

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

© Copyright by Authors
Kraków 2019

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

OBRONA INFORMACYJNA – według definicji R. Szpyry jest to „zapobieganie, rozpoznanie i niedopuszczenie do ataku informacyjnego lub uzyskanie pożądanego jego efektywności”. Jest to również ochrona zasobów informacyjnych wykorzystywanych w działaniach operacyjnych. Obrona informacyjna jest elementem militarnej → walki informacyjnej, która może przybrać formę ochrony informacyjnej, w której działania polegają na: → kontrowiadzie [t. 1], zabezpieczeniu technicznym infrastruktury informatycznej, ochronie informatycznej, rozbudowie inżynieryjnej wyprzedzającej działania przeciwnika, ochronie psychologicznej czy kontrdezinformacji. Dodatkowo jednostki mogą przeciwdziałać zagrożeniom poprzez aktywność rozpoznawczą, zwykle polegającą na odstraszeniu czy obezwładnianiu przeciwnika. Obrona informacyjna jest zbiorem wszelkich działań, metod i procedur, które są podejmowane przez uprawnione do tego podmioty, aby zabezpieczyć → informacje [t. 1] przed niepożądanym ujawnieniem lub modyfikacją czy też zniszczeniem.

Elementem obrony infrastruktury w walce informacyjnej jest realizacja operacji defensywnych, które obejmują osłonę → środowiska informacyjnego (np. źródeł informacji). Techniki agresji stosowane przez przeciwników są szerokie, nie ma jednej uniwersalnej propozycji działania w celu ochrony informacji, które mogą pozyskać agresorzy.

Najważniejsze są wiedza i przekonanie, że można zostać zaatakowanym. Istotnym elementem ochronnym jest również umiejętność wyposażenia kraju w jednostki, które mogą zapewnić ochronę obywatelom i całemu państwu przed agresją. W przypadku pojawienia się przesłanek ataku należy przede wszystkim: pozyskać wiedzę o potencjalnym źródle agresji oraz jego działaniach; korzystać z wszelkich możliwych źródeł, aby móc wykryć fałsz, manipulację i dezinformację płynącą ze strony przeciwnika; zachować czujność, aby być przygotowanym na techniki i metody oraz rozwiązania kierowane ze strony przeciwnika w słabe i mocne strony atakowanego; unikać przekonania, że agresor może wykorzystywać identyczne metody – w tym przypadku należy zakładać, że przeciwnik może się wykazać większą inteligencją oraz przebiegłością.

Ochrona informacji w codziennym funkcjonowaniu państwa jest jednym z najważniejszych elementów systemu bezpieczeństwa, dlatego w ramach postawionych celów dotyczących również informacji niejawnych, zgodnie ze Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, przyjęto strategiczne zadania w tym zakresie, które obejmują: „zapewnienie państwa poprzez zapobieganie uzyskaniu nieuprawnionego dostępu do informacji niejawnych i ich ujawnieniu; zapewnianie personalnego, technicznego i fizycznego; akredytację systemów teleinformatycznych służących przetwarzaniu tych informacji; zapewnienie realizacji funkcji krajowej władzy bezpieczeństwa w celu umożliwienia międzynarodowej wymiany informacji niejawnych”.

Obrona informacyjna jest jednym z ważnych elementów w walce informacyjnej zarówno w przypadku pozyskiwania informacji, jak i ich zakłócania. Niedoprecyzowanie technik i metod w pozyskiwaniu informacji przeciwnika, a także niewłaściwie prowadzona obrona informacyjna własnych zasobów może skutkować przejęciem informacji przez agresora, co może doprowadzić do przegranej na polu walki informacyjnej. Celem strategicznym obrony jest uzyskanie przewagi nad przeciwnikiem. Pozwala to na podejmowanie odpowiednich decyzji i wdrażanie działań w walce informacyjnej.

Justyna Rokitowska

W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (red.), Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016; R. Szypra, *Militarne operacje informacyjne*, Akademia Obrony Narodowej, Warszawa 2003; A. Żebrowski, *Determinanty walki informacyjnej*, [w:] *Walka informacyjna: uwarunkowania, incydenty, wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Kraków 2017; tenże, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Uniwersytet Pedagogiczny w Krakowie, Kraków 2016; tenże, M. Żmigrodzka, *Media uczestnikami walki informacyjnej*, „Doctrina. Studia społeczno-polityczne” 2012, nr 9; Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014, https://www.bbn.gov.pl/ftp/dok/01/sbn_rp_2014.pdf (dostęp 23.05.2019).

OCHRONA WŁASNOŚCI INTELEKTUALNEJ W SIECI – zespół uregulowań prawnych i czynności zmierzających do zabezpieczenia interesów podmiotów prawa własności intelektualnej (autora utworu, twórcy, współtwórcy dzieła) przed zaborem, kradzieżą, przywłaszczeniem lub bezprawnym wykorzystaniem wytworów ludzkiego intelektu w wirtualnej przestrzeni przez osoby do tego nieupoważnione. Ochrona ta obejmuje niektóre dobra materialne, które są efektem pracy twórczej. Prawo własności intelektualnej dzieli się na prawo autorskie i prawa pokrewne (prawo własności artystycznej, literackiej, naukowej) oraz prawo własności przemysłowej (m.in. wynalazki, wzory użytkowe, znaki towarowe), jednak z punktu widzenia charakteru opracowania oraz stosunkowo częstego łamania praw autorskich w internecie, przez własność intelektualną należy tu rozumieć zwłaszcza pierwszą z wymienionych kategorii (węższe znaczenie własności intelektualnej).

Zagwarantowana prawnie ochrona dzieł o charakterze własności intelektualnej obejmuje utwory artystyczne, literackie i naukowe już od momentu nabycia prawa autorskiego, czyli od chwili wykonania takiego dzieła. Takie dzieło musi być podane do powszechnej wiadomości (rozpowszechnione), oznaczone imieniem i nazwiskiem jego autora oraz datą jego powstania (ukazania się). Prawa autorskie chronione są do 70 lat po śmierci autora, a po upływie tego czasu przechodzą na jego spadkobierców. Jak podkreśla E. Tytyk, prace dyplomowe oraz naukowe (licencjackie, inżynierskie, magisterskie, doktorskie, habilitacyjne, profesorskie) są objęte