną jednostki może powodować poważne zagrożenia. Każdy rodzaj bezpieczeństwa narodowego, począwszy od politycznego, militarnego, społecznego, ekonomicznego czy kulturowego staje się coraz bardziej zależny od ochrony oraz przepływu informacji. Warto nadmienić, że XXI wiek to czas wojen cybernetycznych, informacyjnych i cyberterroryzmu. Dlatego bezpieczeństwo informacyjne staje się wyzwaniem dla państwa, zaś przez obywateli odbierane jest głównie jako szansa. O bez-

pieczeństwie informacyjnym możemy mówić w dwóch aspektach: jako bezpieczeństwie państwa i bezpieczeństwie psychospołecznym obywateli. Płaszczyzny te przenikają się wzajemnie i uzupełniają się.

Bogata literatura uplasowała bezpieczeństwo informacyjne w kryterium przedmiotowym, obok bezpieczeństwa politycznego, ekonomicznego, militarnego itp. Według P. Potejki bezpieczeństwo informacyjne to „zbiór działań, metod oraz procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem". Zaś w ujęciu szerszym E. Nowak i M. Nowak „określają je jako stan warunków wewnętrznych i zewnętrznych, który pozwala państwu na posiadanie, przetrwanie i swobodę rozwoju społeczeństwa informacyjnego".

Z zadowoleniem trzeba przyjąć fakt, że na rynku księgarskim ukazała się wartościowa pozycja z zakresu bezpieczeństwa informacyjnego. Jest to podręcznik akademicki przygotowany głównie przez pracowników związanych z Instytutem Nauk Społecznych i Bezpieczeństwa Wydziału Humanistycznego UPH w Siedlcach, a także pracowników Akademii Sztuki Wojennej, Uniwersytetu w Białymstoku i Politechniki Rzeszowskiej.

Książka *Bezpieczeństwo informacyjne w XXI wieku* składa się z dziesięciu rozdziałów, które tworzą tematyczną całość. Jest aktualną syntezą zagadnień bezpieczeństwa informacyjnego, widzianą przez pryzmat nie tylko standardowych podstaw politycznych, militarnych i ekonomicznych, ale także wewnętrznych, socjalnych i w obszarze środowiskowym. Wiemy, że problematyka ta cały czas się zmienia ze względu na pojawianie się nowych wyzwań i zagrożeń, będących pochodną procesu globalizacji i postępu technologicznego. Praca porządkuje warstwę teoretyczną (definicje, podziały, zależności), wskazuje na ewolucję pewnych poglądów, jak również dotyka prawnych rozwiązań ochrony ważnych informacji.

Publikacja skierowana jest do wszystkich specjalistów zajmujących się, z racji wykonywanego zawodu, bezpieczeństwem informacyjnym, a także studentów takich specjalności, jak: bezpieczeństwo komputerów, bezpieczeństwo sieci i systemów, inżynieria bezpieczeństwa oraz bezpieczeństwo cyberprzestrzeni. Z książki tej można korzystać wybierając, w zależności od potrzeb, poszczególne rozdziały. Każdy z nich stanowi zamkniętą całość zakończoną spisem literatury. Będzie pomoc-

na studentom w przygotowaniu się do zajęć, pisania referatów, robienia prezentacji dotyczącej powyższej tematyki.

W rozdziale pierwszym Bogdan Szulc z Akademii Sztuki Wojennej podejmuje rozważania na temat różnić między naukami o bezpieczeństwie a naukami o obronności. Ze względu na umieszczenie obu istniejących wówczas dyscyplin w dziedzinie nauk społecznych wielu badaczy utożsamia ich aparat metodologiczny. Autor analizuje obie dyscypliny wykazując istniejące między nimi podobieństwa i różnice.

Z kolei Włodzimierz Fehler zamieścił w książce artykuł zatytułowany *O pojęciu bezpieczeństwa informacyjnego*. Uważa, „że w kwestiach związanych z pojmowaniem istoty bezpieczeństwa informacyjnego istnieje spory chaos zwiększany przez propagowanie (często na zasadzie bezrefleksyjnego powielania cudzych poglądów) pojęć błędnych i nieprecyzyjnych bądź też nieaktualnych i nieodzwierciedlających aktualnego stanu wiedzy. Warto zauważyć także, iż rozważania dotyczące bezpieczeństwa informacyjnego bardzo często przyjmują formę inkluzywną, ograniczającą się tylko do ochrony informacji niejawnych i poufnych, cyberprzestrzeni i zachodzących tam zjawisk oraz stosowanych technik oraz narzędzi”. Jego zadaniem było uporządkowanie aparatu pojęciowego, który ma służyć dalszym badaniom w sferze bezpieczeństwa informatycznego. Autor skupił się na takich pojęciach, jak: bezpieczeństwo informacyjne, bezpieczeństwo informacji, polityka bezpieczeństwa informacyjnego, polityka bezpieczeństwa informacji, zagrożenia bezpieczeństwa informacji, walka informacyjna, wojna informacyjna.

W trzecim rozdziale Marian Cieślarczyk podjął problematykę psychospołecznych i prakseologicznych aspektów bezpieczeństwa informacyjnego. Podkreśla on, że w systemach bezpieczeństwa najsłabszym ogniwem jest człowiek i jego kultura bezpieczeństwa. Zwraca więc uwagę na zjawisko kultury bezpieczeństwa informacyjnego i jego element, którym jest kultura informacyjno-komunikacyjna. Zdaniem autora kluczowe znaczenie ma dbałość o bezpieczeństwo informacyjne, bez którego nie można sobie wyobrazić zapewnienia bezpieczeństwa w innych obszarach przedmiotowych, takich jak: bezpieczeństwo ekologiczne i zdrowotne, ekonomiczne i polityczne, społeczne, publiczne i militarne.

Kolejny autor artykułu zatytułowanego *Bezpieczeństwo informacyjne człowieka cywilizacji zachodniej*, Krystian Kiszka zaznacza, że bezpieczeństwa informacyjnego nie można interpretować tylko przez pryzmat ochrony danych zapisanych na różnego rodzaju nośnikach, czy

kanałów ich transmisji lub też ograniczać do zabezpieczania sieci informatycznych. Badacz ten przedstawia perspektywę szerszego pojmowania bezpieczeństwa informacyjnego.

Piąty rozdział, autorstwa Leszka Smolaka, charakteryzuje zjawisko cyberprzestępczości. Analiza przepisów prawnych, umów międzynarodowych, rozporządzeń czy raportów służy definiowaniu, rozumieniu oraz ujęciu skali zjawiska przestępstw w cyberprzestrzeni. Wzrost nowych zagrożeń stanowi niezwykle duże wyzwanie dla prawników i organów prokuratury w zakresie definiowania czynu przestępczego, jak również dla organizacji, służb i podmiotów państwowych. W podsumowaniu autor prezentuje wnioski, z których jeden mówi o tym, „że instytucje i służby koncentrują się głównie zgodnie z prawem na sprawach ściganych z urzędu. A to znaczy, że przed organami ścigania stoi duże wyzwanie, aby zapewnić bezpieczeństwo wszystkim obywatelom na równym poziomie".

Kolejny artykuł dotyczy zjawiska cyberterroryzmu w kontekście zagrożeń dla bezpieczeństwa informacyjnego. Jego autorem jest Waldemar Krztoń. Wzrost znaczenia cyberprzestrzeni i wykorzystania technologii informatycznych powoduje, że cyberterroryzm jest jednym z głównych zagrożeń współczesnego świata. Na początku autor skupia się na zdefiniowaniu terminów „cyberterroryzm" i „cyberprzestrzeń", zestawiając je z obowiązującymi definicjami prawnymi. Nadmienia również, że chociaż organizacje przestępcze nie rezygnują z konwencjonalnych form oddziaływania przestępczego, to jednak trzeba liczyć się z tym, że coraz częściej będą one prowadziły ataki cyberterrorystyczne. Sprzyjają one zachowaniu anonimowości oraz pozwalają na zaatakowanie infrastruktury krytycznej.

Rozdział siódmy autorstwa Magdaleny El Ghamari nosi tytuł *Od Al-Zarkawiego i drugiej generacji Al-Kaidy do kalifatu Al-Baghdadiego – terroryści w „socialmediach"*. Artykuł ten został poświęcony działalności grup terrorystycznych w mediach społecznościowych. Ocenie zostały poddane dostępne materiały odnoszące się do cyberterrorystycznych działań grup wiązanych z Al-Kaidą i z Państwem Islamskim. Praca została wzbogacona zdjęciami, mapami i wykresami. Jednak osoby nieznające języka angielskiego mogą mieć problem ze zrozumieniem tekstu, gdyż nie został on przetłumaczony na język polski.

Mariusz Pala w kolejnym rozdziale zajmuje się problemem zagrożeń bezpieczeństwa informacyjnego. Wymienia dwie główne grupy: zagrożenia dla informacji przechowywanych w systemach informatycz-

nych oraz zagrożenia dla infrastruktury technicznej. Autor poddaje analizie szerokie spektrum podmiotów, które stoją na straży bezpieczeństwa i zestawia je z możliwymi niebezpieczeństwami. Przedstawia również ważne wnioski dla bezpieczeństwa Polski dziś i w przyszłości. Autor wskazuje, że należy liczyć się z naszymi wschodnimi sąsiadami, którzy są pionierami w sferze technologii informatycznych oraz których aktywność w cyberprzestrzeni ciągle wzrasta. Atakują oni nie tylko elementy infrastruktury krytycznej, ale coraz częściej ich ofiarami są dzieci nieświadome zagrożeń płynących z cyberprzestrzeni.

W rozdziale dziewiątym Maciej Tołwiński poruszył problem etyki mediów i etyki dziennikarskiej, wiążąc je z bezpieczeństwem informacyjnym. Jego istotą jest nie tylko ochrona zasobów informacyjnych, ale także nie zawsze rzetelne informowanie obywateli. Do analizy autor wykorzystał dostępne akty prawne. Zwrócił on głównie uwagę na ustawę *Prawo prasowe* oraz *ustawa o radiofonii i telewizji*. Przedstawił katalog dylematów moralnych dziennikarzy, związanych głównie z definiowaniem prawdy. Autor podejmuje się także próby odpowiedzi na pytanie, czy informacja może być oceniana w kategoriach aksjologicznych? Odpowiedź jest bardzo ciekawa, dlatego zachęcam do lektury tego tekstu.

Problematykę wyzwań dla bezpieczeństwa informatycznego Polski i Unii Europejskiej podjął Mariusz Wódka. Przez wyzwania autor rozumie głównie sytuacje problemowe w obszarze bezpieczeństwa informacyjnego, stwarzane zwłaszcza przez szanse i ryzyka oraz dylematy decyzyjne, przed jakimi stoi podmiot w rozstrzyganiu spraw w tym zakresie. Wychodząc od bezpieczeństwa państwa, autor przedstawia możliwe szanse i zagrożenia dla bezpieczeństwa informacyjnego. Szczególną uwagę zwraca na cyberzagrożenia. Załamanie się infrastruktury związanej z szeroko rozumianą informatyzacją państwa może także powodować dezorganizację instytucji odpowiedzialnych za bezpieczeństwo.

Zaletą opracowania jest znaczna liczba danych statystycznych, zestawionych m.in. w tabelach. Podejmowane w książce problemy są zilustrowane, także poprzez rysunki i wykresy. Szkoda tylko, że na końcu pracy nie ma ich spisu, co ułatwiłoby poszukiwanie stosownych informacji. O wysokiej jakości recenzowanej książki stanowią głównie: aktualność i ranga podjętej problematyki, skład zespołu autorskiego, poziom naukowy wszystkich zaprezentowanych w książce referatów, ponadto wpływ profesjonalnej redakcji naukowej na spójność książki, która choć jest pracą zbiorową, stanowi jednak publikację zwartą. Słabszą stroną

książki jest to, że nie zawiera ona zakończenia. Dodatkowym minusem jest fakt, iż – jak już wspomniano – nie przetłumaczono na język polski artykułu Pani Magdaleny El Ghamari. Niemniej jednak książkę można rekomendować wszystkim zainteresowanym problematyką bezpieczeństwa informacji w XXI wieku.

Weronika Siluszyk *– studentka kierunku bezpieczeństwo narodowe, Wydziału Humanistycznego UPH w Siedlcach w Instytucie Nauk Społecznych i Bezpieczeństwa.*