VADEMECUM
BEZPIECZEŃSTWA INFORMACYJNEGO

TOM 2

Instytut Nauk o Bezpieczeństwie
Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej
w Krakowie 2019

VADEMECUM
BEZPIECZEŃSTWA INFORMACYJNEGO

TOM 2

N–Z

REDAKCJA NAUKOWA
OLGA WASIUTA, RAFAŁ KLEPKA

ISBN 978-83-66445-09-3
ISBN 978-83-66269-26-2

Recenzenci:
prof. dr hab. inż. Włodzimierz Gogołek
dr hab. Mirosław Lakomy, prof. AIK

Redakcja:
Agnieszka Gruszka

Korekta:
Joanna Kłos

Skład:
LIBRON

Projekt okładki:
Justyna Rokitowska

Źródło grafiki wykorzystanej na okładce:
https://pixabay.com/pl/photos/haker-silhouette-sieka%C4%87-anonimowy-3342696/

Publikacja sfinansowana przez Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej

Wydawcy:

AT Wydawnictwo
ul Zachodnia 9/49
30-350 Kraków
tel.: 504 799 323
e-mail: wydawnictwoat@atgroup.pl
www.atwydawnictwo.pl

Wydawnictwo LIBRON – Filip Lohner
al. Daszyńskiego 21/13
31-537 Kraków
tel. 12 628 05 12
e-mail: office@libron.pl
www.libron.pl

Civili 7" 2018, nr 257; A. Śmigielska, *Technologie informacyjne i komunikacyjne w pracy nauczyciela*, Mikom, Warszawa 2002; K. Warzecha, *Stan posiadania i wykorzystywanie nowoczesnych środków komunikacji przez śląską młodzież oraz ryzyko uzależnienia od nich*, „Nierówności Społeczne a Wzrost Gospodarczy" 2015, nr 44 (4), cz. 2.

ZAKŁÓCENIA INFORMACYJNE są to wszelkie odchylenia od normy, trudności w działaniu oraz krzyżowanie planów przeciwnika, które prowadzą do pojawienia się nieprawidłowości, zmniejszenia wydajności operacyjnej, a także do całkowitego zniszczenia infrastruktury przesyłającej →informacje [t. 1]. Zakłócenia informacyjne są elementem →walki informacyjnej, a dokładniej: aktywna i szeroka odpowiednia działalność sił zbrojnych, →służb specjalnych, mediów, polityków, dyplomacji, partii, organizacji czy podmiotów międzynarodowych oraz organizacji przestępczych i terrorystycznych, która ma na celu zdezorganizowanie działań przeciwnika. W walce informacyjnej zakłóceniu podlegają wszelkie procesy informacyjno-decyzyjne, a także te, które dotyczą systemu dowodzenia w państwie. Do zakłóceń informacyjnych wykorzystuje się dyplomację oraz działania polityczne wpływające na monitorowanie otoczenia przeciwnika, a więc zarówno wewnętrzne, jak i zewnętrzne działania odpowiednich służb, a przy tym zdobywanie i filtrowanie informacji oraz ich przetwarzanie mogące posłużyć do poznania przeciwnika. Zdobyta wiedza jest elementem planowania, organizowania oraz prowadzenia zakłócania informacyjnego. Uporządkowane wiadomości na temat działań przeciwnika pozwalają na wprowadzanie szumów oraz luk informacyjnych. Za zakłócenia informacyjne zwykle są odpowiedzialne jednostki, które mogą mieć dostęp do informacji niejawnych oraz mogą prowadzić działania w kraju i poza jego granicami, np. służby specjalne, Policja, Żandarmeria Wojskowa czy Straż Graniczna. Monitorowanie działalności przeciwnika oraz określanie zdobytych wiadomości jest elementem trwającym przez dłuższy czas i może być realizowane w czasie kryzysu, pokoju czy wojny. W kontekście walki informacyjnej zakłócanie informacyjne jest nakierowane na wprowadzanie dezinformacji, propagandę, manipulację i działalność niszczącą infrastrukturę informacyjną przeciwnika.

W wyniku zakłóceń informacyjnych pojawiają się:

- szumy informacyjne, które są wynikiem nierówności, jaka zachodzi pomiędzy nadmiarem a możliwościami przetwarzania informacji u użytkowników. Dochodzi również do zjawiska niemożności odczytania informacji prawdziwych i najbardziej istotnych. Cechy szumu informacyjnego to niespójność elementów, niska ich jakość, fragmentaryczność oraz nieaktualność;
- luki informacyjne, czyli różnica pomiędzy ilością dostępnych informacji w systemach komunikacyjnych a popytem na nie wśród użytkowników. Dodatkowo jest to również rozbieżność pomiędzy otrzymywanymi informacjami a tymi, które użytkownik powinien otrzymać. Luką informacyjną jest również niedobór informacji niezbędnych do podjęcia decyzji w określonym czasie;
- szeroka manipulacja informacjami: wiadomości są zmyślane, zatajane, przekręcane, przeinaczane i pozorowane w celu osiągnięcia korzyści przez przeciwnika, np. przekazywanie fałszywych, zniekształconych lub niemożliwych do zweryfikowania informacji; blokowanie i opóźnianie przekazu informacji; prowokacje; ośmieszanie osób, zjawisk i sytuacji; wzbudzanie poczucia lęku.

Dostęp do informacji, które mają odpowiednią wartość w walce informacyjnej, i zostaną pozyskane we właściwym czasie, może być skutecznie zakłócany przez jednostki oraz wpływać na podejmowanie decyzji.

Justyna Rokitowska

T.R. Aleksandrowicz, *Podstawy walki informacyjnej*, Wydawnictwo Editions Spotkania, Warszawa 2016; W. Babik, *Zarządzanie informacją we współczesnych systemach informacyjno-wyszukiwawczych – nowe wyzwanie współczesności*, „Zagadnienia Informacji Naukowej" 2000, nr 1 (75); H. Batorowska, *Walka informacyjna*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; H. Batorowska, R. Klepka, O. Wasiuta, *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem*, Wydawnictwo Libron, Kraków 2019; *Encyklopedia Zarządzania*, hasło: *Luka informacyjna,* https://mfiles.pl/pl/index.php/Luka_informacyjna (dostęp 22.05.2019); J. Janczak, *Zakłócanie informacyjne*, Wydawnictwo AON, Warszawa 2001; P. Motylińska, *Manipulacja informacją*, [w:] *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018; A. Żebrowski, *Agentura*

wpływu uczestnikiem walki informacyjnej, „Acta Universitatis Wratislaviensis – Studia nad Autorytaryzmem i Totalitaryzmem" 2018, nr 1 (40); tenże, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Uniwersytetu Pedagogicznego im. KEN w Krakowie, Kraków 2016.

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACYJNYM to zespół działań uwzględniających planowanie, organizowanie i kontrolowanie →procesów informacyjnych (takich jak m.in. tworzenie, gromadzenie, przechowywanie, transmisja, transformacja, udostępnianie, interpretacja i wykorzystywanie →informacji [t. 1]). Zarządzanie →bezpieczeństwem informacyjnym [t. 1] ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa (tzn. odpowiedniego, ustalonego poziomu kluczowych atrybutów bezpieczeństwa: poufności, integralności, dostępności, oraz innych: rozliczalności, autentyczności i niezawodności) procesów informacyjnych, systemów informacyjnych i samej informacji. W procesach zarządzania bezpieczeństwem informacyjnym uwzględnia się wszystkie elementy systemu informacji (czyli użytkowników systemu – nadawców i odbiorców informacji, źródła informacji, samą informację, kanały przekazu informacji, otoczenie procesów informacyjnych, sprzęt, narzędzia i sieć teleinformatyczną).

Szerokie ujęcie zarządzania bezpieczeństwem informacyjnym pozwala na uwzględnienie w nim, oprócz tworzenia i utrzymania systemów zarządzania bezpieczeństwem informacji (SZBI) w organizacji, także zarządzanie zachowaniami i postawami ludzi w świecie informacji (np. w internecie, zob. →bezpieczeństwo w sieci [t. 1]). W literaturze przedmiotu zarządzanie bezpieczeństwem informacyjnym najczęściej jednak jest charakteryzowane w ujęciu węższym: jako zarządzanie bezpieczeństwem informacji, które odnosi się bezpośrednio do funkcjonowania i zadań organizacji. Podstawy tworzenia systemu zarządzania bezpieczeństwem informacji w organizacji określono m.in. w serii norm ISO/IEC 27000, np. w normach *PN-EN ISO/IEC 27001:2017-06 – wersja polska, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, *PN-EN ISO/IEC 27002:2017-06 – wersja polska, Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji* lub *PN-ISO/IEC 27006:2016-12 – wersja*