H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; *Bezpieczeństwo. Teoria – badania – praktyka,* A. Czupryński, B. Wiśniewski, J. Zboina (red.), Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. J. Tuliszkowskiego, Józefów 2015; A. Ferrari, *DIGCOMP. Ramy odniesienia dla rozwoju i rozumienia kompetencji cyfrowych w Europie. Raport EUR 26035*, tłum. K. Urban, Biuro Publikacji Komisji Europejskiej, Luksemburg 2013; T. Goban-Klas, *Nadchodzące społeczeństwo medialne*, „Chowanna" 2007, nr 2 (29); *Katalog kompetencji medialnych, informacyjnych i cyfrowych*, Fundacja Nowoczesna Polska–Narodowy Instytut Wizualny, Warszawa 2014; R. Klepka, *Bezpieczeństwo medialne*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; tenże, *Kompetencje medialne społeczeństwa wiedzy*, W. Strykowski, W. Skrzydlewski (red.), Wydawnictwo eMPi2, Poznań 2004; tenże, *Medialna walka o dobrą zmianę. Obraz wyborów parlamentarnych w 2015 roku w wybranych mediach*, Wydawnictwo Libron, Kraków 2018; tenże, *Obrazy polityki w mediach: podstawowe uwarunkowania*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego im. KEN, Kraków 2018; B. McNair, *An Introduction to Political Communication*, Routledge, Taylor & Francis Group, London–New York 2011; R.M. Perloff, *The Dynamics of Political Communication: Media and Politics in a Digital Age*, Routledge, Taylor & Francis Group, New York–London 2014; A. Ogonowska, *Kompetencje medialne*, [w:] *O potrzebie edukacji medialnej w Polsce*, M. Federowicz, S. Ratajski (red.), Polski Komitet ds. UNESCO–KRRiT, Warszawa 2015; O. Wasiuta, S. Wasiuta, *Medialna manipulacja informacją w wojnie hybrydowej Rosji przeciwko Ukrainie*, [w:] *Medialne obrazy świata*, R. Klepka (red.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego im. KEN, Kraków 2018.

BEZPIECZEŃSTWO TELEINFORMATYCZNE/TELEINFORMACYJNE to pojęcie węższe znaczeniowo od terminu →bezpieczeństwo informacyjne, używanego na określenie sposobu pozyskiwania dobrej jakości →informacji oraz metod ochrony przed jej utratą. Bezpieczeństwo informacyjne w praktyce jest utożsamiane przede wszystkim z podmiotem zagrożonym brakiem dostępu do informacji lub ewentualną utratą określonych zasobów informacyjnych. W sensie negatywnym ma więc również na celu zagwarantowanie poufności, integralności i powszechnej dostępności informacji poprzez wykluczenie ewentualnych zagrożeń. Należy zauważyć, że zapewnienie bezpieczeństwa państwa we współczesnym świecie jest uwarunkowane właściwym poziomem

bezpieczeństwa informacyjnego, gdyż najistotniejsze obszary funkcjonowania kraju (m.in. siły zbrojne, energetyka, ekonomia, media, systemy transportowe, finansowe, a także obszar ochrony zdrowia) są zależne od sprawnych i efektywnych systemów informatycznych. Bezpieczeństwo informacyjne rozumiane w kategoriach wyłącznie negatywnych zatem staje się niewystarczające i wymaga podejścia z uwzględnieniem aspektu pozytywnego, a więc odwołania się w definicji do implementacji takiej polityki bezpieczeństwa, której wytyczne zagwarantują ochronę funkcjonujących w państwie systemów z jednoczesnym umożliwieniem dalszego swobodnego rozwoju wszystkich podmiotów → społeczeństwa informacyjnego [t. 2].

Przy omawianiu zagadnienia bezpieczeństwa informacyjnego kluczowe jest zrozumienie określonych prawidłowości. Po pierwsze, nie jest możliwa polemika na temat bezpieczeństwa teleinformatycznego/teleinformacyjnego bez odwołania się do bezpieczeństwa informacyjnego – jest to niezgodne chociażby ze standardami określonymi normą ISO/IEC 17799 (systemowe podejście do bezpieczeństwa informacji). Po drugie, informacja jest traktowana w kategoriach zasobu strategicznego współczesnych podmiotów, stając się jednocześnie istotnym czynnikiem produkcyjnym. Po trzecie, sektor informacyjny jest w XXI w. głównym obszarem pozyskiwania większości dochodów współczesnych państw. Po czwarte, wszelkie systemy informacyjne związane z pozyskiwaniem i przetwarzaniem informacji będą implikować procesy decyzyjne w pozostałych sektorach funkcjonowania państwa i społeczeństwa. Po piąte, dezorganizacja systemów informacyjnych nie jest kosztowna, a rozgrywki pomiędzy przeciwnikami mogą przybrać formę → walki informacyjnej [t. 2].

Jak już wspomniano, w zakres bezpieczeństwa informacyjnego wchodzi bezpieczeństwo teleinformatyczne/teleinformacyjne, odnoszące się do zakresu form wymiany informacji z wykorzystaniem konkretnych technicznych środków łączności, takich jak telefony komórkowe i stacjonarne, radiostacje, sieci komputerowe, telefaksy, wideotelefony, sieci i systemy teleinformatyczne itp. Bezpieczeństwo teleinformatyczne/teleinformacyjne jest rozumiane także w kategoriach uzasadnionego poziomu zaufania, że podmiot nie poniesie strat wynikających z niepożądanego ujawnienia, zmiany bądź zniszczenia informacji. Rozpatrywane w aspekcie

organizacyjnym, technicznym oraz prawnym, stanowi poniekąd syntezę aktywności interdyscyplinarnego zespołu ekspertów. Nie może więc być utożsamiane z jednorazowym procesem zmierzającym do implementacji konkretnych zabezpieczeń, jest to bowiem proces dynamiczny, wielokierunkowy i skomplikowany, który należy permanentnie kontrolować i dostosowywać do zmieniającej się rzeczywistości.

Bezpieczeństwo teleinformatyczne/teleinformacyjne wiąże się z ochroną informacji na etapie jej przetwarzania, przechowywania i przekazywania przez systemy teleinformatyczne. Celem tak rozumianej ochrony jest zabezpieczenie jej (nie komputerów) przed jej potencjalnym ujawnieniem (zwłaszcza danych poufnych), modyfikacją, utratą lub destrukcją. Informacja wymaga ochrony, ponieważ może mieć znaczenie strategiczne dla konkretnych podmiotów, stanowiąc podstawowy element procesów gospodarczych, politycznych, militarnych i społecznych. Ponadto ochronę informacji wymuszają obowiązujące regulacje prawne. Zgodnie z §5.1 Rozporządzenia Prezesa Rady Ministrów z 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym zapewnia się poprzez implementację spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych informacji. Usługi świadczone w zakresie bezpieczeństwa teleinformatycznego obejmują zarówno telekomunikację, jak i informatykę, a polegają w głównej mierze na ocenie i kontroli ryzyka podejmowanego w związku z korzystaniem z komputerów, sieci komputerowych oraz przesyłaniem danych do zdalnych lokalizacji. Pomimo podejmowanych wysiłków na rzecz udoskonalenia systemów teleinformatycznych oraz ze względu na wielowymiarowość wdrożonych rozwiązań istniejące luki w zabezpieczeniach w dalszym ciągu stanowią poważny problem dla wszystkich użytkowników sieci teleinformatycznych. Konstruowanie bezpiecznych, a zarazem efektywnych systemów teleinformatycznych i aplikacji stało się kluczowe dla funkcjonowania współczesnej gospodarki, biznesu i armii oraz dla właściwej realizacji ustawowych zadań jednostek administracji publicznej. Liczne próby usprawnienia systemów teleinformatycznych przyczyniły się do wypracowania określonych metod oceny bezpieczeństwa i analizy potencjalnych zagrożeń. Niestety, wdrożenie

w pełni bezpiecznego systemu nie jest możliwe z uwagi nie tylko na ryzyko wystąpienia standardowych usterek i błędów, ale także na dylemat określenia i spełnienia niekiedy sprzecznych oczekiwań podmiotów systemów teleinformatycznych. Warto zdać sobie sprawę, że walka o zapewnienie bezpieczeństwa teleinformacyjnego/teleinformatycznego może generować kolejne zagrożenia dla współczesnej cywilizacji.

Julia Anna Gawęcka

J.A. Grochocka, *Oblicza wojny hybrydowej na terytorium Ukrainy – stanowisko Federacji Rosyjskiej, Sojuszu Północnoatlantyckiego i Unii Europejskiej*, [w:] *Wojna hybrydowa na Ukrainie. Wnioski i rekomendacje dla Europy i świata*, B. Pacek, J.A. Grochocka (red.), Wydawnictwo Uniwersytetu Jana Kochanowskiego w Kielcach, Filia w Piotrkowie Trybunalskim, Piotrków Trybunalski 2017; J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2013; Metodyka – Standard ISO/IEC 17799; L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Wydawnictwo Difin, Warszawa 2012; K. Liderman, *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" 2002, nr 17; K. Liedel, *Bezpieczeństwo informacyjne jako element bezpieczeństwa narodowego*, 27.11.2008, Liedel.pl (dostęp 12.04.2019); Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz.U. z 2011 r. nr 159 poz. 948.

BEZPIECZEŃSTWO W KAMPANIACH WYBORCZYCH W INTERNECIE – ogół problemów i zagadnień odnoszących się do problematyki bezpieczeństwa, które podejmowane są w toku prezentowanych w internecie kampanii poprzedzającej wybory parlamentarne, prezydenckie, samorządowe lub europejskie. Podejmowanie zagadnień dotyczących bezpieczeństwa w kampaniach wyborczych wynika z tego, że jest to grupa problemów znajdująca się na ogół w centrum zainteresowania potencjalnych wyborców, ponadto większość podmiotów uczestniczących w wyborach ma swoje stanowisko w odniesieniu do najistotniejszych kierunków działań odnoszących się do bezpieczeństwa. Kampania wyborcza z uwagi na skalę medialnego nagłośnienia ma też wpływ na kształtowanie się →opinii publicznej [t. 2], stanowiąc przyczynek do licznych debat i dyskusji.