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

M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Wolters Kluwer, Warszawa 2014; R. Faligot, R. Kauffer, *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie*, Iskry, Warszawa 2006; M. Herman, *Potęga wywiadu*, Dom Wydawniczy Bellona, Warszawa 2002; J. Hughes-Wilson, *Największe błędy wywiadów świata*, Dom Wydawniczy Bellona, Warszawa 2002; P. Swoboda, *Co w tych służbach jest specjalne? Problemy związane ze stosowaniem pojęcia „służby specjalne" w Polsce po 1989 r.*, „e-Studia nad Bezpieczeństwem i Terroryzmem" 2014, nr 1; tenże, *Służby specjalne w Polsce po 1989 roku – problemy definicyjne*, [w:] *Niepodległa Polska: bezpieczeństwo i polityka w latach 1918–2018*, P. Łubiński (red.), Uniwersytet Katolicki KUL, Kraków 2018; tenże, *Wywiad i kontrwywiad w Polsce w procesie przemian systemowych (1989–2007)*, Avalon, Kraków 2016; S. Zalewski, *Służby specjalne w państwie demokratycznym*, Akademia Obrony Narodowej, Warszawa 2005; A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003)*, Oficyna Wydawnicza Abrys, Kraków 2005; tenże, *Wywiad i kontrwywiad w XXI wieku*, Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji, Lublin 2010.

SOCIAL MEDIA INTELLIGENCE (SOCMINT) – wykorzystanie technik w celu pozyskiwania →informacji [t. 1] z →mediów społecznościowych [t. 1]. SOCMINT, czyli inteligencja mediów społecznościowych, odnosi się do zbiorowych narzędzi i rozwiązań, które pozwalają odpowiednim instytucjom monitorować kanały społecznościowe i rozmowy, reagować na sygnały społeczne i syntetyzować dane w sensowne trendy i analizy oparte na potrzebach użytkownika. Media społecznościowe umożliwiają gromadzenie danych wywiadowczych z serwisów społecznościowych przy użyciu zarówno natrętnych, jak i nieinwazyjnych środków, z otwartych i zamkniętych sieci społecznościowych. Ten typ gromadzenia danych wywiadowczych jest jednym z elementów OSINT (Open Source Intelligence) – otwartego oprogramowania wywiadowczego, które obejmuje gromadzenie i pozyskiwanie informacji z otwartych źródeł, przy zachowaniu prawa do prywatności, zdefiniowane jako „informacje publicznie dostępne i mogące być zgodnie z prawem uzyskane przez prośbę, zakup lub obserwację". SOCMINT definiowana jest nie przez otwartość informacji, na których jest oparta, ale przez swoje istnienie na platformie mediów społecznościowych jako otwarta lub zamknięta inteligencja. Istotą jej działania jest zaplanowane i zorganizowane pozyskanie,

przetworzenie oraz dystrybucja zgromadzonych wiadomości dla określonej grupy odbiorczej, która wcześniej sprecyzowała zainteresowanie danym zakresem informacji (zwykle na potrzeby podjęcia decyzji lub rozwiązania problemu). SOCMINT, wykorzystując podobne mechanizmy do OSINT, skupia swoją uwagę wyłącznie na informacjach (zwykle prywatnych, udostępnionych przez samego użytkownika) w mediach społecznościowych (→ Facebook [t. 1], → Twitter, → Instagram [t. 1]). Przy czym należy pamiętać, że nie wszystkie dane w mediach społecznościowych są udostępnione publicznie.

Termin został po raz pierwszy użyty przez D. Omanda, J. Bartletta i C. Millera w cyklu artykułów z 2012 r. napisanych dla londyńskiej organizacji non-profit Demos. Autorzy argumentowali, że media społecznościowe są obecnie ważną częścią pracy wywiadowczej i bezpieczeństwa, ale zanim będzie można je uznać za nową potężną formę inteligencji, konieczne jest wprowadzenie zmian technologicznych, analitycznych i regulacyjnych, w tym poprawek do brytyjskiej ustawy z 2000 r. o uprawnieniach dochodzeniowo-śledczych (Regulation of Investigatory Powers Act, RIPA). W dokumencie tym uregulowano uprawnienia organów publicznych do prowadzenia nadzoru, dochodzeń i dostępu do komunikacji elektronicznej danej osoby oraz przechwytywania informacji. Zostały one wprowadzone w celu uwzględnienia zmian technologicznych takich jak rozwój internetu i nowe możliwości szyfrowania.

SOCMINT jest zbudowana na narzędziach i rozwiązaniach do monitorowania mediów społecznościowych w celach wywiadowczych i bezpieczeństwa, ale także w dziedzinie reklamy i marketingu, co pokazuje niedawno opublikowane badanie „Rynek mediów masowych rządu USA". Zgodnie z analizą Burton-Taylor International Consulting wydatki na informacje wywiadowcze i rozwiązania programowe specjalistów ds. public relations zwiększyły się o 9,3% w 2017 r. (do 3,5 mld dol.). Wzrost ten jest napędzany przez coraz większe kwoty przeznaczane na śledzenie i analizowanie mediów społecznościowych.

Według raportu Market Research Media „Wymiar technologiczny i rynkowy operacji informacyjnych i działań wojennych (wpływy), szacunki rynkowe" wydatki na informacje wywiadowcze i rozwiązania programowe agencji rządowych przekroczą 2 mld dol. w 2020 r., a korporacyjni

specjaliści ds. public relations przeznaczą ok. 4 mld dol. na SOCMINT w 2020 r.

SOCMINT jest coraz ważniejszym komponentem cyfrowej inteligencji, która jest obecnie głównym źródłem informacji dla policji, struktur bezpieczeństwa i → w y w i a d u na temat tożsamości osób podejrzanych, ich lokalizacji i przepływu środków finansowych między nimi. Technika SOCMINT jest nadal silnie powiązana z OSINT i z innymi systemami wyszukiwania informacji, takimi jak TechINT, GeoINT, SIGINT, HumINT, MasINT, które są częścią cyklu gromadzenia danych wywiadowczych. Wzrasta wykorzystanie mediów społecznościowych do tych celów wraz z przykładami wykorzystania taktycznego, operacyjnego i strategicznego. Pojawiają się nowe metody i narzędzia, które można wykorzystać do gromadzenia i analizowania danych i informacji z mediów społecznościowych, powstają coraz to nowe programy do zbierania informacji oraz walki z → c y b e r p r z e s t ę p c z o ś c i ą [t. 1]. Geolokalizacja i sieci społecznościowe pozwalają wywiadowi nie tylko na określenie miejsca, z którego pochodzi obraz, ale również na buforowanie danych i rozpoznawanie twarzy.

Dzisiaj media społecznościowe to miejsce, w którym ludzie publikują niemal wszystko. Znacząco zwiększyła się możliwość przekazywania i przechwytywania informacji, czyniąc sieci społecznościowe nowym kanałem komunikacji dla przestępców i oszustów. W tysiącach serwisów społecznościowych istnieją miliardy profili. Codziennie aktualizuje się ok. 200 mln pozycji, ustawień kont na Facebooku, tworzą się kopie zapasowe danych etc. Obszary aplikacyjne SOCMINT są rozległe, służby wywiadowcze używają ich do analizowania i monitorowania szczególnych zagrożeń, takich jak terroryzm, co często sprawia, że firmy z obszaru social media są zobowiązane udostępniać wymagane informacje. Na poziomie lokalnym SOCMINT może być wykorzystywana do działań wywiadowczych i gromadzenia danych o osobach, firmach, organizacjach, ale także o wydarzeniach, pozycjonowania, analizy nastrojów i monitorowania społeczeństwa.

SOCMINT zapewnia głębokie zrozumienie przekazu społecznego, którego dane są gromadzone, segregowane, analizowane i przetwarzane w celu wytworzenia uporządkowanej informacji. Monitoring internetu i analiza danych ze źródeł otwartych stanowią istotną część działań

antyterrorystycznych o charakterze prewencyjnym. Bogactwo informacji i danych osobowych możliwych do uzyskania z mediów społecznościowych jest wykorzystywane nie tylko do zwalczania zagrożeń terrorystycznych, lecz także do walki z przestępczością.

Skuteczność technik SOCMINT wynika częściowo z tego, że użytkownicy mediów społecznościowych, publikując w sieci informacje o sobie (w celu szeroko pojętej samoekspresji, np. artystycznej czy towarzyskiej), jednocześnie przekazują wiele danych, których by nie przekazali zapytani o nie wprost (zwłaszcza przez służby państwowe).

W przeciwieństwie do forów tematycznych funkcjonujących w internecie od wielu lat media społecznościowe zostały zaprojektowane w taki sposób, aby pobudzać swobodną, publiczną ekspresję użytkowników, szczególnie w zakresie informacji dotyczących stylu życia, tj. zachęcać ich do dzielenia się własnymi przemyśleniami, planami, opiniami, zdjęciami i wydarzeniami ze swojego życia. Widoczna jest tendencja użytkowników mediów społecznościowych do tzw. naddzielenia się (ang. *over-sharing*) informacjami prywatnymi. Miewa to groźne konsekwencje, ponieważ zwiększa ryzyko stania się ofiarą różnego rodzaju działań przestępczych. Jednak dokładnie to samo zjawisko wpływa na dużą skuteczność technik SOCMINT, które są wykorzystywane do ochrony szeroko rozumianego bezpieczeństwa wewnętrznego. Media społecznościowe są więc źródłami danych, które mogą służyć pracy wywiadowczej. Ponad 81% funkcjonariuszy amerykańskich organów ścigania wykorzystuje tego typu źródła jako narzędzia pozyskiwania informacji na temat osób obecnych w prowadzonych przez siebie sprawach.

SOCMINT jest potencjalnie użyteczną i ważną częścią działań, których przedmiotem jest zwalczanie terroryzmu i podejmowanie wysiłku na rzecz bezpieczeństwa publicznego.. W USA znaczenie technik SOCMINT wzrasta, obejmując dane handlowe, zamówienia, opinie ekspertów oraz różnego rodzaju „szarą literaturę" publikowaną przez osoby prywatne, agencje rządowe i pracowników akademickich. Amerykański Komitet Bezpieczeństwa Wewnętrznego uważa, że SOCMINT powinna się stać narzędziem federalnym i być używana przez lokalne organy ścigania do opracowywania aktualnych, istotnych i możliwych do wykorzystania informacji wywiadowczych, zwłaszcza jako uzupełnienie danych niejawnych.

Niedawno w USA pojawiły się głosy wzywające do rozszerzenia i pogłębienia wykorzystania OSINT jako części szerszej reformy wywiadowczej, bezpieczeństwa narodowego i zarządzania.

Media społecznościowe są obecnie niewątpliwie wyposażone w duży zasób danych o instytucjach (reklamy, podaż i popyt na towary oraz usługi) oraz – przede wszystkim – osobach prywatnych, które wykorzystując platformy, udostępniają takie informacje o sobie, jak: sytuacja majątkowa, status związku, relacje z otoczeniem, poglądy polityczne czy orientacja seksualna. Informacje dostarczane social mediom pozwalają również określić sytuację i nastroje polityczne, przewidzieć wydarzenia, jakie mogą nastąpić na świecie w kontekście bezpieczeństwa, oraz przeanalizować, jak kształtują się trendy marketingowe czy biznesowe. W obszarze zainteresowania SOCMINT pozostają:

- ***Social mobile*** – dostęp do aplikacji mediów społecznościowych z poziomu smartfonów to swoista rewolucja, internet bezprzewodowy pozwala na bycie online praktycznie w każdym miejscu na świecie. Komunikacja poprzez social media może się odbywać bez przerwy, łatwy dostęp do połączeń internetowych (np. na terenie Unii Europejskiej) sprzyja wymianie informacji o miejscu pobytu, nastrojach czy relacjonowaniu wydarzeń na żywo (Facebook Live, Instagram Story). Istotnym wydarzeniem była integracja systemu iOS Apple z Twitterem, w wyniku której platforma ta odnotowała 300-procentowy wzrost liczby użytkowników.
- **Wyszukiwarki społecznościowe** – ich działanie opiera się na największej wyszukiwarce, tj. Google. Zastosowanie szczegółowego algorytmu pozwala na doskonałe pozycjonowanie stron internetowych, a także na wskazywanie w wynikach wyszukiwania tych stron i portali, które są polecane przez naszych sieciowych znajomych. Wystarczy, aby liczba kliknięć „Lubię to" w popularnych serwisach czy na kanałach społecznościowych uległa zwiększeniu.
- **Geotargetowanie** – pozostawianie w sieci śladów naszej aktywności, a w szczególności informacji o tym, gdzie się znajdujemy. Obserwowany w ostatnich latach wzrost zainteresowania geotargetowaniem jest niewątpliwie efektem rozpowszechnienia internetu mobilnego i zwiększenia się liczby smartfonów.

- ***E-commerce* w *social mediach*** – coraz więcej znanych marek oraz mniejszych firm sprzedaje swoje towary w social mediach, np. Facebook umożliwia swoim użytkownikom zakup najpopularniejszych rzeczy bez konieczności migracji na inne platformy sprzedażowe. Odpowiednie algorytmy śledzące użytkowników dopasowują produkty i marki, które będą im się wyświetlać jako pierwsze w powiadomieniach, np. przeglądając ofertę internetowego sklepu obuwniczego, użytkownik wysyła informacje do algorytmów, że jest zainteresowany kupnem obuwia, i w rezultacie po upływie chwili w social mediach wyświetlają mu się reklamy obuwia.
- ***Social gaming*** – umożliwia użytkownikom granie w gronie znajomych, co sprzyja również zakupom w sieci rozszerzonych wersji aplikacji. Dodatkowo wykorzystanie tej technologii jest jednym z elementów dzisiejszej edukacji, np. Quizlet – narzędzie e-learningowe do nauki języków poprzez samodzielne tworzenie fiszek (możliwości gry w gronie znajomych czy na zajęciach edukacyjnych).

Pamiętajmy, że logując się na różnych serwisach czy w aplikacjach, zostawiamy ślad, który może być wykorzystany do identyfikacji, nawiązania potencjalnego kontaktu oraz określenia naszych preferencji. Odpowiednio skonstruowany algorytm wykorzystujący udostępnione przez nas informacje może zabiegać o naszą uwagę w sieci. Przy klasyfikowaniu technik wykorzystywanych przez SOCMINT można wyróżnić kategorie celów:

- dostarczanie napływających od użytkowników social mediów informacji oraz ich uporządkowanie według określonych w badaniu parametrów, aby określić ogólny obraz sytuacji w czasie rzeczywistym (szczegółowe zbieranie danych jest dostosowane do tego, jakie informacje są obecnie poszukiwane);
- użyteczność informacji dla celów wywiadowczych i sklasyfikowania rodzajów zagrożeń jako szansa na poprawę bezpieczeństwa publicznego – media społecznościowe są coraz częściej wykorzystywane przez przestępców do koordynowania swoich działań.

Wykorzystanie odpowiednich algorytmów wiąże się z pozyskiwaniem szczegółowych danych. Zgodnie z możliwościami wyodrębnionymi dla SOCMINT dane są udostępniane za pomocą komercyjnych rozwiązań,

np. programów operacyjnych: IBM COBRA – analiza rynku, jego konkurencyjności oraz podaży i popytu na towar i usługi; Meltwater Buzz, Big Screen – monitorowanie trendów, marek oraz najpopularniejszych produktów i firm. Istnieją również niekomercyjne rozwiązania wykorzystujące dane w czasie rzeczywistym, np. Bitly, oraz przeznaczone np. do tworzenia profili poszczególnych użytkowników Twittera – Twitalyzer, czy ustalania statystyki liczby odwiedzin Facebooka: Facebook Audience Insights.

Narzędzia wykorzystywane przez → sztuczną inteligencję w social mediach (e-commerce również) pozwalają dopasować odpowiednie treści do użytkowników lub też dostarczyć producentom informacji o tworzących się nowych trendach, np. na podstawie częstości wyszukiwania treści poprzez: **rozpoznanie głosu** – aplikacja Siri w urządzeniach z systemem iOS pełni funkcję osobistego asystenta, który wykonuje wybrane zadania na podstawie poleceń głosowych właściciela smartfonu; **rozpoznawanie tekstu** – analiza danych ukazuje dominujące, aktualne trendy i umieszcza je na początku listy, treści są pozycjonowane od najbardziej pożądanych do najmniej; a także **rozpoznawanie obrazu** oraz **podejmowanie decyzji** – firma IBM zastosowała prototypowe rozwiązanie dla edukacji, wdrażając testowy program, na podstawie którego dokonywano syntezy informacji ze zwrotnym raportem dla uczniów (na podstawie ocen weryfikowano i dopasowywano ścieżki rozwoju dla każdego ucznia).

Oczekuje się, że wkrótce rozwój zdolności komunikacyjnych zmusi dostawców usług internetowych do przechowywania informacji o tym, kiedy, gdzie i przez kogo są wysyłane e-maile. Istotne jest, aby monitoring był oparty na legalnych podstawach, tak aby osoby, które w ustawieniach prywatności na swoich kontach w sieciach społecznościowych zaznaczyły, że nie chcą podlegać monitorowaniu, nie podlegały mu.

Monitorowanie mediów społecznościowych musi być oparte na odpowiednich przepisach prawnych, ale trzeba też pamiętać, że bez monitorowania i gromadzenia informacji z mediów społecznościowych, a więc bez technik SOCMINT, sieć może się zapełnić „tajnymi zaułkami", w których osoby prowadzące nielegalną działalność będą się swobodnie komunikować. Media społecznościowe powinny być monitorowane przez policję i służby bezpieczeństwa, stały się bowiem nową przestrzenią publiczną (a więc też miejscem popełniania przestępstw, np. przez pedofilów

czy terrorystów). Wykorzystanie technik SOCMINT na tym polu może mieć decydujący wpływ na bezpieczeństwo publiczne: wspierać zwalczanie działalności przestępczej, pomagać we wczesnym ostrzeganiu społeczeństwa o zagrożeniach lub budować świadomość sytuacyjną w szybko zmieniających się okolicznościach. Techniki SOCMINT są też ważnym elementem cyfrowego wywiadu, istotnym źródłem informacji nie tylko dla policji i wymiaru sprawiedliwości, ale także dla środowisk biznesowych czy osób fizycznych. Na podstawie przepływu informacji można uzyskać dane na temat tożsamości danego użytkownika, miejsca jego pobytu, relacji z różnymi środowiskami oraz potencjalnymi zamiarami (często przestępczymi). Informacje udostępniane w mediach społecznościowych są np. wykorzystywane przez funkcjonariuszy, którzy mając dostęp do wrażliwych danych osobistych weryfikują je pod kątem przyznawania wiz wjazdowych do krajów.

Techniki SOCMINT mają zarówno rzeszę sprzymierzeńców, jak i przeciwników. Przeciwnicy uważają, że technologie zastosowane w tym obszarze wykraczają poza ramy działalności OSINT, czyli gromadzenie danych ze źródeł publicznych, dostępnych dla wszystkich. Media społecznościowe niejednokrotnie udostępniają treści tylko tym członkom danej sieci, którzy zostali zaakceptowani przez użytkownika (dodani do kręgu jego znajomych). Dlatego organa ścigania zwykle pozyskują informacje z tzw. fake kont (kont fikcyjnych), do których założenia używa się fałszywych danych. Wiele osób traktuje to jako nadużycie i uznaje za nieuprawnione wnikanie w sprawy osobiste innych użytkowników sieci i zbyt daleko idącą inwigilację. Jednak służby, które stosują metody SOCMINT, odpierają te zarzuty, twierdząc, że ich działania opierają się przede wszystkim na wnikliwej analizie treści sieci, a zatem tych danych, które zostały udostępnione publicznie. Reasumując, jest to obszar pełen nieścisłości zarówno natury prawnej, jak i etycznej.

Zmieniające się trendy wyszukiwania informacji oraz ogrom danych udostępnianych przez użytkowników sprawiają, że istnieje konieczność konstruowania coraz to nowszych narzędzi do pozyskiwania danych z sieci społecznościowych. Podnoszenie kwalifikacji przez ekspertów zatrudnionych w laboratoriach informatyki śledczej oraz przedstawicieli → b i a ł e g o w y w i a d u [t. 1] jest kluczowym elementem, który wpływa na skuteczne

wykorzystanie technik SOCMINT w gromadzeniu danych i ich analizie, umożliwiając skuteczne rozpoznawanie zagrożeń.

Justyna Rokitowska, Olga Wasiuta

N. Antonius, L. Rich, *Discovering collection and analysis techniques for social media to improve public safety*, „The International Technology Management Review" 2013, no. 3.1; J. Bartlett, L. Reynolds, *The State of the Art 2015: a literature review of social media intelligence capabilities for counter-terrorism*, Demos, London 2015; J. Bartlett, C. Miller, *The state of the art: a literature review of social media intelligence capabilities for counter-terrorism,* November 2013; Published by Demos 2013, London, https://www.publicsafety.gc.ca/lbrr/archives/cn28613-eng.pdf (dostęp 19.05.2019); A. Burato, *SOCial Media INTelligence: un nuovo spazio per la raccolta di informazioni rilevanti*, „Sicurezza, Terrorismo e Societa. International Journal – Italian Team for Security, Terroristic Issues and Managing Emergencies" 2015, nr 1–2; K. Jarek, G. Mazurek, S. Hałas-Dej, *Marketing i sztuczna inteligencja*, „Przedsiębiorczość i Zarządzanie" 2018, t. XIX, z. 5, cz. II; P. Karasek, *Analiza informacji z mediów społecznościowych jako narzędzie wspierające kontrolę bezpieczeństwa w procedurach migracyjnych.* „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19 (10); M. Landon-Murray, *Social Media and US Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?*, „Journal of Strategic Security" 2015, no 8.3; I.A. Liviu i in., *Social media intelligence: opportunities and limitations*, „CES Working Papers" 2015, no. 7.2A; G. Małecki, *Współczesny OSINT i jego potencjał w dziedzinie kierowania państwem*, https://www.defence24.pl/wspolczesny-osint-i-jego-potencjal-w-dziedzinie-kierowania-panstwem (dostęp 14.04.2019); W.W. Moe, D.A. Schweidel, *Social Media Intelligence*, Cambridge University Press, Cambridge 2014, https://doi.org/10.1017/CBO9781139381338 (dostęp 15.04.2019); D. Omand, C. Bartlett, J. Miller, *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, no. 6; D. Omand, C. Miller, J. Bartlett, *Towards the discipline of social media intelligence*. *Open Source Intelligence in the Twenty-First Century*, Palgrave Macmillan, London 2014; M. Sadowski, *Rewolucja social media*, Helion, Gliwice 2013; *Salvum-Online, SOCMINT – Social Media Intelligence, czyli Inteligencja Mediów Społecznościowych*, https://salvum.online/informatyka-sledcza/socmint-social-media-intelligence-czyli-inteligencja-mediow-spolecznosciowych/ (dostęp 20.04.2019); B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*. Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Warszawa 2015; J. Surma, *Znaczenie analiz sieci społecznych online dla bezpieczeństwa narodowego,* „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 8, s. 92–101, http://cejsh.

icm.edu.pl/cejsh/element/bwmeta1.element.desklight-cfc304ec-540d-4edc-9db6-6513410874b9 (dostęp 14.04.2019); E. Şuşnea, A. Iftene, *The Significance of Online Monitoring Activities for the Social Media Intelligence (SOCMINT)*, „Conference on Mathematical Foundations of Informatics" 2018, https://www.researchgate.net/publication/330753592_The_Significance_of_Online_Monitoring_Activities_for_the_Social_Media_Intelligence_SOCMINT (dostęp 15.04.2019); D. Trottier, *Open source intelligence, social media and law enforcement: Visions, constraints and critiques*, „European Journal of Cultural Studies" 2015, no. 18.4–5.

SPIN DOCTORING (ang. *spin* – obracanie) jest procesem zarządzania →informacją [t. 1], prezentowania tej lub innej wiadomości pod odpowiednim kątem. Od lat 80. XX w. w krajach europejskich rośnie zainteresowanie nowym kierunkiem zarządzania polityką informacyjno-komunikacyjną dzięki wykorzystaniu technologii spin doctoringowej. Skierowanie uwagi technologów politycznych na spin doctoring wynika z następujących czynników: zwiększenia roli środków masowego przekazu we wszystkich dziedzinach życia publicznego; coraz większych możliwości manipulowania opinią publiczną za pomocą różnych kanałów komunikacji; zwracania uwagi →opinii publicznej na dane zagadnienie poprzez umiejętne zarządzanie przepływem informacji. W większości przypadków spin doctoring zajmuje się korygowaniem różnych zniekształceń obrazu określonego zdarzenia w mediach już po tym, jak wywołało ono negatywny efekt.

Określenie „spin doctoring" zaczęło być wykorzystywane przez technologów politycznych w latach 80. ubiegłego stulecia. Jego dokładne pochodzenie nie jest znane, ale często używali go eksperci w dziedzinie stosunków społecznych i przedstawiciele sił politycznych lub korporacyjnych, których praca polegała na prezentacji wydarzenia lub sytuacji z pozytywnej strony. Niektórzy specjaliści od PR używają terminu „spin doctoring", gdy mają na myśli oddzielną usługę, którą oferują, inni używają takich terminów jak „transformacja strategii" lub „transformacja obrazu". Czasami eksperci porównują koncepcję spin doctoringu z rebrandingiem, czyli transformacją wszystkich elementów marki w celu podniesienia jej pozycji na rynku. Firmy i organizacje polityczne potrzebują także politechnologów i specjalistów ds. spin doctoringu, aby „sprzedać" swoją misję i idee publiczności.