DOI:10.17951/we.2020.6.2.79-93 | Wschód Europy • Восток Европы • East of Europe vol 6, 2 / 2020

Anatoliy Kruglashov
Czerniowiecki Uniwersytet Narodowy im. Jurija Fedkowicza
ORCID ID: https://orcid.org/0000-0003-0611-2698

Sergii Shvydiuk
Czerniowiecki Uniwersytet Narodowy im. Jurija Fedkowicza
ORCID ID: https://orcid.org/0000-0003-2295-9960

Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory

1. Wprowadzenie

Wolne, cykliczne i powszechne wybory stanowią podwaliny demokracji. To właśnie podczas wyborów rozstrzyga się nowy porządek polityczny, lecz także pełne zastosowanie ma reguła *majority rule* („reguła większości") zarówno w kwestii wyboru konkretnych rządów, jak i reguł gry[1]. W świetle znanych teorii demokracji wybory odgrywają ważną rolę w realizowaniu zasad i wartości demokratycznych oraz pozwalają na zastosowanie m.in. zasady suwerenności narodu. W większości systemów politycznych synonimem demokracji stały się wolne wybory[2]. Z tego względu, rywalizując z demokratycznym Zachodem na arenie międzynarodowej, autorytarna Rosja dąży do osłabienia potencjału państw demokratycznych przez ingerencję w proces wyborczy. Ustępując państwom zachodnim względem potencjału ekonomicznego, Rosja w obliczu ukształtowanych symetryczno-asymetrycznych relacji z Zachodem poszukuje możliwości oddziaływania na inne państwa[3]. Wielowymiarowe działania hybrydowe (militarne, polityczne, ekonomiczne, informacyjne i in.) pozwalają Moskwie na skuteczne prowadzenie polityki międzynarodowej względem tzw. bliskiej i dalekiej zagranicy.

Federacja Rosyjska dąży do rewizji porządku światowego, ukształtowanego po II wojnie światowej. Powyższe działania Kreml rozpoczął długo przed 2014 rokiem,

[1] G. Sartori, *Teoria demokracji*, Wydawnictwo Naukowe PWN, Warszawa 1994, s. 175.
[2] W. Sokół, *Geneza i ewolucja systemów wyborczych w państwach Europy Środkowej i Wschodniej*, Wydawnictwo UMCS, Lublin 2007, s. 19–20.
[3] Зоb. Г. Перепелиця і ін., *Асиметрія міжнародних відносин*, Вид. дім Стилос, Київ 2005.

kiedy to dokonano aneksji Krymu oraz inwazji we wschodniej Ukrainie. Starania Władimira Putina o przywrócenie Rosji statusu najpierw lidera regionalnego w Eurazji, a następnie mocarstwa w skali globalnej sprzyjały polityce rewizjonistycznej. Momentem przełomowym było wystąpienie prezydenta Rosji podczas monachijskiej Konferencji Bezpieczeństwa w 2007 roku, w trakcie którego Władimir Putin werbalnie zaatakował USA i UE. Prezydent Rosji kategorycznie odrzucił możliwość zbliżenia Ukrainy z NATO[4], a ponadto publicznie nakreślił czerwone linie, markujące obszar rosyjskich interesów w Europie, który Rosja gotowa będzie bronić przy pomocy wszelkich możliwych środków. Wystąpienie Putina pozostało wówczas bez należytej odpowiedzi ze strony przywódców państw zachodnich, co zostało odczytane na Kremlu jako przyzwolenie do działania.

Już w sierpniu 2008 roku Rosja dokonała inwazji na Gruzję. Reakcja UE była opieszała i tylko odpowiedź Stanów Zjednoczonych Ameryki na rosyjską agresję była bardziej stanowcza. Zachód nie był przygotowany do odpowiednej reakcji na coraz bardziej agresywną politykę Federacji Rosyjskiej. Kreml odebrał powyższe podejście Zachodu jako przyzwolenie do działania oraz uwierzył w możliwość szybkiego powrotu na arenę międzynarodową w charakterze centrum polityki światowej. Dążąc do odbudowy swojej strefy wpływów na obszarze poradzieckim, Rosja nie zaproponowała konstruktywnego planu integracji w wymiarach gospodarczym, technologicznym, bezpieczeństwa i innym, lecz przeszła od kuszących obietnic do twardej polityki ograniczania suwerenności państw poradzieckich[5].

Powyższe działania zaczęły niszczyć ustalone zasady polityki międzynarodowej oraz demontować system gwarancji bezpieczeństwa. Podstawowym założeniem takiej polityki Kremla była rezygnacja Rosji z przyjętych i zaakceptowanych przez społeczność międzynarodową zasad, zamiast tego podejmowano próby narzucania własnych reguł gry. W tym celu wykorzystano cały arsenał środków – od szantażu energetycznego i propagandy do użycia siły militarnej wobec innych państw.

Aneksja Krymu oraz początki rosyjskiej agresji na Donbasie zapoczątkowały szerokie wykorzystanie w dyskursie publicystycznym i naukowym pojęcia „wojna hybrydowa". W literaturze naukowej powyższa kategoria jest żywo omawiana ze względu na jej znaczenie dla bezpieczeństwa międzynarodowego. Wojna hybrydowa różni się od wojny klasycznej tym, że dla osiągnięcia przewagi nad przeciwnikiem jest wykorzystywana nie tylko siła militarna, ale także metody walki informacyjnej, propaganda, działania wywrotowe i inne. Ponadto podejmowane są próby destrukcyjnego wpływu na opinię publiczną, wspierania antysystemowych sił politycznych i radykalnych ruchów społecznych, ingerowania w systemy informatyczne organów władzy państwowej oraz firm prywatnych. Ponadto są podejmowane także możliwości wywierania wpływu przy

[4] *Выступление и дискуссия на Мюнхенской конференции по вопросам политики безопасности. 10 февраля 2007 года*, http://kremlin.ru/events/president/transcripts/24034, inf. 23 X 2019.

[5] І. Мельничук, *Інтеграційні проекти Російської Федерації на пострадянському просторі*, Чернівці 2015, s. 400.

pomocy organizacji międzynarodowych oraz za pośrednictwem mediów społecznościowych. Podejmując tego typu działania, Rosja dąży do osłabienia i podziału struktur zachodnich (UE i NATO), uzyskując korzyści geopolityczne i ekonomiczne. Ponadto wśród ważnych celów można nadmienić zmianę prozachodnich rządów w państwach postradzieckich na prorosyjskie, stworzenie warunków do interwencji militarnej oraz aneksji cudzego terytorium[6] itp. Formy agresji hybrydowej ze strony Federacji Rosyjskiej mają na celu wewnętrzne osłabienie kraju przeciwnika, sprowokowanie kryzysów politycznych i społecznych, a także trwałych podziałów społeczeństwa. Ukraina jest dobrym przykładem prowadzenia przez Rosję wojny hybrydowej na wielu płaszczyznach (militarnej, politycznej, ekonomicznej, kulturowo-cywilizacyjnej).

Działania hybrydowe dotyczą przede wszystkim wewnętrznej przestrzeni państw demokratycznych: systemu politycznego, systemu informacyjnego i społeczeństwa obywatelskiego. Stosowane przez Rosję metody hybrydowe uderzają w instytucję, zasady i normy, wartości i procedury, obniżając witalność i skuteczność funkcjonowania państwa demokratycznego. W rywalizacji z państwami demokratycznymi Rosja wykorzystuje przeciwko nim podstawowe wolności – słowa, myśli, zrzeszania się i zgromadzeń – tworząc fake newsy, prowadząc propagandę i dezinformację, tworząc i wspierając organizację i grupy wywrotowe. W istocie autorytarna Rosja przy pomocy metod hybrydowych podejmuje działania zniszczenia demokracji od wewnątrz, uniemożliwienia jej prawidłowego funkcjonowania.

2. Wybrane przykłady ingerencji Rosji w wybory

Jak zostało podkreślone wyżej, jednym z priorytetowych kierunków oddziaływania Rosji na państwa demokratyczne jest ingerowanie w proces wyborczy, zapewniający w reżimach demokratycznych wyraz woli obywateli oraz legitymizację władzy, wymianę elit politycznych, a także wybór strategicznych kierunków rozwoju społeczeństwa i państwa. Dlatego korumpowanie przez Kreml polityków, dyskredytowanie procesu wyborczego w państwach demokratycznych jako wyrazu woli obywateli lub doprowadzanie do władzy polityków prorosyjskich wpisuje się w logikę rosyjskiej „wojny hybrydowej".

W praktyce systematyczna ingerencja Rosji w wybory w różnych państwach stała się realnym narzędziem Kremla do osiągania celów geopolitycznych. Jako przykład możemy podać ingerencję Rosji w przedterminowe wybory prezydenckie na Ukrainie w maju 2014 roku przy pomocy środków masowego przekazu. Pierwszy kanał rosyjskiej telewizji państwowej, prowadząc politykę manipulacji i dezinformacji, poinformował o zwycięstwie Dmytra Jarosza, ówczesnego lidera Prawego Sektora. Celowy zabieg rosyjskiej propagandy polegał na szerzeniu nieprawdziwych informacji o rzekomo znaczących wpływach ukraińskich nacjonalistów.

[6] Ch.S. Chivvis, *Understanding Russian "Hybrid Warfare" and What Can be Done About it*, Testimony presented before the House Armed Services Committee on March 22, 2017, p. 1, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf, inf. 15 IX 2019.

Rosyjskie media często wykorzystywały obraz Prawego Sektora do demonizowania wizerunku Ukrainy po rewolucji godności, pokazując zwycięstwo prawicowych radykalnych sił i strasząc odbiorców wewnętrznych i zagranicznych[7]. W rzeczywistości wspomniany powyżej kandydat zdobył mniej niż jeden procent głosów wyborców. Powyższa operacja informacyjna w rosyjskich mediach propagandowych została poprzedzona atakiem cybernetycznym na stronę internetową ukraińskiej Centralnej Komisji Wyborczej (CKW), powodując chwilową awarię sieci. I chociaż ataku z terytorium Ukrainy dokonała prorosyjska grupa CyberBerkut, to nie ma żadnych wątpliwości, kto stoi za jego przeprowadzeniem[8]. Skoordynowane działania rosyjskiej machiny propagandowej oraz hakerów pokazały sposoby i metody informacyjnego oddziaływania Rosji w ramach procesu wyborczego w innym państwie. Wniosek jest jednoznaczny, iż Rosja wykazywała szczególne zainteresowanie wywieraniem wpływu na proces wyborczy na Ukrainie w kontekście prowadzonej przez Kreml wojny hybrydowej.

Ukraina nie była jedynym państwem, w którym Rosja podejmowała próby ingerencji w proces wyborczy. Systematyczny charakter oraz globalna skala oddziaływania powodowały coraz większe zaniepokojenie i potrzebę rzetelnej analizy tego niebezpiecznego zjawiska celem opracowania środków przeciwdziałania zagrożeniom bezpieczeństwa państw demokratycznych. W związku z tym w listopadzie 2018 r. ogłoszono Raport Ogólny Komitetu Nauki i Technologii Zgromadzenia Parlamentarnego NATO *Rosyjska ingerencja w wybory i referenda w Sojuszu*[9]. Raport oparty na wielu źródłach podawał informację na temat ingerencji Rosji w proces wyborczy w pięciu państwach członkowskich NATO w okresie ostatnich kilku lat. Jako przykłady takiej ingerencji podano wybory prezydenckie w USA w 2016 roku, referendum w sprawie Brexitu w 2016 roku i wybory parlamentarne w 2017 roku w Wielkiej Brytanii, wybory prezydenta we Francji w 2017 roku, wybory parlamentarne w Niemczech w 2017 roku oraz referendum w sprawie statusu Katalonii w 2017 roku.

Podejmując ingerencję, Rosja wykorzystywała dość jednolity schemat działania: nieupoważniona ingerencja w systemy informatyczne i komputerowe partii politycznych i struktur rządowych; złamanie prywatnej i służbowej poczty elektronicznej, a także kradzież danych osobowych; skoordynowana „wrzutka" skradzionych informacji wraz z masowym rozpowszechnianiem ich w mediach społecznościowych za pomocą botów, trolli i innych środków.

[7] J. Świątkowska, *Działania prowadzone w cyberprzestrzeni jako metoda ingerencji w demokratyczny proces wyborczy*, [w:] *Walka informacyjna: uwarunkowania, incydenty, wyzwania*, red. H. Batorowska, Wydawnictwo UP, Kraków 2017, s. 258, http://hdl.handle.net/11716/2031, inf. 20 VII 2020.

[8] L. Galante, S. Ee, *Defining Russian Election Interference: an Analysis of Select 2–14 to 2018 Cyber Enabled Incidents,* Atlantic Council, Scowcroft Center for Strategy and Security, September 2018, p. 7.

[9] *Russian Meddling in Elections and Referenda in the Alliance*, General Report by Susan DAVIS (United States) General Rapporteur – 181 STC 18 E fin. 11 November 2018, https://www.nato-pa.int/sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf, inf. 19 VI 2020.

Zdaniem amerykańskiej polityk Susan Davis, Rosja ingerując w wybory innych państw, realizuje następujące cele:

– zaostrzenie już istniejących napięć społecznych w tych państwach,

– podważanie zaufania obywateli do liberalnych instytucji demokratycznych,

– promowanie osób i grup politycznych przyjaznych wobec rosyjskich wpływów oraz dyskredytowanie tych, których postrzega jako wrogo nastawionych,

– tworzenie atmosfery chaosu i niepewności w państwach zachodnich[10].

Skonkretyzowane cele rosyjskiej ingerencji różnią się w zależności od okoliczności i wzajemnie się nie wykluczają. Najczęściej ingerencja Rosji ma na celu uaktywnienie i wzmocnienie istniejących społecznych i politycznych napięć. Gdziekolwiek pojawiło się podejrzenie rosyjskiej ingerencji, hakerzy i trolle wykazywali się dość dobrą znajomością narodowej specyfiki podziałów i nastrojów społecznych. W Stanach Zjednoczonych Ameryki rosyjscy agenci publikowali płatne reklamy, wywołujące polityczne i religijne sprzeczności uderzające w społeczeństwo obywatelskie. W Niemczech rosyjskie botnety wykorzystywały problem uchodźców, próbując osłabić pozycję kanclerz Angeli Merkel oraz podważyć zaufanie do polityki niemieckiego rządu. W Hiszpanii rosyjskie media i botnety gorliwie wspierały zwolenników katalońskiego separatyzmu[11]. Ingerencja Rosji jest ukierunkowana na wykorzystanie problemów i podziałów wewnętrznych w państwach zachodnich celem osłabienia państw i struktur europejskich (UE) i euroatlantyckich (NATO).

Najbardziej znanym medialnie przypadkiem rosyjskiej ingerencji były wybory prezydenckie w USA w 2016 roku. W tym kontekście badacze i eksperci wyróżnili cztery główne obszary wpływu: kradzież informacji; selektywny przekaz informacji; stosowanie propagandowy i dezinformacji; wyprowadzenie z użytku systemu głosowania w całym kraju[12]. Wydarzeniom tym towarzyszyła skoordynowana stopniowo prowadzona kampania w mediach społecznościowych. Za pomocą ostatnich dokonywano kontrolowanego wycieku informacji, wrzucano fake newsy i prowadzono kampanię dezinformacyjną w celu delegitymizacji rządu USA.

W szczególności podczas kampanii wyborczej USA latem 2016 roku WikiLeaks opublikowało skradzione dokumenty elektroniczne Partii Demokratycznej. Założyciel WikiLeaks, Julian Assange, przyznał, że przez ten wyciek próbowano uniemożliwić Hillary Clinton wygranie wyborów prezydenckich[13]. Według amerykańskich służb wywiadowczych odpowiedzialnymi za cyberataki, w tym za te, które doprowadziły do kradzieży dokumentów Partii Demokratycznej, są dwie grupy hakerów związane z Rosją, mianowicie Fancy Bear i Cozy Bear.

[10] *Ibidem*, p. 2.

[11] *Ibidem*.

[12] J. Van De Velde, *The Law of Cyber Interference in Elections*, Available at SSRN 3043828 (May 15, 2017), p. 10, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828, inf. 15 VI 2020.

[13] C. Savage, *Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention*, "New York Times" 26.07.2016, https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html, inf. 15 VI 2020.

We wspólnym oświadczeniu Departamentu Bezpieczeństwa Wewnętrznego i Biura Dyrektora Wywiadu Narodowego ds. Bezpieczeństwa Wyborczego z 7 października 2016 roku stwierdzono, że „publikacje na stronach internetowych, takich jak DCLeaks.com i WikiLeaks, skradzionych e-mailów, a także działalność online Guccifer 2.0, są zgodne z metodami działań i motywacją Rosji. Kradzież i ujawnienie informacji mają na celu zakłócenie procesu wyborczego w USA”[14].

29 grudnia 2016 r. Departament Bezpieczeństwa Narodowego i Federalne Biuro Śledcze Stanów Zjednoczonych Ameryki wydały wspólną analizę szczegółów technicznych narzędzi wykorzystywanych przez rosyjskich cywilów i służby wywiadowcze dla cyberataków na urządzenia komputerowe i sieci instytucji wyborczych w Stanach Zjednoczonych Ameryki, a także rządu federalnego, instytucji politycznych i prywatnych[15].

Według amerykańskich organów ds. bezpieczeństwa cybernetycznego działania rosyjskich grup hakerskich były skierowane wobec rządu i obywateli USA, w tym agencji rządowych, obiektów infrastruktury krytycznej, think tanków, uniwersytetów, organizacji politycznych i korporacji w celu kradzieży informacji. Jednocześnie ataki hakerów były maskowane jako działalność osób trzecich, w tym z wykorzystaniem fałszywych postaci online, na przykład Guccifer 2.0, aby ukryć źródło ataku i zwiększyć wiarygodność w oczach odbiorców takich informacji[16].

Amerykański ekspert ds. bezpieczeństwa cybernetycznego Dave Aitel zauważył, że publikacja skradzionych plików przez rosyjskie służby specjalne w celu ingerencji z zewnątrz w wybory prezydenckie odpowiada definicji cyberwojny[17]. Według Michaela Jensena, działalność rosyjskich trolli została dobrze przemyślana nie tylko jako atak informacyjny na Stany Zjednoczone Ameryki, ale także jako kampania propagandowa przeciwko państwu amerykańskiemu. Analiza autora potwierdza powyższe przypuszczenia. Przebadano 20 348 tweetów utworzonych między 14 lipca 2014 r. a 26 września 2017 r., wskazując również, że 2752 profile na Twitterze są związane z działalnością rosyjskiej Agencji Badań Internetowych[18], znanej jako „fabryka trolli”.

Z kolei rosyjscy urzędnicy odrzucali wszelkie zarzuty dotyczące manipulacji i prób ingerowania w życie polityczne Stanów Zjednoczonych Ameryki. Jednak to nie przekonało Waszyngtonu i nie powstrzymało przed wprowadzeniem nowych antyrosyjskich

[14] *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, Release Date: October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, inf. 12 VI 2020.

[15] *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, December 29, 2016. Reference Number: JAR-16-20296A, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf, inf. 10 VI 2020.

[16] *Joint Statement from the Department*….

[17] D. Aitel, *Guest editorial: The DNC hack and dump is what cyberwar looks like*, “Ars Technica” 2016, no. 17, https://arstechnica.com/information-technology/2016/06/guest-editorial-the-dnc-hack-and-dump-is-what-cyberwar-looks-like/, inf. 10 VI 2020.

[18] M. Jensen, *Russian Trolls and Fake News: Information or Identity Logics?*, „Journal of International Affairs” 2018, vol. 71, no. 1.5, p. 118, www.jstor.org/stable/26508125, inf. 25 VI 2020.

sankcji związanych z ingerencją w kampanię prezydencką. Wówczas Stany Zjednoczone Ameryki odesłały z kraju 35 rosyjskich dyplomatów[19].

W wyniku dalszych badań na Facebooku znaleziono co najmniej 120 sfałszowanych rosyjskich kont rozsyłających wiadomości, obejmując swoim zasięgiem ponad 29 milionów obywateli amerykańskich. Dzięki powyższym kontom próbowano zorganizować 129 wydarzeń offline z udziałem 33 800 osób w Stanach Zjednoczonych Ameryki. Jednak brakuje informacji na temat tego, ile wydarzeń z zaplanowanych udało się zorganizować w rzeczywistości. Od stycznia 2018 r. na Twitterze znaleziono co najmniej 50 258 rosyjskich kont, zawierających informacje dotyczące wyborów w USA[20].

Problem rosyjskiej ingerencji w wybory prezydenckie w USA nie warto sprowadzać jedynie do tzw. pomocy obywatelom amerykańskim w rozwiązaniu dylematu wyboru pomiędzy Donaldem Trampem a Hillary Clinton. Amerykańscy politycy i eksperci wciąż debatują nad tym, w jakim stopniu rosyjska ingerencja przyczyniła się do zwycięstwa urzędującego prezydenta. Poglądy na ten temat zależą w dużym stopniu od identyfikacji partyjnej. Demokraci i ich zwolennicy przywiązują dużą wagę do konsekwencji takiej ingerencji w wynik wyborów. Natomiast wśród Republikanów bardziej powszechne jest łagodzenie jej skutków. Partyjne ramy debaty w tej sprawie narzucają Amerykanom ocenę. Wysiłki strony rosyjskiej na rzecz zwycięstwa D. Trumpa do pewnego stopnia wpłynęły na amerykańskich wyborców, ale to stosunkowo krótkoterminowe oddziaływanie miało niższą skalę oraz mniej negatywnych skutków w porównaniu z innymi bardziej destrukcyjnymi konsekwencjami takiej ingerencji. Spośród takich konsekwencji można wymienić rozczarowanie obywateli wynikami wyborów, wątpliwości co do demokratycznego charakteru elekcji oraz amerykańskiego systemu politycznego[21].

W Wielkiej Brytanii wykorzystano rozpowszechnianie dezinformacji, wpływ propagandy na wyborców przez manipulowanie informacjami w mediach społecznościowych. W przeddzień i podczas referendum w sprawie Brexitu Rosjanie używali setki kont na Twitterze i na Facebooku, a także botnetów w celu rozpowszechniania tysięcy wiadomości ze wzmianką o Brexicie[22].

We Francji w przededniu wyborów prezydenckich przeprowadzono zmasowane ataki na sieć komputerową kandydata E. Macrona i jego partii politycznej, natomiast 36 godzin przed wyborami opublikowano dziewięć gigabajtów skradzionych informacji mających zaszkodzić temu kandydatowi. Wśród opublikowanych oryginalnych dokumentów znalazły się także liczne sfałszowane materiały, mające zasiać wątpliwości i dezinformujące francuskich wyborców. Dzięki internetowym botom, skrajnie pra-

[19] *Obama expels 35 Russian diplomapts in retaliation for US election hacking*, https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack, inf. 24 VI 2020.

[20] *Russian Meddling in Elections*…, p. 5.

[21] M. Tomz, J. Weeks, *Public Opinion and Foreign Electoral Intervention*, Accessed: 8 October 2018, p. 24–26, https://web.stanford.edu/~tomz/working/TomzWeeks-ElectoralIntervention-2018-08-24.pdf, inf. 26 VI 2020.

[22] *Russian Meddling in Elections*…, p. 7.

wicowym aktywistom i WikiLeaks informacje te szybko rozprzestrzeniły się online[23]. Jednak w tym wypadku atak na kandydata w wyborach prezydenckich Emanuela Macrona nie doprowadził do pożądanego przez Rosjan efektu ze względu na jego znaczącą przewagę nad kontrkandydatem[24].

W Niemczech ingerencja polegała na zainfekowaniu rządowych komputerów wirusowymi trojanami oraz dużych kradzieżach informacji[25]. Rozprzestrzenianie dezinformacji przez tak zwanych trolli Kremla oraz zniekształcanie informacji przyczyniły się do osłabienia pozycji A. Merkel oraz jej politycznego zaplecza. Ponadto zapewniły bezprecedensowy sukces wyborczy niemieckiej ultraprawicy, wykazującej prorosyjskie sympatie.

W Hiszpanii rozpowszechnianie informacji separatystycznych i wezwań do oddzielenia się Katalonii również było związane z działalnością rosyjskich botnetów. Pośrednim dowodem na to była niezwykle duża liczba repostów wiadomości rosyjskich agencji informacyjnych Russian Today i Sputnik przez konta wenezuelskie i anonimowe[26].

Rosja podjęła również próby wywierania wpływu na społeczeństwo Holandii. Operacje informacyjne Moskwy dotyczyły postępowania holenderskich śledczych w sprawie zestrzelenia przez rosyjskich wojskowych cywilnego lotu MH17 nad Donbasem oraz referendum w sprawie ratyfikacji Umowy o stowarzyszeniu między Ukrainą a UE w kwietniu 2016 roku. Wywierając wpływ na wewnętrzną debatę polityczną, Rosja oprócz elektronicznych kanałów rozpowszechniania informacji stosowała również inne metody, np. kreując fałszywy obraz Ukraińców i Ukrainy przez podstawione postacie[27].

Biorąc pod uwagę ostrzeżenia służb specjalnych o potencjalnym zagrożeniu związanym z ingerencją Rosji w systemy informacyjne i wyborcze, władze holenderskie podjęły wiele środków zapobiegawczych. W szczególności zrezygnowały z elektronicznego głosowania i automatycznego liczenia głosów, a także zakazały urzędnikom komisji wyborczych korzystania z poczty elektronicznej i urządzeń pamięci USB. Podjęte środki pozwoliły zapobiec znaczącym wpływom Rosji na wynik głosowania w Holandii w 2017 roku[28].

[23] *Ibidem*, p. 8.

[24] *How France successfully countered Russian interference during the presidential election*, EURACTIV, https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/, inf. 27 VI 2020.

[25] C. Stelzenmuller, *The impact of Russian Interference on Germany's 2017 Elections*, Testimony before U.S. Senate Select Committee on Intelligence, Wednesday, June 28, 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections, inf. 27 VI 2020.

[26] D. Alandete, *Russian Network Used Venezuelan Accounts to Deepen Catalan crisis*, „El Pais", 11 November 2017, https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html, inf. 28 VI 2020.

[27] E. Brattberg, T. Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435, inf. 25 VI 2020.

[28] *Ibidem*.

Ingerencja Rosji przebiegała według ściśle określonego schematu. Najpierw partie polityczne lub instytucje państwowe zgłaszały nieuprawniony dostęp do swoich sieci i serwerów, złamanie zabezpieczeń poczty elektronicznej i kradzież danych osobowych. Następnie skradzione dane wyciekały i rozprzestrzeniały się za pośrednictwem sieci społecznościowych i botów, a później były wykorzystywane przez tradycyjne media do publikowania najbardziej sensacyjnych informacji. W tym samym czasie „zbiorniki drenażowe" (media publikujące niezweryfikowane informacje), powiązane lub kontrolowane przez władze rosyjskie, publikowały wymyślone historie, zachęcając do dyskusji polaryzujących społeczeństwo i potęgujących myślenie z kategorii spiskowych teorii.

Susan Davis stwierdziła, że Rosja, wykorzystując wolność słowa i prasy na Zachodzie, będzie dążyła do delegitymizacji instytucji demokratycznych w państwach członkowskich NATO. „Nie ma wątpliwości, że udział Rosji w takich operacjach będzie kontynuowany w najbliższej przyszłości"[29]. Powyższe działania Federacji Rosyjskiej należy ekstrapolować także na realia ukraińskie, zwłaszcza że w poprzednich latach pojawiły się liczne próby takiej ingerencji w wewnętrzne sprawy Ukrainy. Ponadto Ukrainę można uznać za swego rodzaju poligon doświadczalny, na którym Rosja wykorzystuje praktycznie cały arsenał swoich działań wywrotowych[30], testując skuteczność metod i narzędzi wpływu informacyjnego w skali regionalnej i globalnej.

Potwierdzeniem tej tezy są informacje z otwartych źródeł o ujawnieniu i zablokowaniu sieci internetowych agitatorów zaangażowanych przez rosyjskie służby specjalne celem ingerencji w wybory prezydenta Ukrainy w 2019 roku. W szczególności angażowano mieszkańców miast Dnipro, Kryvy Rih i Nikopol będących administratorami grup w sieciach społecznościowych, przygotowując grunt do manipulacji opinią publiczną. Rosyjscy mocodawcy nakazali znaleźć blogerów i aktywnych użytkowników sieci społecznościowych, mających publikować wiadomości polityczne wysyłane z Rosji za odpowiednie wynagrodzenie. Kolejnym zadaniem było przyciąganie „fałszerzy" informacji do rejestrowania stron internetowych w ukraińskim segmencie nazw domen oraz wyszukiwanie i zamawianie usług przez obywateli Ukrainy w celu promowania zasobów internetowych i treści w firmach informatycznych zlokalizowanych w południowo-wschodnich regionach Ukrainy. Zgodnie z planem działania rosyjskich służb specjalnych miały pozostać niejawne, a zaangażowanie służb w upowszechnianie fałszywych informacji miało nie przeszkadzać w poparciu prorosyjskich uczestników procesu wyborczego.

Rosyjscy kuratorzy zaplanowali zaostrzenie sytuacji społeczno-politycznej na Ukrainie w przeddzień i podczas wyborów prezydenckich. W tym celu wykonawcy musieli „zniekształcić" informację, aby zdyskredytować władze państwa i samorząd lokalny oraz stworzyć rzekomo patriotyczny kierunek narracji w sieciach społecznościowych.

[29] *Russian Meddling in Elections*…, p. 10.

[30] A.F. Rasmussen, M. Chertoff, *West still isn't prepared to stop Russia meddling into elections*, "Polityko", https://www.politico.com/magazine/story/2018/06/05/russia-election-meddling-prepared-218594, inf. 27 VI 2020.

Na wybranych stronach zaplanowano publikacje materiałów dyskredytujących państwo, w tym wezwania do gwałtownych zmian społecznych i porządku konstytucyjnego Ukrainy z naruszeniem jej integralności terytorialnej[31].

Na początku lutego 2019 roku Służba Bezpieczeństwa Ukrainy wyśledziła mieszkańca obwodu czernihowskiego, który prowadził antyukraińską agitację w sieciach społecznościowych zgodnie z instrukcjami służb specjalnych Federacji Rosyjskiej. Celem działalności jego i współpracowników było rozpowszechnianie fałszywych informacji i manipulacja opinią publiczną w kontekście kreowania pożądanych dla Rosji nastrojów wyborczych[32].

W połowie lutego 2019 roku przerwano w obwodzie czerniowieckim działalność „Białej Kominiarki", obywatela Ukrainy współpracującego z agentami rosyjskimi i przygotowującego zakłócenia procesu wyborczego. W pierwszym etapie, w celu podniesienia poziomu aktywności protestacyjnej w społeczeństwie, organizatorzy sfilmowali i opublikowali w sieci wideo z wezwaniem do obalenia porządku konstytucyjnego na Ukrainie i siłowego przejęcia władzy. Zadaniem „Białej Kominiarki" było także zaangażowanie w ramach ruchu protestacyjnego przywódców organizacji obywatelskich i działaczy z różnych regionów Ukrainy nieuznających wyboru dokonanego przez „lud", zwołanie „wiecu", narzucenie władzom wymogów trudnych do spełnienia. Następnym krokiem było wyjście na ulicę i zajęcie budynków administracji państwowej, w tym Rady Najwyższej Ukrainy. Do rzekomego przejęcia władzy siłą planowano wykorzystać działaczy struktur patriotycznych i nacjonalistycznych. Plan przewidywał zorganizowanie „pokojowych" protestów w celu sprowokowania starć pomiędzy demonstrantami a służbami mundurowymi. W odpowiednim momencie zza pleców „pokojowych" demonstrantów miały wyłonić się grupy bojowe.

Podjęcie aktywnych działań zaplanowano na 31 marca 2019 roku – dzień wyborów prezydenta Ukrainy. Natychmiast po zamknięciu lokali wyborczych, zgodnie ze scenariuszem „fałszowania wyników wyborów", planowano zwołanie wieców w Kijowie i regionach, a także sprowokowanie ofiar śmiertelnych celem mobilizacji i radykalizacji protestów społecznych[33].

Innym udokumentowanym faktem ingerencji były próby pozyskania przez rosyjskie służby wywiadowcze danych dotyczących sieci informatycznej obsługującej wybory prezydenckie. W tym celu mieszkaniec Dnipra stworzył i kierował grupą osób upowszechniającą fałszywe informacje i inne destrukcyjne materiały, w tym publiczne apele o zmianę granic państwowych Ukrainy. Internetowy prowokator, pracując w branży telekomunikacyjnej, prowadził korespondencję elektroniczną z mieszkań-

[31] *На Дніпропетровщині СБУ викрила підготовку РФ до втручання у майбутні вибори Президента України* (відео), https://ssu.gov.ua/ua/news/1/category/1/view/5159#.zrUem400.dpbs, inf. 30 VIII 2018.

[32] *На Чернігівщині СБУ викрила організатора мережі антиукраїнських інтернет-агітаторів*, https://ssu.gov.ua/ua/news/1/category/21/view/5681#.avZZwvs6.dpbs, inf. 7 II 2019.

[33] *„Біла балаклава". СБУ розкрила новий план Росії щодо зриву виборів в Україні*, „Тиждень.ua" 19 лютого 2019, https://tyzhden.ua/News/226813, inf. 20 II 2019.

cem Rosji i gromadził dane dotyczące sieci strategicznie ważnych operatorów telekomunikacyjnych, lokalizacji węzłów telekomunikacyjnych oraz czasu potrzebnego do przywrócenia ich funkcjonowania po uszkodzeniu.

Według rosyjskich służb specjalnych, masowe uszkodzenia linii przesyłowych i urządzeń wybranych operatorów telekomunikacyjnych zakłócą stabilne funkcjonowanie systemu Państwowego Rejestru Wyborców, jak również zablokują lub sparaliżują pracę Jednolitego Systemu Informacyjnego i Analitycznego „Wybory"[34].

3. Podsumowanie

Przedstawione w niniejszym artykule przykłady pokazują znaczące zaangażowanie Rosji w walkę informacyjną w ramach rywalizacji z Zachodem, w której Ukraina dla Kremla występuje w podwójnej roli – jako część „świata ruskiego" oraz pole konfrontacji ze strukturami zachodnimi (UE i NATO). „Nieobojętność" Rosji w procesie wyborów w państwach demokratycznych i transformujących się wskazuje na wysokie stawki w tej geopolitycznej grze. Biorąc pod uwagę fakt, iż Rosja w dalszym ciągu prowadzi wobec Ukrainy wojnę hybrydową, w tym agresję zbrojną, ingerencja Kremla w wybory ukraińskie ma na celu zniekształcenie ich wyników oraz doprowadzenie do władzy polityków prorosyjskich, działających zgodnie z jej interesami strategicznymi.

Pozostaje mieć nadzieję, że państwo ukraińskie odpowiednio oceni i zareaguje na tego typu zagrożenia oraz podejmie działania zapobiegające i neutralizujące powyższe praktyki strony rosyjskiej. Centralna Komisja Wyborcza utworzyła specjalną grupę roboczą z udziałem SBU i Specjalnej Służby Komunikacji w celu szczegółowej analizy technicznej i audytu systemów CKW, uruchamiania i bezpiecznego funkcjonowania Centralnego Systemu Wyborczego[35]. W wyniku czego udało się unieszkodliwić rosyjskie ataki DDoS na system CKW, dokonane 24–25 lutego 2019 roku. Celem zabezpieczenia przed tymi i innymi atakami cybernetycznymi Rada Bezpieczeństwa Narodowego i Obrony wspólnie ze Służbą Bezpieczeństwa Ukrainy i policją opracowały mechanizmy obrony cybernetycznej CKW przy współpracy z partnerami ze Stanów Zjednoczonych Ameryki[36]. Dużą rolę w neutralizowaniu destrukcyjnego wpływu rosyjskiej propagandy na społeczeństwo ukraińskie odgrywa społeczeństwo obywatelskie (Ukraińskie Kryzysowe Centrum Medialne i StopFake) oraz odpowiednie instytucje rządowe. Dmytro Zolotukhin, ekspert ds. walki informacyjnej i wiceminister w Ministerstwie Polityki Informacyjnej Ukrainy w latach 2017–2019 stwierdził, że rosyjska propaganda posługuje się metodą serialową w narzucaniu konkretnym jej odbiorcom określonego, zafałszowanego obrazu rzeczywistości społecznej i politycznej, w której stosowana narracja opiera się na

[34] *СБУ викрила наміри спецслужб РФ блокувати роботу систем, задіяних для забезпечення проведення виборів* (відео), https://ssu.gov.ua/ua/news/1/category/2/view/5775#.HqDw7Cn8.dpbs, inf. 26 II 2019.

[35] *ЦВК та СБУ створять спеціальну групу – представник спецслужби*, https:/dt.ua/UKRAINE/cvk-ta-sbu-stvoryat-specialnu-grupu-predstavnik-specsluzhbi-302478_.html, inf. 12 II 2019.

[36] *Порошенко розповів про кібератаки на ЦВК з російської сторони*, https://dt.ua/POLITICS/poroshenko-rozpoviv-pro-kiberataki-na-cvk-z-rosiyskoyi-storoni-303983_.html, inf. 26 II 2019.

fałszywkach, manipulacji, sfabrykowanych wypowiedziach działaczy politycznych i społecznych, nieprawdziwych lub niepełnych danych statystycznych oraz perswazji mających na celu „przekonanie" do rosyjskiej racji stanu[37].

Badania destrukcyjnych działań oraz wymierzonych ataków informacyjnych ze strony Rosji wobec społeczeństwa amerykańskiego i wielu państw UE dowodzą, że nawet dojrzałe demokracje nie są jeszcze w stanie skutecznie przeciwstawić się trwającej ingerencji w stabilne funkcjonowanie reżimów demokratycznych. Ukraina jako demokratyzujące się państwo w obliczu przedłużającego się rosyjsko-ukraińskiego konfliktu zbrojnego posiada zdecydowanie większe problemy z przeciwstawieniem się rosyjskiej ingerencji w życie polityczne, w tym w proces wyborczy. Ukraina potrzebuje zarówno wewnętrznej konsolidacji politycznej, jak i wsparcia ze strony sojuszników i partnerów w zakresie przeciwdziałania różnego rodzaju zagrożeniom ze strony Rosji.

~

Streszczenie: Współczesne konflikty wojenne zmieniają charakter stosowanych środków i pod wieloma względami cele, do których dążą strony. Widać to na przykładzie operacji specjalnych, które współczesna Rosja podejmuje w celu zdestabilizowania strategicznych rywali i zwiększenia wpływów w krajach, które sama określiła jako sferę swoich interesów. Jednym z ważnych narzędzi realizacji korzystnej dla Kremla polityki są celowe, wywrotowe wysiłki zmierzające do zniekształcenia przebiegu i wyników demokratycznych wyborów. W szczególności przez wykorzystanie agentów wpływu, kształtowanie agendy przez poszczególne środki masowego przekazu, wprowadzanie destrukcyjnych tendencji do dyskursu publicznego. Nie będąc pionierem w tej dziedzinie, Rosja wielokrotnie interweniowała podczas wyborów w różnych krajach. Stany Zjednoczone Ameryki, Wielka Brytania i Francja nie uniknęły tego losu. Ponadto rosyjska ingerencja jest widoczna w przestrzeni poradzieckiej, np. w Gruzji, Mołdawii, a szczególnie intensywnie na Ukrainie. Artykuł analizuje przykłady takich ingerencji w proces wyborczy i zwraca uwagę na konieczność opracowania i wdrożenia środków przeciwdziałających im.
Słowa kluczowe: ingerencja wyborcza, podważanie demokracji, wojna hybrydowa, Rosja

Hybrid challenges to democracy: some cases of Russia's foreign interference in elections

Abstract: Contemporaneous wars are subjected to some profound changes regarding applied means and sometimes goals of the confronting parties. It is becoming clear with the cases of special operations, launched by Russia against its strategic rivalries and countries, which have been proclaimed by the latter sphere of Russia's geopolitical interests. Kremlin tries to undermine the electoral process and distort their results. They serve very important tools of Russia's actual policy. For instance, they aim at distortion of the election agenda settings, spreading fake news and false perception of main

[37] D. Zolotukhin, *„Biała Księga" specjalnych operacji informacyjnych wobec Ukrainy w latach 2014–2018*, „Biuletyn/Monitoring Propagandy i Dezinformacji" 2020, nr 1, s. 10, https://phavi.umcs.pl/at/attachments/2020/0728/105857-biuletyn-politologiav2-ostateczna-.pdf, inf. 27 VIII 2020.

topics for a public discourse into targeted countries. USA, France, Great Britain seem to be only a few examples of those actions.
Most of all, the vulnerability towards Russia's interference into democratic elections are attributed with Georgia, Moldova, Ukraine and some other post-soviet counties. The article characterizes some cases of such intrusion and points out at the urgent necessity to set in forth counter-policy against this kind of the interference.
Keywords: interference in elections, challenged democracy, hybrid war, Russia

Гибридные вызовы демократии. Избранные примеры внешнего вмешательства России в выборы

Аннотация: Современные войны меняют природу используемых средств, а во многом и преследуемых сторонами целей. Это просматривается на примере тех спецопераций, которые предпринимаются современной Россией для дестабилизации своих стратегических соперников и усиления влияния в тех странах, которые она сама провозгласила сферой своих интересов. Одним из важных инструментов осуществления выгодной для Кремля политики выступают ее целенаправленные подрывные усилия, направленные на искажение хода и результатов демократических выборов. В частности, путем использования агентов влияния, формирования повестки дня отдельными средствами массовой информации, внесения деструктивных тенденций в публичный дискурс. Не будучи первопроходцем в данной сфере, Россия неоднократно осуществляет вмешательство в ход выборов в различных странах. Этой судьбы не избежали США, Великобритания, Франция. Тем более российское вмешательство заметно на постсоветском пространстве, как-то в Грузии, Молдове, и особенно интенсивно в Украине. В статье рассматриваются отдельные примеры такого вмешательства в избирательный процесс и обращается внимание на необходимость разработки и осуществления мер по противодействию им.
Ключевые слова: вмешательство в выборы, подрыв демократии, гибридная война, Россия

Bibliografia

Aitel D., *Guest editorial: The DNC hack and dump is what cyberwar looks like*, "Ars Technica" 2016, no. 17, https://arstechnica.com/information-technology/2016/06/guest-editorial-the-dnc-hack-and-dump-is-what-cyberwar-looks-like/, inf. 10 VI 2020.

Alandete D., *Russian Network Used Venezuelan Accounts to Deepen Catalan crisis*, „El Pais", 11 November 2017, https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html, inf. 28 VI 2020.

„Bila balaklava". SBU rozkryla novyy plan Rosiyi shchodo zryvu vyboriv v Ukrayini, „Tyzhden'.ua" 19 II 2019, https://tyzhden.ua/News/226813, inf. 20 II 2019.

Brattberg E., Maurer T., *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435, inf. 25 VI 2020.

Chivvis C.S., *Understanding Russian "Hybrid Warfare" and What Can be Done About it*, Testimony presented before the House Armed Services Committee on March 22, 2017, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf, inf. 15 IX 2019.

Galante L., Ee S., *Defining Russian Election Interference: an Analysis of Select 2–14 to 2018 Cyber Enabled Incidents*, Atlantic Council, Scowcroft Center for Strategy and Security, September 2018.

Grizzly Steppe – Russian Malicious Cyber Activity, December 29, 2016. Reference Number: JAR-16-20296A, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf, inf. 10 VI 2020.

How France successfully countered Russian interference during the presidential election, EURACTIV, https://www.euractiv.com/section/elections/news/how-france-successfully-countered-russian-interference-during-the-presidential-election/, inf. 27 VI 2020.

Jensen M., *Russian Trolls and Fake News: Information or Identity Logics?*, „Journal of International Affairs" 2018, vol. 71, no. 1.5.

Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security, Release Date: October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, inf. 12 VI 2020.

Mel'nychuk I., *Intehratsiyni proekty Rosiys'koyi Federatsiyi na postradyans'komu prostori*, Chernivtsi 2015.

Na Chernihivshchyni SBU vykryla orhanizatora merezhi antyukrayins'kykh internet-ahitatoriv, https://ssu.gov.ua/ua/news/1/category/21/view/5681#.avZZwvs6.dpbs, inf. 7 II 2019.

Na Dnipropetrovshchyni SBU vykryla pidhotovku RF do vtruchannya u maybutni vybory Prezydenta Ukrayiny (video), https://ssu.gov.ua/ua/news/1/category/1/view/5159#.zrUem400.dpbs, inf. 30 VIII 2018.

Obama expels 35 Russian diplomapts in retaliation for US election hacking, https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack, inf. 24 VI 2020.

Perepelytsya H. i in., *Asymetriya mizhnarodnykh vidnosyn*, Kyyiv 2005.

Poroshenko rozpoviv pro kiberataky na TsVK z rosiys'koyi storony, https://dt.ua/POLITICS/poroshenko-rozpoviv-pro-kiberataki-na-cvk-z-rosiyskoyi-storoni-303983_.html, inf. 26 II 2019.

Rasmussen A.F., Chertoff M., *West still isn't prepared to stop Russia meddling into elections*, "Politico", https://www.politico.com/magazine/story/2018/06/05/russia-election-meddling-prepared-218594, inf. 27 IV 2020.

Russian Meddling in Elections and Referenda in the Alliance, General Report by Susan DAVIS (United States) General Rapporteur – 181 STC 18 E fin. 11 November 2018, https://www.nato-pa.int/sites/default/files/2018-11/181%20STC%2018%20E%20fin%20-%20RUSSIAN%20MEDDLING%20-%20DAVIS%20REPORT.pdf, inf. 19 VI 2020.

Sartori G., *Teoria demokracji*, Wydawnictwo Naukowe PWN, Warszawa 1994.

Savage C., *Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention,* "New York Times" 26.07.2016, https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html, inf. 15 VI 2020.

SBU vykryla namiry spetssluzhb RF blokuvaty robotu system, zadiyanykh dlya zabezpechennya provedennya vyboriv (video), https://ssu.gov.ua/ua/news/1/category/2/view/5775#.HqDw7Cn8.dpbs, inf. 26 II 2019.

Sokół W., *Geneza i ewolucja systemów wyborczych w państwach Europy Środkowej i Wschodniej*, Wydawnictwo UMCS, Lublin 2007.

Stelzenmuller C., *The impact of Russian Interference on Germany's 2017 Elections*, Testimony before U.S. Senate Select Committee on Intelligence, Wednesday, June 28, 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections, inf. 27 VI 2020.

Świątkowska J., *Działania prowadzone w cyberprzestrzeni jako metoda ingerencji w demokratyczny proces wyborczy*, [w:] *Walka informacyjna: uwarunkowania, incydenty, wyzwania*, red. H. Batorowska, Wydawnictwo UP, Kraków 2017.

Tomz M., Weeks J., *Public Opinion and Foreign Electoral Intervention*, Accessed: 8 October 2018, https://web.stanford.edu/~tomz/working/TomzWeeks-ElectoralIntervention-2018-08-24.pdf, inf. 26 VI 2020.

TsVK ta SBU stvoryat' spetsial'nu hrupu – predstavnyk spetssluzhby, https://dt.ua/UKRAINE/cvk-ta-sbu-stvoryat-specialnu-grupu-predstavnik-specsluzhbi-302478_.html, inf. 12 II 2019.

Van De Velde J., *The Law of Cyber Interference in Elections*, Available at SSRN 3043828 (May 15, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828, inf. 15 VI 2020.

Vystupleniye i diskussiya na Myunkhenskoy konferentsii po voprosam politiki bezopasnosti. 10 fevralya 2007 goda, http://kremlin.ru/events/president/transcripts/24034, inf. 23 X 2019.

Zolotukhin D., *„Biała Księga" specjalnych operacji informacyjnych wobec Ukrainy w latach 2014–2018*, „Biuletyn/Monitoring Propagandy i Dezinformacji" 2020, nr 1.